وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR ANNABA

جامعة باجي مختار- عنابة

**Année : 2016**

**Faculté: Sciences de l'Ingéniorat**
**Département: Electronique**

**MEMOIRE**
**Présenté en vue de l'obtention du diplôme de : MASTER**

**THEME**

# IMPLEMENTATION D'UN GENERATEUR BBS POUR LE CRYPTAGE D'IMAGE

**Domaine : Sciences et Technologies**
**Filière : Electronique**
**Spécialité: Electronique Biomédicale**

**Par : KERMACHE LYLIA**

**DEVANT Le JURY**

| | | | |
|---|---|---|---|
| **Président** | **: ZEDAM MOUHAMED** | **MCB** | **U.ANNABA** |
| **Directeur de mémoire** | **: MANSOURI KHALED** | **MCA** | **U.ANNABA** |
| **Examinateur** | **: BOUGHAZI MOUHAMED** | **MCA** | **U.ANNABA** |

# Conclusion générale :

La sécurité des images est un domaine en pleine expansion, vu la quantité importante d'images qui circule dans divers réseaux de télécommunications, particulièrement Internet.

Cette large utilisation des images, impose la mise en œuvre de systèmes cryptographiques capable de fournir un bon niveau de sécurité tout en assurant une vitesse de traitement élevée.

Et avec le développement des systèmes embarqués ,le cryptage partiel (chiffrement sélectif) s'est imposé petit, ou' il garantit un bon compromis entre de sécurité et vitesse de traitement.

Nous nous sommes intéressé dans ce travail à la sécurité des images utilisant le cryptage partiel.

La méthode utilisée dans ce travail basé sur le générateur pseudo aléatoire BBS, elle est très simple et meilleure pour la mise en œuvre le chiffrement et déchiffrement d'image.

# Sommaire :

**Introduction générale**……1

**Chapitre : Introduction générale à la cryptologie**

……

I . Introduction……2

I.2 Cryptographie ……2

I.2.1 Historique……2

I.2.2 Définitions et Terminologie……3

I.2.3 Objectifs de la cystographie……4

I.2.4 Principes de la cystographie ……5

I.2.4.1 Principe de Kirchhoff……5

I.2.4.2 Principe de Shannon……5

I.2.5 Famille de la cryptographie……6

I.2.5.1 Chiffrement symétrique……6

I.2.5.1.1 Présentation……6

I.2.5.1.2 Avantages et inconvénients……7

I.2.5.2 Chiffrement asymétrique……7

I.2.5.2.1 Présentation……7

I.2.5.2.2 Avantages et inconvénients……8

I.2.6 Méthode pour Chiffrer en Clé Secrète ……9

I.2.6.1 Chiffrement à flot……9

I.2.6.2 Chiffrement par Blocs……9

I.3 Cryptanalyse……9

I.3.1 Définition……9

I.3.2 Evolution ……10

I.3.3 Types d'attaques cryptanalytiques……10

I.3.4 Modèle d'attaque sur un schéma de chiffrement symétrique……11

I.3.5 Sécurité d'un crypto-système……12

I.4 conclusion……13

## Chapitre II : L'image et cryptage sélectif

II.1 Introduction……14

II.2Définition de l'image……14

II.3 Présentation de l'image……14

II.3.1 Représentation des images numériques……15

II.3.2 Caractéristique d'une image numérique……15

II.3.3 Les différents types de l'image numérique……17

II.4 Outils d'évaluation de system de cryptage de l'image……18

II.4.1 Déviation maximale……19

II.4.3 Entropie……19

II.5Méthodes de cryptage des images……19

II.6 Cryptage sélectif……21

II.6.1 Définition……21

II.6.2 Applications du chiffrement sélectif……23

II.7 Les types de cryptage sélectif……23

II.7.1 Chiffrement sélectif par région d'intérêt……23

II.7.2 Chiffrement sélectif des plans de bits……..24

II.8 Conclusion……24

Chapitre III : Le Chiffrement à flot

III.1Introduction……25

III.2 Définition……25

III.3 Principe du chiffrement par flot……25

III.4 Le chiffrement de vernam……26

III.5 Propriétés générales de chiffrement à flot……26

III.6 Avantages et inconvénients de chiffrement à flot……26

III.6.1 Les Avantage……26

III.6.2 Les inconvénients……26

III.7 Chiffrement à flot et générateurs pseudo-aléatoires……27

III.8 Le masque jetable……27

III.8.1 Définition……27

III.8.2 Sécurité……28

III.9 Les types de chiffrement à flot……28

III.9.1Chiffrements synchrones……28

III.9.2 Chiffrement auto-synchronisants……29

III.10 Caractéristiques du chiffrement auto-synchronisant……30

III.11 Les types d'attaque par flot……30

III .11.1 Les attaques par corrélation…… 30

III.11.2 Les attaque par corrélation rapides……31

III.11.3 Les attaque algébriques……32

III.11.3.1 Attaque algébriques rapides……32

III.11.3.2 Attaques algébriques évoluées sur le chiffrement à flot……33

III.12 Conclusion……33

## Chapitre IV : Les Générateurs pseudo-aléatoire

… ……..

IV.1 Introduction…… 34

IV.2 Les générateurs pseudo-aléatoire pour le chiffrement à flot……..34

IV.3 Sécurité des générateurs pseudo-aléatoires……..35

IV.4 Générateurs basés sur des LFSRs……35

IV.4.1 Les générateur à combinaison non-linéaire……36

IV.4.2 Les générateurs à filtre non-linéaire……..36

IV.4.3 Les générateurs à horloge contrôlée……36

IV.5 Générateur de Blum-Blum-Shub(BBS)……..…38

IV.6 Sécurité du générateur BBS……40

IV.7 Conclusion……40

Chapitre V : Chiffrement sélectif en utilisant le générateur BBS

…….

V.1 Introduction…… 41

V.2 Description de la méthode……..41

V.3 Algorithme de chiffrement et de chiffrement d'image……44

V.3.1 Chiffrement……44

V.1.2 Déchiffrement……45

V.4 Algorithme de calcul la suite chiffrante engendrée par le générateurBBS..45

V.5 Simulation et résultat……45

V.6 Test visuel……..46

V .6.1 Teste 1 : une seule région……46

V.6.2 Teste 2 : Deux régions ……47

V.6.3 Teste 3 : plusieurs régions……48

V.7 Analyse de la sécurité……50

V.7.1 Analyse de l'histogramme……..50

V.7.2 Analyse de coefficient de corrélation……53

V.7.3Analyse de l'entropie……54

V.8 Conclusion……55

**Conclusion générale**

**Bibliographie**

# *Liste des figures*

Liste des figures

Figure I.1 : Fonctionnement d'un système cryptographique……4

Figure I.2 : Schéma simple d'un chiffrement symétrique……6

Figure I.3 : Schéma simple d'un chiffrement asymétrique……8

Figure I.4 : Problème de communication en présence d'adversaire posé par Shannon……..12

Figure II.1 Image en pixel……..15

Figure II.2 : Voisinage d'un pixel……16

Figure II.3 : Histogramme d'une image……17

Figure II.2 : Image en niveaux de gris……18

Figure II.5 : Image couleur……18

Figure II.6 : Chiffrement complet……20

FigureII.7Diagramme de base crypto système d'image basé sur le chiffrement……22

Figure II.8 : chiffrement sélectif par région intérêt……23

Figure II.9 : Cryptosystème d'image basé sur le chiffrement sélectif des plans de bits…… 25

Figure III.1 : principe de chiffrements à flot synchrones……..29

Figure III.2: principe de chiffrements à flot synchrones additifs……..29

Figure III.3 : principe de chiffrements à flot auto-synchronisants……30

Figure III.4 : Modèle de l'attaque par corrélation……31

Figure III.5 : Modèle de l'attaque par corrélation rapide……32

Figure IV.1 : Trois finalistes de eSTREAM……36

Figure IV.2 : Exemple de LFSR binaire…… 40

Figure IV.3 : Trois constructions classiques basées sur des LFSRs……37

Figure IV.4 : générateur BBS……39

Figure V.1 : Bloc diagramme de l'approche proposée ……42

Figure V.2 : Organigramme de Chiffrement……43

Figure V.3 : Organigramme de Déchiffrement……44

Figure V.4: test 1 pelvis.gif……46

Figure V.5: test 2 thighs .tif……..48

Figure V.6: 1 test 3 cameramen .tif……50

Figure V.7: les histogrammes de test 1……51

Figure V.8: les histogrammes de test 2……51

Figure V.9: les histogrammes de test 3……52

# Liste des tableaux

# Liste des tableaux

Tableau V.1 : Analyse du Corrélation……..53

Tableau V.2 : Analyse de l'entropie de test 1…….……..54

Tableau V.3 : Analyse de l'entropie de test 2……..…54

Tableau V.4 :Analyse de l'entropie de test 3……..54

# Liste des abréviations

**RSA :** Revenu de solidarité active

**ECB :** Electronique Code Book

**CBC:** Cipher Blok Chaining

**DES:** Data Encryption Standard

**DEA:** Data Encryption Algorithm

**AES:** Advanced Encryption Standard

**MSB:** Most Signifiant Bit plane

**LSB:** Least Signifiant Bit plane

**LSFR:** Linear Feedback Shift Register

**LSFRs:** Log Song From Ren and Stimpy

**OFB:** L'Organisation Féline belge

**UmMTS:** Universal Mobile Telecommunications System

# Chapitre I :

# Introduction Générale à la Cryptologie

# Chapitre 02 :
# L’image et cryptage sélectif

# Chapitre 03 :

# Le Chiffrement à flot

# Chapitre 04 :

# Les Générateurs pseudo-aléatoire

# Chapitre 5 :

# Chiffrement sélectif en utilisant le générateur BBS

# Conclusion Générale:

# Bibliographie

# Introduction Générale:

# Remerciement

*Avant tout, je remercie tout puissant qui j'ai donné la force et la volonté pour finir ce projet.*

*Je remercie chaleureusement  mon encadreur*

*Ms.mansouri . k  pour son suivi, son aide, sa patience qu'il trouve ici l'expression de notre profonde gratitude, sa gentillesse et sa grande disponibilité.*

*Je remercie également les membres de jury d'avoir accepté de juger mon travail.*

*La liste serait encore longue à devant l'évidence d'un oubli, je tenue à remercier tous ceux qui  j'ai encouragé.*

# Dédicace

*Je dédie ce travail :*

*A mes chers parents pour leurs encouragements.*

*Sacrifices et amour*
*Que dieu les bénissent et me les garde.*

*A mes très chères sœurs*

*A mon très cher frère*

*Et a toute ma famille*

*A tous mes amis*

*A tous les étudiants de la promotion*

*2015 /2016*

*Et à tout ce qui m'aime*

***Lylia***

# Introduction générale

Depuis toujours, l'homme s'est beaucoup intéresse aux différentes techniques permettant aux être de communiquer entre deux. Au cours du temps, l'évolution des sciences a permis de mettre en place des systèmes de transmission donnant la possibilité à chacun de communiquer avec n'importe lequel de ses voisins, quel que soit la distance qui les sépare.

Avec le développement d'utilisation l'internet, de plus en plus d'entreprises ouvrent leur systèmes d'information à leurs fournisseurs, il est donc essentiel de connaitre les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs des systèmes d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

L'information transmise n'est pas exclusivement sous forme de données textuelles mais également audio, images numériques et autre multimédia.

Les fichiers images sont très largement utilisés dans notre vie quotidienne, et plus leur sécurité n'est vitale.

Et c'est pour répondre à ces besoins que la cryptologie, avec ces deux disciplines :

Crypto graphie et cryptanalyse, s'est intéressé à la sécurité de la transmission ou du stockage des fichiers ont vu de jour.

Cependant, chiffrer entièrement les données n'est pas toujours raisonnable, particulièrement dans les systèmes ou l'énergie est limitée, Dans ce genre de cas , gagner du temps, et donc économiser l'énergie consommée, devient une question primordiale et c'est pour ces raisons que le chiffrement sélectif (ou cryptage partiel) s'impose. Ce dernier consiste à chiffrer une partie de l'image, et transmettre (ou stocker) la partie chiffrée avec la partie non chiffrée (en clair).

On traite dans ce mémoire, le cryptage sélectif de l'image par le générateur pseudo aléatoire BBS.

# Chapitre I :

# Introduction Générale à la cryptologie

## 1.1Introduction :

Depuis toujours, l'être humain a essayé de mettre en place des protocoles servant à un échange sûr d'informations tels que les cachets d'enveloppes et les signatures manuscrites. De nos jours ces mêmes procédés trouvent leurs analogues dans le monde informatique et ceci grâce à la cryptologie.

Le terme cryptologie signifie littéralement « science du secret ». D'un point de vue historique, cette science a été créée pour garantir la confidentialité des communications militaires. L'objectif recherché par ses utilisateurs était de transformer un message clair en un texte incompréhensible, sauf pour son destinataire légitime.

## 1.2Cryptographie :

### 1.2.1 Historique :

L'histoire de la cryptographie est déjà longue. On rapporte son utilisation en Égypte il y'a4000 ans. Cependant, la première attestation de l'utilisation délibérée d'un moyen de chiffrement des messages vint de la Grèce vers le VIème siècle avant J.-C., et se nomme le scytale, qui était un bâton sur lequel l'expéditeur enroulait une bandelette autour et écrivait. Longitudinalement le message sur le bâton, puis déroulait la bandelette et l'expédiait au destinataire. Sans la connaissance du diamètre du bâton qui jouait le rôle de clé, il était impossible de déchiffrer le message .Plus tard, les romains adoptèrent un chiffrement qui consistait en une substitution mono alphabétique simple en décalant de trois lettres de l'alphabet. Cette technique était connue sous le nom de chiffre de Jules César**.**

Puis pendant des siècles, on assista à la mise au point de plusieurs techniques de chiffrement mais qui étaient pour la plupart limitées au besoin de l'armée et de la diplomatie. Mais c'est la prolifération actuelle des systèmes de communication qui a fait sortir la cryptographie de l'ombre. De plus elle a diversifié la demande et provoqué le développement de nouvelles techniques cryptographiques. Elle est à l'origine d'un développement rapide depuis les dernières décennies, qui ne semble pas s'essouffler aujourd'hui, bien au contraire.

### 1.2.2 Définitions et Terminologie :

Le mot cryptographie provient du grec kryptus(caché) et graphein(écrire). C'est la technique visant à protéger un échange d'informations par un codage du message. Cette technique est pratiquée par des cryptographes.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une Transformée qui le rend incompréhensible : c'est ce qu'on appelle un chiffrement**,** qui à partir d'un texte en clair (plaintext) donne un texte chiffré ou un cryptogramme (ciphertext).

Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en questions sont des fonctions mathématiques, appelés algorithmes cryptographiques qui dépendent d'un paramètre appelé clé.

- **Cryptographie :** On peut définir la cryptographie comme étant l'étude des théories et techniques mathématiques relative aux aspects de sécurité de l'information tels que : la confidentialité, l'intégrité des données, l'authentification, …etc. La cryptographie n'est pas seulement un moyen de sécuriser l'information mais plutôt un ensemble d'outils et de techniques [1]**.**
- **Algorithme cryptographique :** Un algorithme cryptographique ou algorithme déchiffrement transforme un message, appelé texte clair en un texte chiffré (cryptogramme) qui ne sera lisible que par son destinataire légitime. Cette transformation est effectuée par une fonction de chiffrement généralement paramétrée par une clef de chiffrement. Un interlocuteur privilégié peut alors déchiffrer le message en utilisant la fonction de déchiffrement correspondant. On distingue deux grands types d'algorithmes de chiffrement qu'on verra un peu plus loin, les algorithmes à clef secrète et les algorithmes à clef publique.
- **Clef :** Donnée importante permettant de construire les fonctions de cryptage et de décryptage. Sans connaissance de la clé de décryptage, le décryptage doit être impossible.
- **Système cryptographique :** Un système cryptographique (ou cryptosystème) est unn-uplet (*M, C, K, C, D*) où :
    - *M* est l'ensemble des textes clairs possibles.
    - *C* est l'ensemble des textes chiffrés possibles.

- $K$ est l'ensemble des clefs possibles ;
- Pour tout $k \in K$, il y a une règle de chiffrement dans $E$, $e_k : M \to C$ et une règle dedéchiffrement dans $D$, $d_k : C \to M$ telles que $\forall m \in M, d_k(e_k(m)) = m$.

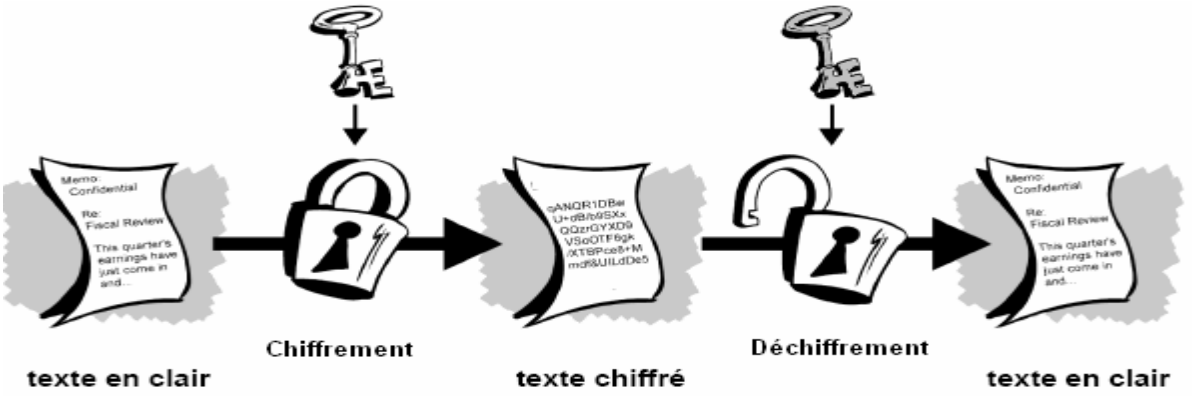



**Figure-1-1: Fonctionnement d'un système cryptographique**

### 1.2.3 Objectifs de la cryptographie :

Les principaux services offerts par la cryptographie moderne sont:

- **Confidentialité :** assurer que les données concernées ne pourront être dévoilées que par les personnes autorisées.
- **Intégrité :** Assurer que les données ne seront pas altérées pendant leur transmission ou leur stockage.
- **Authentification/Identification :** Prouver l'origine d'une donnée ou s'assurer de l'identité d'une personne.
- **Non répudiation :** Garantir que les actions ne seront pas reniées.

En plus de ces quatre objectifs fondamentaux, on peut citer :

- **Signature :** Lier une information à une entité.
- **Autorisation :** Lever une restriction d'accès à une information.
- **Contrôle d'accès :** Restreindre l'accès qu'aux entités privilégiées.
- **Anonymat :** Préserver l'identité d'une entité de la divulgation.

### 1.2.4 Principes de la cryptographie :

La sécurité de la plupart des crypto systèmes classiques reposait sur la confidentialité de l'algorithme de chiffrement, ce qui est considéré aujourd'hui comme absurde et contradictoire avec les principes fondamentaux qui régissent la cryptographie moderne **[2].**

### 1.2.4.1 Principe de Kirchhoff :

Un principe fondamental de la cryptographie a été énoncé par Kirchhoff **[2]** à la fin du dix-neuvième siècle. Il exprime que la méthode de chiffrement utilisée doit "pouvoir tomber sans inconvénients aux mains de l'ennemi". Autrement dit, la sécurité d'un chiffrement ne doit pas reposer sur la confidentialité de celui-ci mais uniquement sur la protection de la clé.
Ce principe a plusieurs justifications principalement:

- La confidentialité d'un algorithme secret est difficile à garantir. Il est en général connu de plusieurs personnes et il est souvent diffusé dans des logiciels ou dispositifs hardware à des utilisateurs non habilités au secret. La confidentialité de l'algorithme peut succomber à la corruption ou au reverse engineering**.**
- La sécurité d'un algorithme secret est difficile à évaluer (nombre d'algorithmes à l'origine secrets se sont révélés extrêmement faibles). Il est généralement admis que la meilleure garantie de sécurité d'un algorithme est apportée par une longue période d'évaluation par la communauté cryptographique mondiale.
- Un algorithme secret peut dissimuler des propriétés indésirables pour l'utilisateur final (existence de clés faibles par exemple). Il n'est donc pas adapté si la confiance envers le concepteur n'est pas établie.
- Enfin, pour le théoricien, c'est une hypothèse de travail sans laquelle il est impossible d'obtenir des résultats rigoureux de sécurité.

### 1.2.4.2 Principe de Shannon :

Shannon énonça que pour gommer les redondances dans un texte en clair, deux techniques s'imposaient : la confusion et la diffusion **[4].**

- **La confusion :**

Elle efface les relations entre le texte en clair et le texte chiffré. Elle évite l'analyse du texte chiffré par recherche de redondances et de motifs statistiques. Le moyen le plus simple cela est la substitution tel que le chiffre de Jules César**.**

- **La diffusion :**

Idéalement, le texte chiffré doit ressembler à une chaîne aléatoire de lettres saisies au clavier par un chimpanzé. Le but du cryptographe est d'éliminer tout indice qui, dans le texte chiffré, aiderait le cryptanalyse à retrouver le texte clair. Il s'agit pour cela d'éliminer les relations statistiques entre le texte chiffré et le texte clair correspondant. La diffusion combine

transposition et substitution et diffuse la structure statistique du texte clair parmi le texte chiffré.

La plupart des algorithmes de chiffrement modernes utilisent à la fois la confusion et la diffusion.

### 1.2.5 Famille de la cryptographie :

La cryptographie moderne a connu le développement de deux grandes familles d'algorithmes à base de clé :

- La cryptographie symétrique.
- La cryptographie asymétrique.

Les deux classes sont différentes dans leur conception et leurs domaines d'application néanmoins elles coexistent et ont chacun des avantages et inconvénients.

### 1.2.5.1 Chiffrement Symétrique :

#### 1.2.5.1.1 Présentation :

Les algorithmes de chiffrement symétrique (à clef secrète ou à clef privée) sont ceux pour lesquels émetteurs et destinataires partagent une même clef secrète, autrement dit, les clefs de chiffrement et de déchiffrement sont identiques (Fig.-1.2). L'emploi d'un algorithme à clef secrète lors d'une communication nécessite donc l'échange préalable d'un secret entre les deux protagonistes à travers un canal sécurisé ou au moyen d'autres techniques cryptographiques.

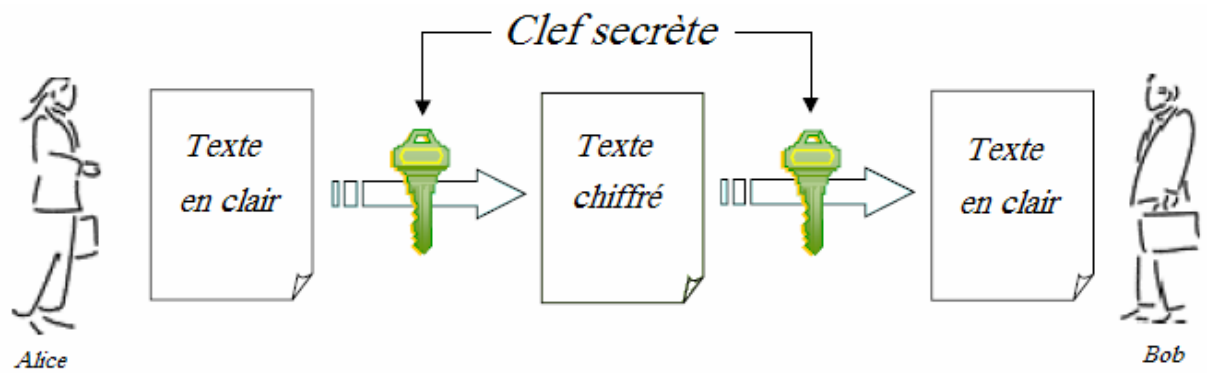



**Fig1.2 Schéma simple d'un chiffrement symétrique**

Un paramètre essentiel pour la sécurité d'un système à clef secrète est la taille de l'espace des clefs. En effet, il est toujours possible de mener sur un algorithme de chiffrement une attaque dit exhaustive pour retrouver la clef. Cette attaque consiste simplement à énumérer toutes les

clefs possibles du système et à essayer chacune d'entre elles pour décrypter un message chiffré. Une telle attaque devient donc hors de portée dès que l'espace des clefs est suffisamment grand. Au vu de la puissance actuelle des ordinateurs, on considère qu'une clef secrète doit comporter au minimum 64 bits.

Nous décrivons dans ce qui suit, les primitives de cryptographie symétrique, que sont les algorithmes de chiffrement par bloc et par flot.

#### 1.2.5.1.2 Avantages et inconvénients :

- **Avantage :**
  - Vitesse de traitement élevée.
  - Clés relativement courtes.
  - Permet de concevoir différents mécanismes cryptographiques
- **Inconvénients :**
  - Dans une communication entre deux parties, la clé doit rester secrète des deux côtés.
  - Complexité de la gestion des clés. Dans un réseau de *n* entités, on doit gérer $n * (n-1)/2$ clés.
  - Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique.

### 1.2.5.2 Chiffrement Asymétrique :

#### 1.2.5.2.1 Présentation :

L'inconvénient des chiffrements symétriques reste la distribution des clés : l'expéditeur et le destinataire doivent partager ce secret pour pouvoir respectivement chiffrer et déchiffrer. En effet, la clef étant indispensable au déchiffrement du message, il faut bien qu'à un moment ou à un autre la transmission de celle-ci ait lieu. La difficulté est donc la suivante : comment transmettre cette clé sans que celle-ci tombe entre de mauvaises mains. Pour résoudre en partie le problème de la gestion des clés, une nouvelle façon de chiffrer est proposée en 1976 par Whitfie lDiffie et Martin Hellman. Il s'agit de la cryptographie asymétrique (à clef publique) :

- La principale différence entre le chiffrement à clef secrète et celui à clef publique est la présence de deux clefs dans le second procédé de chiffrement.
- Une clef publique qui est mise à la disposition de quiconque désire chiffrer un message sans que cela ne mette en danger les informations secrètes.

- Une clef privée, qui doit être confidentielle, permettant le déchiffrement du message, chiffré avec la clef publique.

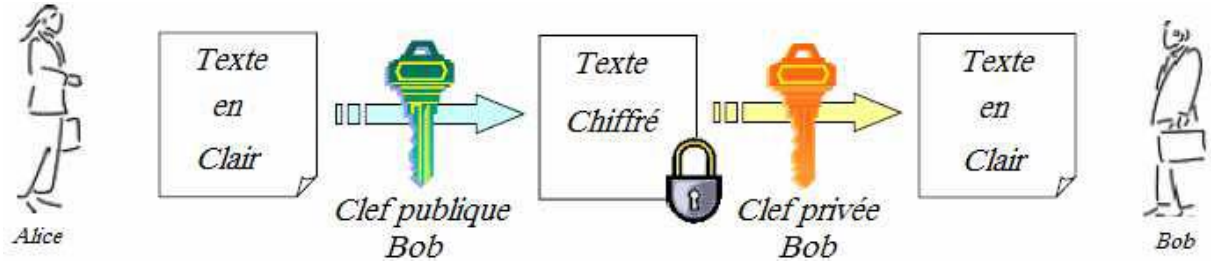



**Fig.1.3: Schéma simple d'un chiffrement asymétrique**

La notion essentielle sur laquelle repose le chiffrement à clef publique est celle de fonction à sens unique avec trappe. Une fonction est appelée à sens unique si elle est facile à calculer mais "impossible" à inverser. Impossible signifie ici infaisable en un temps réaliste avec une puissance de calcul raisonnable. Une telle fonction est dite avec trappe si le calcul de l'inverse devient facile dès que l'on possède une information supplémentaire (la trappe).

La construction d'un système de chiffrement à clef publique s'appuie généralement sur des problèmes mathématiques réputés difficiles, le plus célèbre est celui de la factorisation de grands nombres entiers, qui est à la base du système RSA **[5].**

### 1.2.5.2.2 Avantages et inconvénients :

- **Avantage :**
  - Seule la clé secrète a besoin d'être conservée de manière secrète.
  - Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique.
  - Assure la non-répudiation dans les schémas de signature numérique.
  - Gestion efficace des clés. 2n clés sont nécessaires dans un réseau de n utilisateurs.
- **Inconvénients :**
  - Performances moins bonnes que celles fournies par les systèmes symétriques.
  - Taille des clés, plus grand que celle des systèmes symétriques.
  - Nécessité de la mise en place d'infrastructures afin d'éviter les attaques par milieu.

### 1.2.6 Méthodes pour Chiffrer en Clé Secrète :

Suivant le contexte des données à chiffrer, l'une de ces méthodes de chiffrement est utilisée :le chiffrement à flot (communication, réseau filaire..) et le chiffrement par blocs (carte à puce, disque dur,...).

### 1.2.6.1Chiffrement à Flot :

Le principe des algorithmes à flot informatiquement sûrs repose sur le partage d'une clé K de longueur constante et non sur le partage d'une clé de longueur égale à celle du message à chiffrer. L'algorithme utilisé chiffre "à la volée" le flot de message clair par un ou-exclusif bit à bit (ou une opération similaire) avec une suite chiffrant ($k_i$) pour produire un flot de texte chiffré. La suite chiffrante k= ($k_i$) est produite par un générateur pseudo-aléatoire G à partir de la clé K et d'un vecteur d'initialisation.

### 1.2.6.2Chiffrement par Blocs :

On oppose souvent chiffrement à flot et chiffrement par blocs et pour cause : le premier utilise une suite chiffrante, le deuxième une fonction. Le chiffrement par blocs consiste à découper en blocs de longueur fixe n le message m à chiffrer, puis à traiter chaque bloc séparément. Il faut que n soit suffisamment grand pour éviter les attaques par dictionnaire.

Il existe plusieurs méthodes, appelées modes, pour chiffrer un message *m* à l'aide d'un algorithme de chiffrement par blocs $E_k$et d'une clé *k*. Le mode le plus simple est le mode (**ECB**) : le message *m* est découpé en blocs de taille *n* ; chaque bloc est chiffré séparément et on concatène ensuite les blocs de chiffré obtenus. Un autre mode de chiffrement très employé est le mode (**CBC**) : le message clair est ici encore découpé en blocs de longueur *n*, mais au lieu de chiffrer simplement un bloc, on chiffre le bloc *i* préalablement combiné par ou exclusif avec le chiffré du bloc précédent.

## 1.3 Cryptanalyse :

### 1.3.1 Définition :

La cryptanalyse s'oppose, en quelque sorte à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyse c'est tenter de se passer de cette dernière.

On peut voir la cryptanalyse comme une science complémentaire à la cryptographie, et dont le but est l'étude et l'analyse des procédés cryptographiques afin de prouver leur

robustesse. Il convient de souligner que briser un algorithme cryptographique ne signifie pas nécessairement trouver un moyen pratique de récupérer le texte en clair en utilisant seulement le texte chiffré. D'un point de vue académique, ceci revient à trouver une faiblesse dans le chiffrement qui peut être exploitée avec une complexité inférieure à une attaque par force brute (exhaustive). Le chiffrement ainsi cassé ne devient pas inutile pour autant, mais son degré de sécurité s'affaiblit.

La cryptanalyse d'un système peut être alors soit partielle (l'attaquant découvre le texte clair correspondant à un ou plusieurs messages chiffrés interceptés), soit totale (l'attaquant peut déchiffrer tous les messages, par exemple en trouvant la clé).

### 1.3.2 Évolution :

La cryptanalyse a connu un développement parallèle à celui de la cryptographie, et ceci bien avant l'ère informatique. On rapporte que les premiers traités de cryptanalyse remontent au $X^{éme}$.
Des siècles plus tard, durant la seconde guerre mondiale, la célèbre machine à crypter allemande Enigma fut "cassée" par des cryptanalystes alliés dont Alan Turing.

Mais c'est depuis l'adoption en 1978 du premier standard de chiffrement (DES) que la cryptanalyse moderne a vu le jour et est rentré dans le domaine de la recherche. Ainsi de nombreuses attaques et analyses cryptanalytiques furent menées contre le DES pour en mesurer le degré de sécurité **[6].**

### 1.3.3 Types d'attaques cryptanalytiques :

Il existe plusieurs types génériques d'attaques cryptanalytiques, classées selon les moyens dont dispose l'attaquant. Chacune de ces attaques repose sur l'hypothèse que le cryptanalyste dispose d'une parfaite connaissance de l'algorithme de chiffrement **[7]**:

- **L'attaque à texte chiffré seulement :** Le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffrés avec le même algorithme. La tâche du cryptanalyste est de retrouver le texte en clair du plus grand nombre de messages possible ou mieux encore de trouver la ou les clefs qui ont été utilisées.
- **L'attaque à texte en clair connu :** Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages mais aussi aux textes en clair, correspondants. Sa tâche est de retrouver la ou les clefs utilisées ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

- **L'attaque à texte en clair choisi :**Non seulement le cryptanalyste à accès aux textes chiffrés et aux textes en clair mais de plus il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car l'attaquant peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef. La tâche de l'attaquant consiste à retrouver la ou les clefs utilisées ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef. Cette attaque est parfois appelée "attaque à texte en clair choisi statique".
- **L'attaque à texte en clair choisi adaptative :** C'est un cas particulier de l'attaque à texte en clair choisi. Non seulement le cryptanalyse peut choisir les textes en clair mais il peut également adapter ses choix en fonction des textes chiffrés précédents.
  Dans une attaque à texte en clair choisi, le cryptanalyste est juste autorisé à choisir un grand bloc de texte en clair au départ tandis que dans une attaque à texte en clair adaptative, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite. Cette attaque est parfois appelée" attaque à texte en clair choisi dynamique".
- **L'attaque à texte chiffré choisi :** Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique, sa tâche est de retrouver la clef. Ce type d'attaque est particulièrement applicable aux crypto-systèmes à clef publique.
- **L'attaque à clef choisie :** Cela n'est pas une attaque où le cryptanalyste peut choisir la clef; il est seulement au courant de quelques relations entre différentes clefs.

### 1.3.4 Modèle d'attaque sur un schéma de chiffrement symétrique :

En se référant à l'axiome de Kirchhoff stipulant que l'algorithme de chiffrement était parfaitement connu de l'adversaire, et que seule la clé devait être protégée, Claude Shannon fut l'un des premiers à mettre en évidence le problème de communication en présence d'attaquants (adversaires).

Ainsi on suppose:

- Deux entités communicantes à travers deux canaux. (Expéditeur et Destinataire)
- Un premier canal sûr par sur lequel transitent les messages.
- Un deuxième canal sécurisé pour la transmission de la clé (ou les clés).
- Un adversaire ou attaquant

La figure (Fig. -1-4) montre un schéma illustrant un modèle d'attaque sur un protocole de communication basé sur un crypto système à clé secrète :

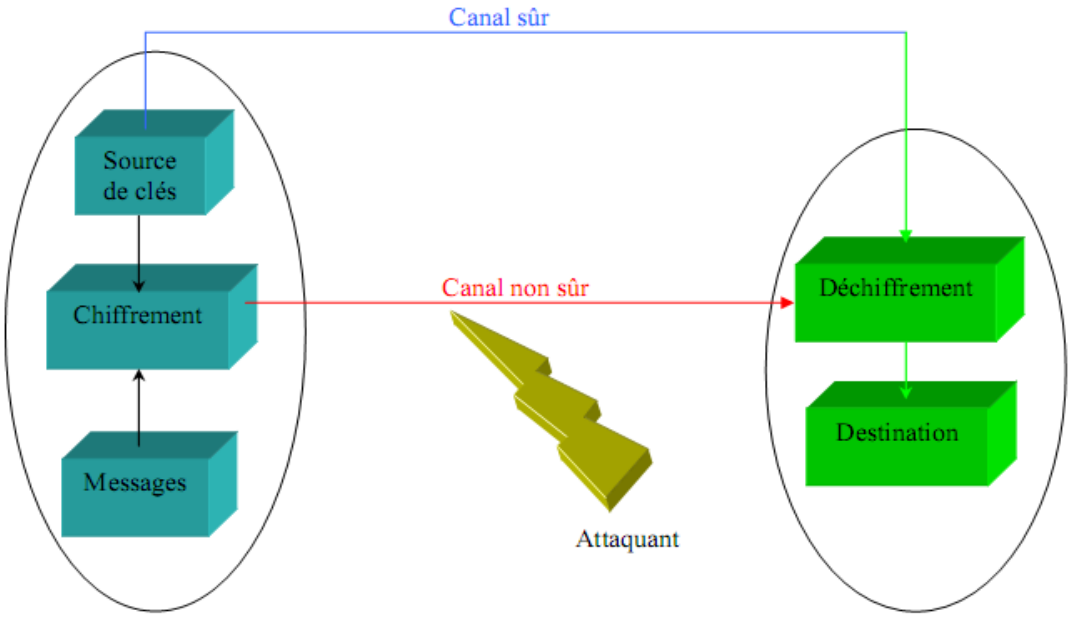



**Fig1-4: Problème de communication en présence d'adversaire posé par Shannon**

### 1.3.5 Sécurité d'un crypto-système :

Les différents algorithmes ont des niveaux de sécurité divers, plus ou moins difficiles à casser. Un algorithme est considéré invulnérable par calcul, s'il ne peut pas être cassé avec les ressources disponibles actuellement et dans le futur. On peut mesurer la complexité d'une attaque de l'une des manières suivantes:

- **Complexité en information :** La quantité d'information nécessaire en entrée pour l'algorithme
- **Complexité en temps :**Le temps nécessaire pour achever l'attaque, appelé aussi effort.
- **Complexité en espace :** La quantité de mémoire nécessaire à l'attaque.

En général la complexité de l'attaque est prise comme le minimum de ces trois facteurs.

Tandis que la complexité d'une attaque est constante (jusqu'à ce qu'un cryptanalyste trouve une meilleure attaque), la puissance de calcul est toute sauf constante. Et avancer qu'un algorithme est sûr parce qu'on ne peut pas le casser avec la technologie d'aujourd'hui est hasardeux. Les bons crypto-systèmes sont conçus pour être invulnérables même avec les puissances de calcul prévues d'ici à de nombreuses années dans le futur  Une autre métrique

peut être utilisée pour mesurer la performance de l'attaque indépendamment du nombre de paires est le rapport Signal/Bruit (signal to Noise Ration :S/N).

Une autre métrique peut être utilisée pour mesurer la performance de l'attaque Indépendamment du nombre de paires est le rapport Signal/Bruit (Signal to Noise Ration:S/N).

## 1.4 Conclusion :

Dans ce chapitre, nous avons donné un aperçu sur le vaste monde de la cryptologie avec ses deux disciplines: cryptographie et cryptanalyse, ainsi que l'évolution de ces deux sciences à travers l'histoire avant et après l'avènement de l'ère informatique. Ce premier chapitre, constitue une fenêtre ouverte sur cette science afin d'initier le lecteur aux aspects de la cryptologie.

Le chapitre qui suit, est consacré à l'image et cryptage sélectif.

# Chapitre II:

# L’image et cryptage sélectif

## II.1 Introduction :

Avec le développement rapide de la technologie et des systèmes numériques, la transmission des données multimédia à travers des réseaux ouverts tel que tâche importante et nécessaire. Beaucoup d’applications nécessitent des systèmes sécuritaires robustes pour le stockage et la transmission des mages. Une image numérique est constituée de points ayant chacun un niveau de gris compris entre 0 et 255, ces points sont appelés « pixel », l’images est représentée par une matrice bidimensionnelle f où chaque élément f (i,j) représente le niveau du gris correspondant, pour les images en couleur, une troisième dimension est utilisée pour les images en couleurs Rouge (R)vert (V) et bleu (B).

Dans la plupart des images, les valeurs des pixels adjacents sont fortement corrélée, la valeur d’un pixel adjacents, un système de cryptage efficace doit réduire la corrélation des pixels adjacents et changer aléatoirement leurs valeurs en utilisent une clé prise dans un espace très large.

### II.2. Définition de l’image :

L’image est une représentation d’une personne ou d’un objet par la peinture, la sculpture, le dessin, la photographie, le film, etc. C’est aussi un ensemble structuré d’informations qui, après affichage sur l’écran, ont une signification pour l’œil humain.

### II.3. Présentation de l’image:

De nos jours, l'utilisation d'images est très répandue que ce soit pour des applications professionnelles ou bien ludiques. Le plus souvent, ces images sont définies dans un espace couleur à trois composantes tel l'espace «RVB 24 » dans lequel la valeur de chaque canal est codée sur un octet. Le nombre de couleurs disponibles pour coder une image est donc supérieur à 16 millions. Ce nombre important de possibilités entraîne que, la plupart du temps, aucun des pixels de l'image n'a une couleur identique aux autres pixels. Nous parlons ici d'images réelles de scènes d'extérieur ou d’intérieur, et pour lesquelles le panel des couleurs existantes n'est limité que par la technologie employée.

L’image constitue l’un des moyens de communication les plus importants, elle est utilisés par l’homme pour communiquer avec l’autrui, donc on peux défini l'image comme une représentation d'une scène par la peinture, le dessin, la photographie, Le film. C'est aussi un ensemble structuré d'information qui, après affichage sur l'écran, a une signification pour l'œil humain.

### II.3.1. Représentation des images numériques:

une image numérique est une matrice de pixels repérés par leur coordonnées (x, y). S'il s'agit d'une image couleur, un pixel est codé par 3 composantes (r, g, b) (chacune comprise au sens large entre 0 et 255), représentant respectivement les "doses" de rouge, vert et bleu qui caractérisent la couleur du pixel. S'il s'agit d'une image en niveau de gris, il est codé par 1 composante comprise au sens large entre 0 et 255, représentant la luminosité du pixel.

### II.3.2. Caractéristique d'une image numérique:

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants :

**a) Pixel :** Le pixel, ou point en français, est l'unité de base d'une image numérique matricielle. C'est le plus petit point de l'image, c'est une entité calculable qui peut recevoir une structure et une quantification. Si le bit est la plus petite unité d'information que peut traiter un ordinateur, le pixel est le plus petit élément que peuvent manipuler les matériels et logiciels d'affichage ou impression. La lettre A, par exemple, peut être affichée comme le groupe de pixels (Voir la Figure II.1.).

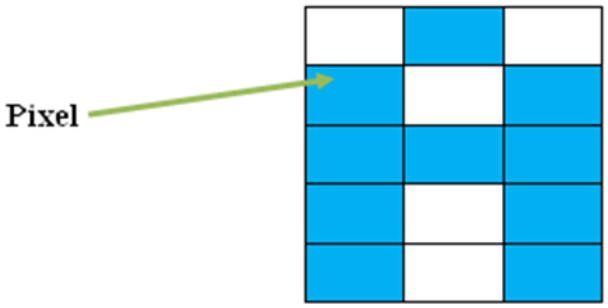
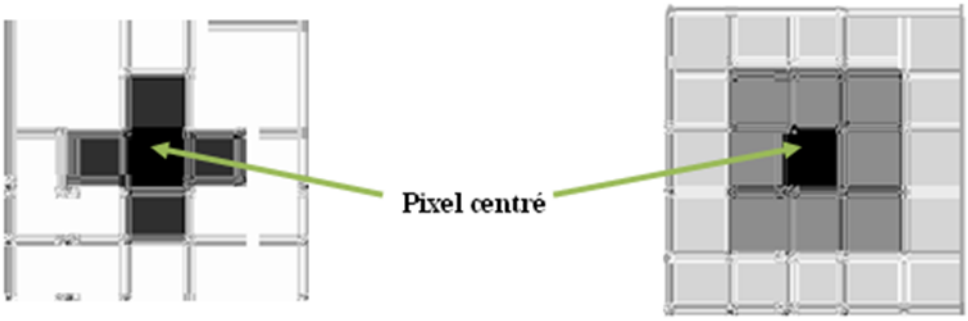



Figure II.1: Image en pixels

**b) Voisinage d'un pixel:** L'image discrète est représentée par un maillage carré. Les métriques couramment utilisées en maillage carré sont désignées par d4 et d8 (Voir la Figure II.2).




a) d4 voisinage d'un pixel b) d8 voisinage d'un pixel

**Figure II.2: Voisinage d'un pixel**

**c) Dimension :** C'est la taille de l'image. Lorsqu'elle est présentée sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multiplié par le nombre de colonnes donne le nombre total de pixels (dimension).

d) Histogramme : L'histogramme est une fonction qui donne la fréquence d'apparition de tous les niveaux de gris. Dans une image donnée et qui ne tient pas compte de leurs distributions spatiales (voir la Figure II.3). On aura en abscisse le niveau de gris allant de 0 à N=255, et en ordonnés, sera représenté Le nombre de pixels affectés à chaque niveau de gris. Le calcul d'histogramme peut faire l'objet, d'une comparaison de deux images obtenues sous éclairages différents et une amélioration de certaines proportions afin d'extraire les informations utiles. Il peut être utilisé pour améliorer la qualité concernant la visualisation d'une image (Rehaussement d'image).

De point de vue statistique, on peut modéliser l'histogramme d'une image comme une probabilité d'une variable aléatoire tel qu'une image en niveaux de gris a:

$$H(i) = \text{prob}(N_j = i) = X_i ; \text{ Dont } 0 \leq X_i \leq 1. \qquad [II.1]$$

Ng : désigne la variable aléatoire (niveau de gris).

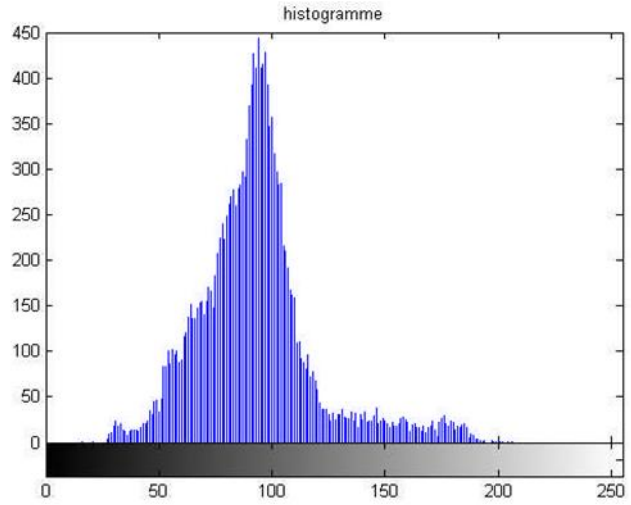



**Figure II.3: Histogramme d'une image**

## 2.3.3. Les différents types de l'image numérique :

L'image est défini par :

Le nombre de pixels en largeur et en hauteur,

L'étendue des teintes de gris ou des couleurs que peut prendre chaque pixel (on parle de dynamique de l'image).

Son format d'enregistrement. Les données de l'image peuvent être structurées de différentes façons = différents formats d'images (tif, gif, jpeg,…).

Selon le progrès technologique, l'image numérique est passée par plusieurs phases, car en trouve:

### a) Image binaire:

Une image binaire est une image de x lignes et y colonne ou chaque point peut prendre uniquement la valeur 0 ou 1.

Généralement les pixels sont noirs (0) ou blancs (1). L'intensité lumineuse est codé sur un bit. Dans ce cas sa valeur devient : f ($i$,$j$)=0 ou f($i$ ,$j$)=1.

Elle est utilisée par exemple dans le cas de numération d'un texte pour envoyer un fax. Elle prendre un espace mémoire faible, le temps de calcule réduit.

### b) Image en niveaux de gris :

Une image en niveaux de gris autorise un dégradé de gris entre le noir et le blanc. Chacun de ses pixels a un niveau de gris dans l'intervalle bien défini [ 0 , max ]. Lorsque chaque pixel représenté sur m bits, l'image possède $2^m$ niveaux de gris différents 0 ou max=$2^m$-1.

Ces images sont codées sur 1 octet et sont utilisées pour reproduire des photos en noir et blanc ou du texte dans certaines conditions (notamment lorsque l'on utilise un filtre pour adoucir les contours pour obtenir des caractères plus lisses) [8].

Exemple : la figure (II.4) ci-dessus représente une image en niveaux de gris.

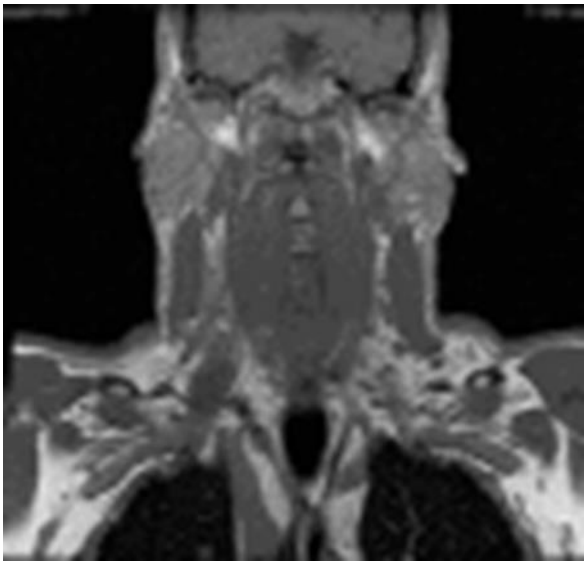


**Figure II.4: Image en niveaux de gris.**

### c) Image couleur:

Exemple : la figure ci-dessus représente une image couleur.

**Figure II.5: Image couleur.**

## II.4 Outils d'évaluation de system de cryptage de l'image :

L'inspection visuelle des images cryptée pour tester les systèmes de cryptage de l'image n'est pas suffisante pour juger les propriétés cachées de l'image, d'autres techniques sont utilisées pour mesurer le degré de cryptage qualitativement. [10] Les histogrammes sont l'argument utilises dans l'évaluation des systèmes de cryptage. Ils représentent le pourcentage de chaque niveau de gris dans l'image. Pour une bonne image cryptée, L'histogramme correspondant doit être aussi uniforme que possible En plus de histogrammes, beaucoup d'autres paramètres sont utilisés, la variation maximale (DM),le coefficient ce corrélation (CC),l'entropie (H) et le taux du nombre de pixels change (TNPC)sont parmi les plus utilisée.

### II.4.1 Déviation maximale :

Elle permet de mesurer la déviation maximale entre le nombre de niveau des gris entre l'image en clair et l'image crypte, DV est donne par :

$$DV=(\frac{h_0+h_1}{2}) +\sum_{i=1}^{i=254} hi \qquad [II.2]$$

Ou hi en l'amplitude de la différence absolue des niveaux du gris a la valeur i , une valeur élevé de DV indique une bonne image cryptée.

### 2.4.2 Coefficient de corrélation:

Il mesure la corrélation entre l'image en clair et l'image cryptée, une valeur proche de 1 indique une très grande ressemblance entre les deux, et une valeur proche de 0 indique au contraire une très grande différence, ce coefficient est donnée par :

$$CC=\frac{cov(x,y)}{\sqrt{d(x)}\sqrt{d(y)}} \qquad [II.3]$$

$$cov(x,y) = \frac{1}{N}\sum_i^n = (xi - E(x)(yi - E(y)) \qquad [II.4]$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^2 \qquad [II.5]$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} xi \qquad [II.6]$$

xi et yi ou i,j=1,2,…N sont les niveaux de gris des images x et y

### 2.4.3 Entropie:

Elle définie comme suit :

$$He = -\sum_{i=0}^{255} P(i)log2p(i) \qquad [II.7]$$

Avec: He : Entropie p(i) Est la probabilité d'apparition du niveau de gris i

Une valeur élevée de l'entropie est une indication d'une image fortement cryptée.

Une propriété très importante des l'image chiffrées est leur sensibilité aux petits changements de clé ou de l'image en clair. Si C_1et C_2 sont les images cryptées correspondantes aux très petites variations de la clé ou de l'image en clair, (un seul pixel qui change), la différence entre

C_1 et C_2 peux être mesurée par le taux du nombre de pixels change TNPC donne par :

$$TNPS= \frac{\sum i,jD(i,j)}{N\times M}100\% \qquad [II.8]$$

D est une matrice de même dimension que C_1 et C_2 avec

$$D(i,j) = \begin{cases} 0, Si\ C_1(i,j) = C_2(i,j) \\ 1, Si\ C_1(i,j) \neq C_2(i,j) \end{cases} \qquad [II.9]$$

N×M est la taille des images C_1 et C_2.

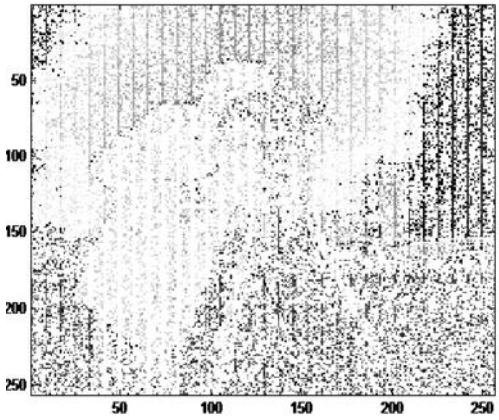
Le TNPC mesure le pourcentage de nombres de pixels différents entre les deux images.

## II.5. Méthodes de cryptage des images :

Les techniques de cryptage de l'image convertissent une image en une autre qui est difficile à comprendre. Les algorithmes classiques tel que DEA, AES,……,ne sont pas adaptés au cryptage des images vu leurs caractéristiques spécifiques telles que la très quantité d'information disponible et la forte corrélation entre les pixels. La plupart des techniques de cryptage de l'image ont été propos »es de cryptage de l'image.

Il existe deux manières d'effectuer un chiffrement. La première consiste en un chiffrement complet où toutes les données sont chiffrées.

L'image original




l'image chiffrée

L'image déchiffrée

**Figure II.6 : Chiffrement complet**

Parmi les inconvénients de cette approche est que le chiffrement est toujours appliqué de la même manière, quelque soient l'application et le niveau de sécurité souhaité.

Aussi, la taille trop importante des données multimédia (images entre autres) n'avantage guère le fait de chiffrer/déchiffrer l'image directement, c'est pour ça qu'il est plus intéressant de chiffrer une partie de l'image seulement. D'où la nécessité du Chiffrement Sélectif ou Cryptage Partiel.

## II.6 Cryptage sélectif :

Un nombre important d'applications peut se contenter d'un niveau inférieur à un chiffrement complet en utilisant un chiffrement sélectif. Nous pouvons citer comme exemple les peintures numériques où elles doivent être présentées sur Internet avec une qualité visible réglable. Le transfert d'images depuis des téléphones portables peut également d'un chiffrement sélectif afin d'assurer un minimum de confidentialité. C'est aussi le cas pour les images médicales prises depuis un appareil médical et devant être envoyées sur le réseau afin d'établir un diagnostic à distance. De plus, l'appareil d'acquisition des images médicales peut se trouver dans une ambulance ou dans tout autre véhicule mobile, et dans ce cas la transmission est effectuée par l'intermédiaire de réseaux sans fil. Pour des raisons vitales, dans ce type d'applications, les images doivent être transmises rapidement et sûrement, et dans ce cas un chiffrement sélectif semble être la solution la plus appropriée, puisqu'il assure un bon compromis temps/niveau de sécurité **[11].**

### II.6.1 Définition [12]:

Le chiffrement sélectif est l'application d'un algorithme de chiffrement à une partie d'un flux de données. Le reste du flux non chiffré est transmis (ou stocké) en clair

Comme suite:

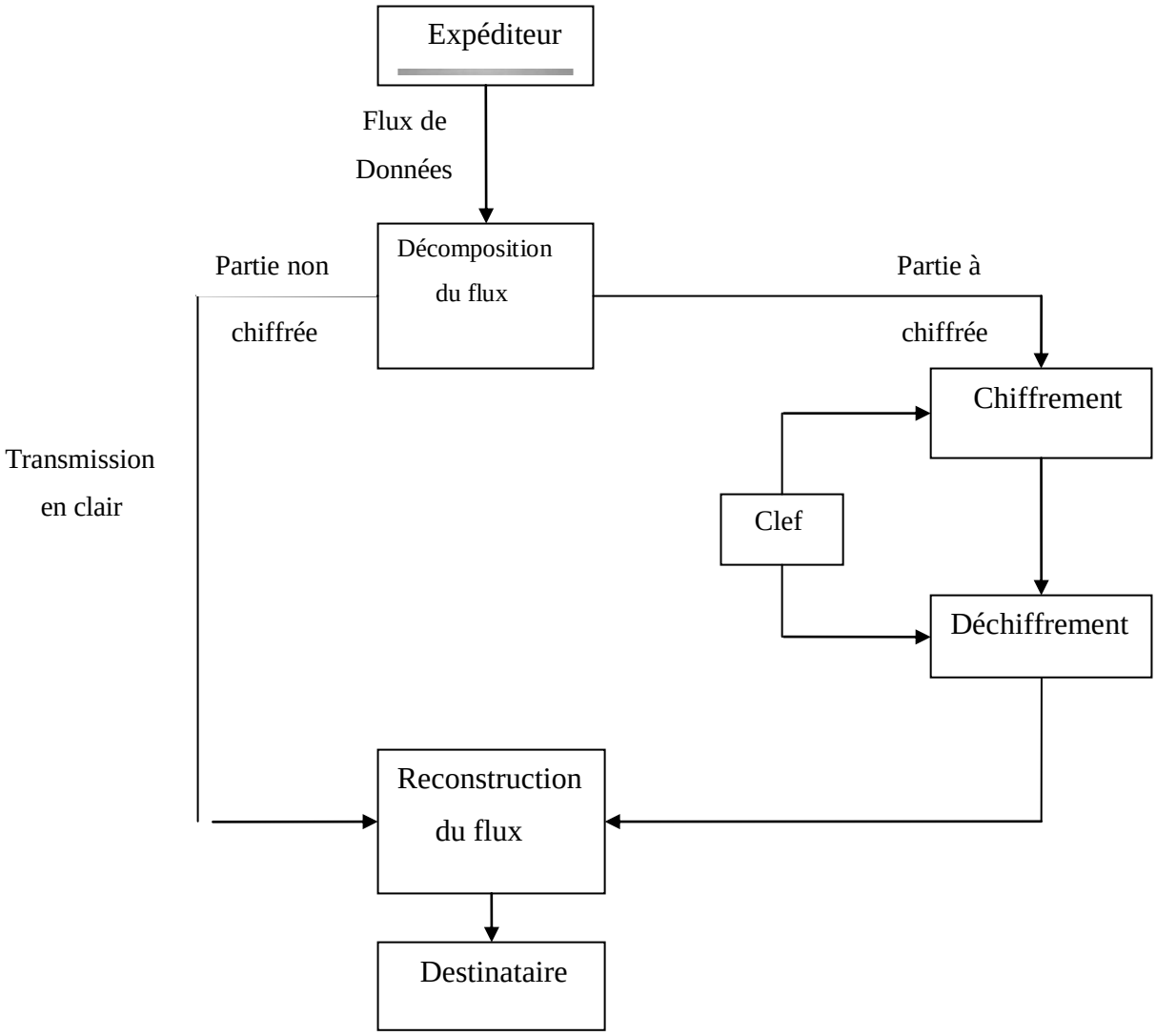



**Figure II.7 Diagramme de base crypto système d'images basé sur le chiffrement sélectif**

Le chiffrement sélectif doit garantir que le flux entier ne serait d'aucune utilité à quiconque personne ne pouvant pas déchiffrer la partie chiffrée, en d'autres termes qu'un message doit incohérent pour toute personnes n'ayant pas connaissance de la partie chiffrée.

Le chiffrement sélectif est particulièrement efficace si les deux raisons suivantes sont satisfaites:

- Difficulté d'exploiter une donnée transmise sans connaissance de la partie chiffre.
- Difficulté ou impossibilité d'attaquer l'algorithme de chiffrement appliqué à la partie chiffrée (la robustesse du chiffre doit être prouvée).

### 2.6.2 Applications du chiffrement sélectif [12][13]:

Le chiffrement sélectif offre plusieurs domaines d'application et plusieurs avantages, on peut citer par exemple:

- Réduire la complexité d'u crypto système en chiffrant uniquement une partie des données. Ceci aura pour effet de moins solliciter les composantes matérielles du système (implémentation hardware), et donc une économie considérable en énergie, Surtout s'il s'agit de systèmes évoluant dans un environnement mobile.
- Opportunités d'ajouter plusieurs schémas de chiffrement pour un même flux de données, en chiffrant chaque portion de la donnée d'une manière différente tout en transmettant les parties non chiffrées (non importantes) en clair.
- Offre plusieurs possibilités d'organiser le stockage de données. Par exemple, dans une application distribuée, où il est préférable de stocker les données en clair (moins importantes) dans des serveurs proches des utilisateurs, tandis que les parties importantes seront stockées dans des serveurs plus éloignés mais aussi plus sécurisés.
- Permet de fournir différentes qualités de flux, en fonction de la demande des utilisateurs. Et ceci en variant le taux de chiffrement.
- Offre la possibilité aux utilisateurs d'appliquer une sécurité proportionnelle ou réglable en fonction du niveau de protection désiré.

## II.7Les types de cryptage sélectif :

### II.7.1 Chiffrement sélectif par région d'intérêt:

L’image numérique fait partie des données dont le stockage nécessite une large capacité et dont la transmission a besoin d’une large bande passante. Cependant, dans la plupart des domaines de traitement d’image, l’utilisateur ne s’intéresse qu’à une partie de l’information transmise à travers l’image .Ex: une image médicale (figII.8) :

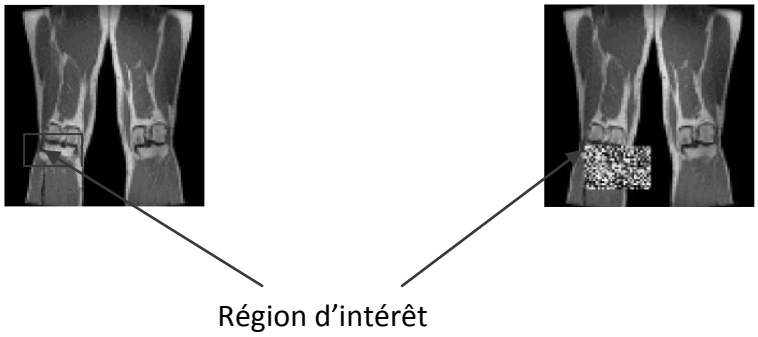



**Figure II-8 chiffrement sélectif par région intérêt**

### II.7.2 Chiffrement sélectif des plans de bits :

Un plan de bits, de l'anglais bitplane, est une structure mémoire qui stocke un seul bit pour chaque pixel d'une image numérique. Un plan de bits est donc une image monochrome.

Le plan de bits contenant les bits de poids fort de chaque pixel est appelé: Most Signifiant Bit plane (MSB). Et celui contenant les bits de poids faible des pixels est appelé : Least Signifiant Bit plane (LSB).

## Conclusion

Dans ce chapitre, on a étudié plusieurs types d'images et on a présenté deux types de chiffrement : complet et sélectif et on également les différentes notions de ce dernier.

Le chapitre qui suit, est consacré au chiffrement à flot.

# Chapitre III :

# Le Chiffrement à flot

## III.1 Introduction

Une des techniques de chiffrement à clef secrète la plus élémentaire et la plus sure est le chiffrement à flot, désignée en anglais par ¨One-Time-Pad ¨ ou ¨Stream Cypher ¨. Le principe est simple : additionner bit à bit le texte clair à une suite binaire de même longueur. Cependant, partager une clef secrète de grande taille n'est pas envisageable dans la plupart des contextes. Une solution consiste à générer de façon déterministe une suite pseudo-aléatoire à partir d'un secret commun court qui lui peut-être partagé facilement.

## III.2 Définition

Du côté du déchiffrement, les bits du texte chiffré sont combinés par ou exclusif avec le
Les algorithmes de chiffrement par flot, appelés aussi algorithmes de chiffrement en continu ou algorithmes de chiffrement de flux, convertissent le texte en clair en texte chiffré 1 bit à la fois en combinant par ou exclusif le flux de bits du texte en clair avec un flux de bits aléatoire.

Même flux aléatoire de bits retrouver les bits du texte en clair.

Ce flux aléatoire de bits peut être:

- Soit une suite aléatoire entièrement secrète partagée par les deux utilisateurs: cette situation correspond à la technique du masque jetable.
- Soit une suite pseudo-aléatoire, c'est-à-dire produite à partir d'une clef secrète par un générateur pseudo-aléatoire.

Contrairement au chiffrement par bloc, un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper [14].

## III.3 Principe du chiffrement par flot :

Les algorithmes de chiffrement par flot peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension relativement petite (1 bit, 1 octet).

Ils appliquent des transformations simples selon un Key Stream donné. Le Key Stream est une séquence de bits utilisée en tant que clef qui peut être générée aléatoirement. Avec un Key Stream choisi aléatoirement et utilisé qu'une seule fois, le message chiffré est excessivement sécurisé.

Les chiffrements par flot sont une approximation des propriétés théoriques de l'algorithme one time pad, appelé aussi chiffrement Vernam [14].( ou masque jetable).

Dans le cas où la génération du Key Stream est dépendante du message clair et du message chiffré le chiffrement par flot est dit asynchrone.

## III.4 Le chiffrement de vernam :

Le chiffrement de Vernam est un algorithme de cryptographie en décalage circulaire.

Bien que simple, facile et rapide, tant pour le codage que pour le décodage, ce chiffrement est le seul qui soit théoriquement impossible à casser. Cependant, il présente d'importantes difficultés de mise en œuvre pratique.

- **Principe**

Le chiffrement par la méthode du masque jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :

- La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.
- Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
- Chaque clef, ou masque, ne doit être utilisée qu'une seule fois.

## III.5 Propriétés générales de chiffrement à flot :

- Avec un algorithme de chiffrement par bloc, on ne peut commencer à chiffrer et à déchiffrer un message que si l'on connaît la totalité d'un bloc. Ceci occasionne naturellement un délai dans la transmission et nécessite également le stockage successif des blocs dans une mémoire tampon. Au contraire, dans les procédés de chiffrement par flot, chaque nouveau bit transmis peut être chiffré ou déchiffré indépendamment des autres, en particulier sans qu'il soit nécessaire d'attendre les bits suivants.
- D'autre part, les chiffrements par flot ne requièrent évidemment pas de padding, c'est-à-dire l'ajout de certains bits au message clair dont le seul objectif est d'atteindre une longueur multiple de la taille de bloc. Ceci peut s'avérer particulièrement souhaitable dans les applications où la bande passante est très limitée ou quand le protocole employé impose la transmission de paquets relativement courts.

## III.6 Avantages et inconvénients de chiffrement à flot :

### 3.6.1 Les Avantages :

- Le processus de déchiffrement ne propage pas les erreurs de transmission (C'est pour cette raison que le chiffrement par flot est également utilisé pour protéger la confidentialité dans les transmissions bruitées).
- Utilisation pour le software : chiffrement très rapide
- Utilisation en hardware avec des ressources restreintes.

### III.6.2 Les inconvénients :

- Sécurité difficile à atteindre.
- Partage préalable d’un secret commun et entre l’émetteur récepteur

## III.7 Chiffrement à flot et générateurs pseudo-aléatoires :

L'algorithme de chiffrement à flot le plus simple est le célèbre chiffre du masque jetable, qui offre une sécurité parfaite mais qui nécessite l'échange au préalable d'une clef secrète aussi longue que le message à chiffrer. Il ne peut donc pas être utilisé en pratique sauf dans des cas extrêmement particuliers où l'on dispose de moyens physiques pour échanger des clefs de grande taille.

Les algorithmes de chiffrement à flot employés en pratique sont donc des versions affaiblies du chiffre du masque jetable dans lesquelles la suite aléatoire secrète est remplacée par une suite produite par un générateur pseudo-aléatoire.

## III.8 Le masque jetable

La technique du masque jetable est un procédé de chiffrement symétrique à flot. Elle consiste à additionner (par un ou exclusif) bit-à-bit le message clair (représenté sous forme d'une suite binaire) à une suite de bits aléatoire de même longueur qui constitue la clef secrète du système. Ce système est inconditionnellement sûr, c'est-à-dire incassable puisqu'il est impossible de retrouver le texte clair à partir du texte chiffré, même pour un adversaire ayant une capacité de calcul infinie. Mais le fait que la clef secrète doive être aussi longue que le texte à transmettre rend son utilisation impossible en pratique.

### III.8.1 Définition :

La technique du masque jetable, appelé aussi chiffre à usage unique et également connu sous son appellation anglo-saxonne "one-time-pad", est un algorithme de chiffrement symétrique à flot.

Ce procédé, inventé par Vernam pour protéger les communications télégraphiques pendant la première guerre mondiale [16], consiste simplement à effectuer un XOR (ou exclusif) bit à bit entre le message clair et une suite de bits aléatoire de même longueur qui constitue la clef secrète du système. Rappelons que l'opération XOR entre deux bits, représentée par le symbole $\oplus$ , est définie par : $0\oplus0=0,0\oplus1=1,1\oplus0=1$, et $1\oplus1=0$ elle correspond à l'addition modulo 2. Le chiffrement du message binaire 10100110 (représentation binaire de la lettre e) avec la clef secrète 01001011 se fait donc de la manière suivante :

| | |
|---|---|
| Message clair | 1 1 1 0 1 1 0 1 |
| | $\oplus\ \oplus\ \oplus\ \oplus\ \oplus\ \oplus\ \oplus\ \oplus$ |
| Clef secrète | 0 1 0 0 1 0 1 1 |
| Message chiffré | 1 0 1 0 0 1 1 0 |

Le déchiffrement est similaire : on retrouve le message d'origine à partir du message chiffré et de la clef par :

| | |
|---|---|
| Message chiffré | 1 1 1 0 1 1 0 1 |

$\oplus \oplus \oplus \oplus \oplus \oplus \oplus \oplus$

Clef secrète 0 1 0 0 1 0 1 1

Message clair 1 0 1 0 0 1 1 0

### III.8.2 Sécurité :

On peut démontrer qu'il est impossible de retrouver le message clair correspondant à un texte chiffré connu même pour un adversaire disposant d'une capacité de calcul et de stockage infinie. En effet, la connaissance du message chiffré n'apporte aucune information sur le message clair : n'importe quel message clair est susceptible de correspondre à un chiffré donné dans la mesure où la clef secrète peut prendre n'importe quelle valeur. Cette propriété, mise en évidence par Claude Shannon [17], est appelée sécurité inconditionnelle. Inversement, Shannon a démontré que tout système inconditionnellement sûr devait nécessairement utiliser une clef secrète aussi longue que le message à chiffrer. Mais cette propriété n'est garantie que si la clef secrète est bien une suite totalement aléatoire aussi longue que le message clair, et qu'elle n'est utilisée que pour transmettre un seul message.

## III.9 Les types de chiffrement à flot :

### III.9.1 Chiffrements synchrones :

Les chiffrements synchrones sont modélisés grâce à :

- un ensemble d'états $\sum$
- une fonction d'initialisation (ou Key/IV setup) de $A^{nk} \times A^{nI}$ dans Σ,
- une fonction de transition δ de Σ dans Σ,
- une fonction d'extraction ω de Σ dans A.
- un ensemble de fonctions inversibles de combinaisons $X_a$ de A dans A paramétrées par a ∈ A.

Grâce au Key/IV setup, on choisit $\sigma_0 \in \Sigma$ l'état initial du chiffrement. Pour chaque nouveau caractère à chiffrer, l'état interne est mis à jour avec δ. Un élément de la suite chiffrante est extrait avec ω. La suite chiffrante est combinée avec le message clair par le biais de X. Pour le déchiffrement, $X^{-1}$ est utilisé. Les fonctions δ, ω et X dépendent du couple (K, IV). On a, comme présenté dans la figure 3.1, pour $i \in N$:

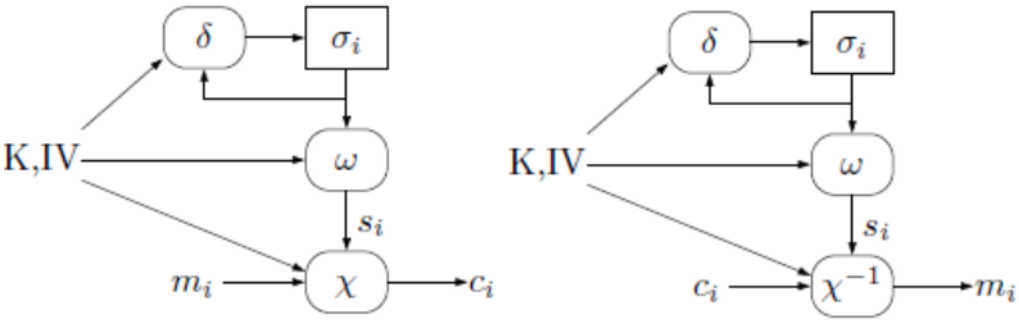
σ_0=key/IV Setup (K/IV) (Initialisation) [III.1]

$\sigma_{i+1}=\delta(\sigma_i)$ (Transition) [III.2]

$S_I=\omega\sigma_i$ (Extraction) [III.3]

$C_i=X_{si}(mi)$ (Chiffrement) [III.4]

$m_i=X_{si}^{-1}(c_i)$ (Déchiffrement) [III.5]




(a) Chiffrement (b) Déchiffrement

**Figure III.1 : Principe des chiffrements à flot synchrones**

Dans le cas d'un chiffrement synchrone additif, l'état interne, la fonction de transition et la fonction d'extraction forment un générateur pseudo-aléatoire (figure 3.2).

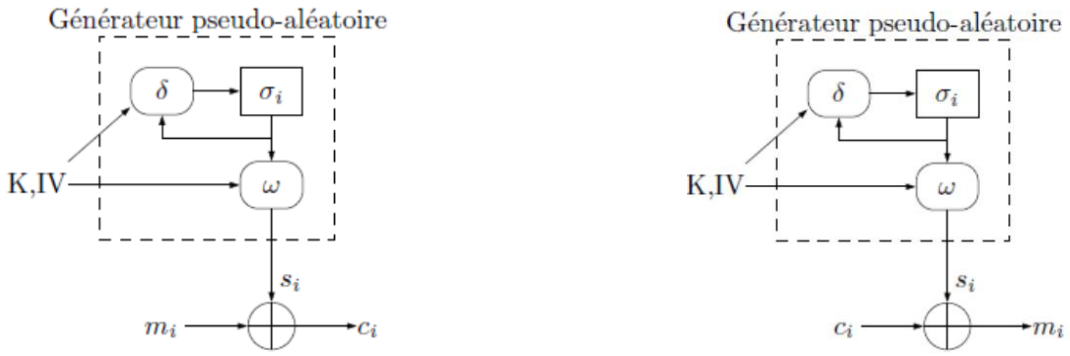



**Figure** (a) Chiffrement (b) Déchiffrement

**III.2 : Principe des chiffrements à flot synchrones additifs**

**III.9.2 Chiffrements auto-synchronisants :**

Les chiffrements auto-synchronisants produisent la suite chiffrante à partir du couple clef/vecteur d'initialisation et d'un nombre fixé d'éléments de la suite chiffrante déjà produits (figure III.3).

Ainsi, même si certains éléments du message chiffré sont perdus, le chiffrement est capable de se resynchroniser après un petit nombre d'itérations. Les chiffrements auto-synchronisant sont :


(a) Chiffrement (b) Déchiffrement

**Figure III.3 : Principe des chiffrements à flot auto-synchronisant**

Cependant très vulnérables aux attaques à clair choisi [18] En pratique, on utilise plutôt des chiffrements synchrones avec un mécanisme de resynchronisation externe

## III.10 Caractéristiques du chiffrement auto-synchronisant :

**Auto-synchronisation :** des caractères sont perdus ou ajoutés dans le texte chiffré, le procédé de déchiffrement se resynchronise au bout de t caractères.

**Propagation d'erreur :** si un caractère du texte chiffré est modifié, le déchiffrement des t caractères suivants est corrompu (aucun pour un procédé synchrone).

**Attaques actives :** la modification d'un caractère se répercutant sur les t caractères suivants, elle a moins de chances de passer inaperçue auprès de Nazim. Par contre l'ajout ou la suppression de caractères seront moins bien détectés que pour les procédés synchrones, ou tout le reste du texte est perdu.

**Diffusion :**

Un caractère mi du texte clair influe via Yi=S (Ri, mi) et $\sigma_{i+1} = Y_{i\_t}, Y_{i_t+1}, \dots, Y_{i\_1}$ sur toute la suite du texte chiffré. Cela rend plus difficiles les attaques basées sur une analyse statistique utilisant les redondances du texte clair.

## III.11 Les types d'attaques par flot :

### III.11.1 Les attaque par correlation:

**Principe:**

Les attaques par corrélation entrent dans la catégorie plus générale des attaques de type divisé pour régner qui s'appliquent à chaque fois que l'on peut décomposer un système en composantes plus petites, crypto graphiquement faibles.

Dans le cas du chiffrement à flot, ces attaques ont été introduites en 1985 par Siegenthaler [19] contre les générateurs par combinaison de LFSRs. Mais, cette cryptanalyse est en fait valide sur tous les générateurs pseudo-aléatoires dont l'état interne est décomposable en plusieurs parties mises à jour indépendamment les unes des autres. On peut alors chercher séparément la valeur initiale de chaque partie de l'état interne.

L'attaque repose sur l'existence d'éventuelles corrélations entre la sortie de la fonction de filtrage et un sous-ensemble de ses entrées qui correspond à la partie incriminée de l'état interne.

**Description:**

Supposons comme à la (figure III .4) que l'on peut séparer l'état interne du générateur à l'instant t en deux parties $\boldsymbol{x_t}$ et $\boldsymbol{y_t}$ de tailles respectives / et (**n-1**), mises à jour indépendamment par $\emptyset_0$ et $\emptyset_1$.

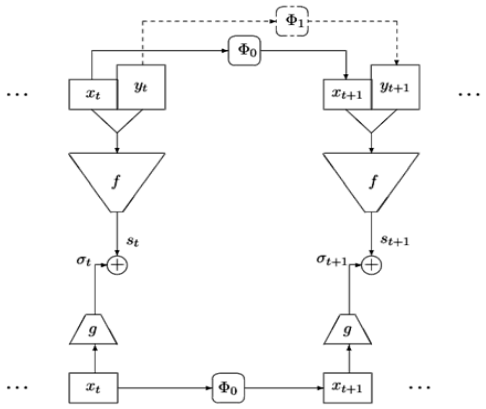



**Figure III.4: Modèle de l'attaque par corrélation**

Plaçons-nous dans le cas où l'attaquant cherche à retrouver la valeur de la première partie de l'état initial, $\boldsymbol{x_0}$. Le vecteur d'entrée de la fonction de filtrage $\boldsymbol{f}$ se décompose de la même manière en deux parties, **x** et **y**. On peut alors appliquer l'attaque s'il existe une fonction **g** à / variables (c'est-à-dire ne dépendant que de x) qui coïncide avec la sortie de f dans plus de la moitié des cas, autrement dit si la probabilité :

$$P_{g=p_{r\,x,y}}[f(X,Y) = g(x)] < \frac{1}{2}$$

La suite $\boldsymbol{\sigma x_0}$produite par le générateur réduit d'état initial $\boldsymbol{x_0}$ et de fonction de filtrage **g** est alors corrélée à la suite chiffrante **s** car, pour tout $\mathbf{t \geq 0}$ :

$$\boldsymbol{P_r[s_{t=\sigma_t}] = P_g > \frac{1}{2}}$$

## 3.11.2 Les attaques par corrélations rapides:

Les attaques par corrélation rapides sont des améliorations des attaques par corrélation classiques, telles que définies par Siegenthaler, dans le cas où il existe une approximation de la suite chiffrante par un générateur pseudo-aléatoire dont la sortie dépend linéairement de l'état initial. Puisque les algorithmes utilisés dans ce cas ne nécessitent plus d'effectuer une recherche exhaustive sur l'état initial, ces attaques s'appliquent même lorsque l'état interne du générateur

pseudo-aléatoire n'est pas décomposable en plusieurs parties indépendantes, contrairement à l'attaque par corrélation originale.

Les algorithmes par corrélation rapides sont particulièrement appropriés pour attaquer les générateurs pseudo-aléatoires dont la fonction de transition est linéaire, notamment les générateurs utilisant des LFSR.

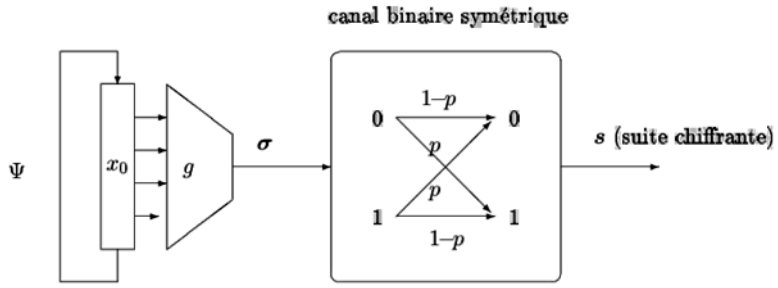



**Figure III.5: Modèle de l'attaque par corrélation rapide**

## 3.11.3 Les attaques algébriques:

Les attaques algébriques sont des attaques à clair connu qui exploitent des relations algébriques entre les bits du clair, ceux du chiffré et ceux de la clef secrète. La connaissance de plusieurs couples clairs-chiffrés fournit donc un système d'équations dont les inconnues sont les bits de la clef secrète.

Ces derniers peuvent alors être retrouvés en résolvant le système, ce qui est possible s'il est de degré faible, de petite taille ou qu'il possède une structure particulière.

## III.11.3.1 Attaques algébriques rapides:

Il existe une variante plus générale et souvent plus efficace des attaques algébriques contre les chiffrements à flot, introduite par Courtois **[20]** sous le nom d'attaque algébrique rapide. Une première amélioration de l'attaque précédente, permettant de diminuer le degré du système d'équations à résoudre, consiste à rechercher des équations de petit degré en les bits de l'état initial, qui font intervenir plusieurs bits consécutifs de suite chiffrante. La recherche de ces équations est souvent un problème complexe, dont la complexité augmente considérablement quand le nombre de bits de suite chiffrante intervenant simultanément dans les équations augmente. On peut alors être amené à ne considérer que des relations ayant une forme particulière, obtenues en additionnant plusieurs relations connues de manière à faire baisser le degré **[21].**

### III.11.3.2 Attaques algébriques évoluées sur les chiffrements à flot :

En **2003,** Courtois et Meier **[22]** ont proposé une amélioration de l'attaque précédente, qui peut parfois aboutir même lorsque le degré de la fonction de filtrage $\boldsymbol{f}$ est élevé. L'attaque fonctionne dès lors qu'il existe des relations de petit degré entre la sortie de la fonction et ses entrées **[23]**.

Plus précisément, l'attaquant recherche des fonctions $\boldsymbol{g}$ et $\boldsymbol{h}$ de petit degré qui vérifient

Pour tous $\boldsymbol{(x_{1,\ldots}x_n), g(x_{1,\ldots}x_n)f(x_{1,\ldots,}x_1) = 0.}$

**Ou pour tous** $\boldsymbol{(x_{0,\ldots\ldots,}x_n)h(x_{1,\ldots,}x_n[1 + f(x_{1,\ldots,}x_n)] = 0.}$

Si de telles fonctions $\boldsymbol{g}$ ou $\boldsymbol{h}$ de degré $\boldsymbol{d}$ existent, on peut engendrer un système d'équations de degré d de la manière suivante :

- Si$s_t = 1, on\ a\ g(z_{t,\ldots\ldots,}z_{(t+n-1)})) = 0\ ou\ (z_t, \ldots, z_{(t+n-1)})$ est l'état du registre à l'instant **t**.
- Si$\boldsymbol{s_t = 0\ on\ a\ h(z_t, \ldots, z_{(t+n-1)}) = 0.}$

En exprimant l'état du registre à l'instant t comme une fonction linéaire de l'état initial, on obtient comme précédemment un système d'équations de degré d en n variables (les bits de l'état initial), que l'on peut résoudre par les techniques évoquées plus haut.

## III.12 Conclusion

Le chiffrement à flot est l'un des deux technique de chiffrement à clé secrète. Ce genre de chiffrement se présenté sous la forme générateur pseudo aléatoire, et Son principe repose sur la combinaison généralement l'addition bit à bit, il contient deux types de chiffrement (synchrone et asynchrone), chacun appartient de ces caractéristique et ces propriétés, en plus il a beaucoup d'avantage par rapport à l'inconvénient, donc il est très apprécié pour leur efficacité.

Dans le chapitre qui suit nous avons étudié le générateur pseudo aléatoire dans le chiffrement à flot.

# Chapitre IV :

# Les Générateurs pseudo-aléatoire

## IV.1 Introduction :

Un générateur pseudo-aléatoire est un procédé qui, à partir d'une initialisation de taille fixée (généralement d'une ou quelques centaines de bits) appelée graine ou germe, engendre de manière déterministe une suite de très grande longueur que l'on ne peut pas distinguer d'une suite aléatoire quand on ne connaît pas la graine.

Un exemple de générateur pseudo-aléatoire est la fonction rand () ou random () que l'on trouve dans la plupart des langages des programmation : dans un programme, n appels consécutifs à rand() fournissent une suite de n nombres aléatoires, mais plusieurs exécutions du programme produisent toujours la même suite si l'on n'a pas modifié la graine du générateur (à l'aide d'une fonction d'initialisation appelée généralement srand() ou srandom()).

La notion de générateur pseudo-aléatoire doit être distinguée de celle de générateur aléatoire, qui désigne également un procédé engendrant une suite semblable à une suite aléatoire, mais de façon non déterministe, ce qui signifie que, contrairement au cas précédent, la génération de la suite n'est pas reproductible. On trouve par exemple parmi les générateurs aléatoires des techniques qui produisent une suite aléatoire (par exemple une clef) à partir des dates (mesurées en fractions de seconde) de divers événements ayant lieu sur une machine : clavier, souris, accès réseau... Ces événements ont en effet lieu à des dates qui ne sont pas toutes prévisibles avec une telle précision. Il est clair dans ce cas que la suite obtenue ne peut pas être reproduite, même par la même personne.

## IV.2 Les générateurs pseudo-aléatoires pour le chiffrement à flot :

Dans un algorithme à flot, le chiffrement consiste à additionner (par ou exclusif bit à bit) le texte clair à la sortie d'un générateur pseudo-aléatoire initialisé par la clef secrète. Le destinataire du chiffré effectue la même opération : il engendre à partir de la clef secrète la même suite pseudo-aléatoire, l'additionne au texte chiffré et retrouve ainsi le message clair.

On voit ici que le déchiffrement impose clairement le fait que la suite pseudo-aléatoire soit reproductible par toute personne connaissant la clef secrète.

Dans la plupart des applications, on utilise des générateurs pseudo-aléatoires dont l'initialisation est calculée à partir de deux données : la clef secrète et une quantité publique, usuellement appelée valeur initiale. En effet, les protocoles de communication transmettent généralement les

messages sous forme de paquets de taille fixée ; la valeur initiale correspond donc souvent au numéro de paquet, la clef secrète restant inchangée au cours d'une même communication.

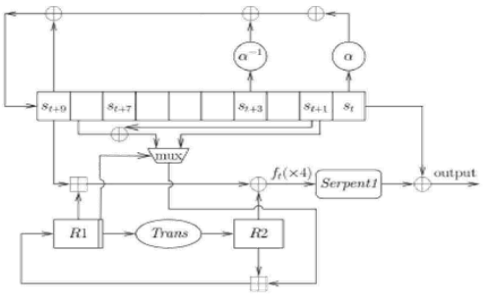
## IV.3 Sécurité des générateurs pseudo-aléatoires :

La sécurité des algorithmes de chiffrement à flot repose entièrement sur les propriétés du générateur pseudo-aléatoire utilisé. En effet, si l'on suppose que l'adversaire dispose de divers messages chiffrés ainsi que des textes clairs correspondants (qu'il a devinés par exemple en utilisant le fait que les messages envoyés suivent un format particulier), un simple XOR entre ces couples clairs-chiffrés fournit alors les valeurs de certains bits produits par le générateur. Dans ce contexte, il doit par exemple être impossible en pratique quand on connaît certains bits produits par le générateur de prédire la valeur des bits suivants. Autrement dit, cette propriété est celle que l'on exigerait si un tel procédé était utilisé pour tirer les numéros gagnants au Loto : une personne qui analyse tous les tirages du Loto doit être dans l'impossibilité matérielle d'en déduire une quelconque information sur les tirages à venir.

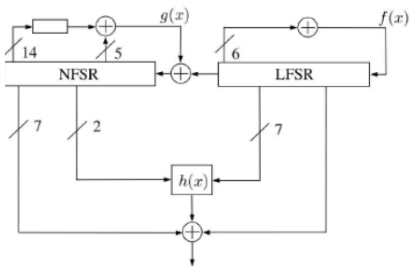
Plus précisément, pour être utilisé dans un chiffrement à flot, un générateur pseudo-aléatoire doit produire des suites que l'on ne peut pas distinguer facilement d'une suite aléatoire même si l'on connaît toutes les caractéristiques du générateur utilisé à l'exception de la clef secrète.

## 4.5 Générateurs basés sur des LFSRs :

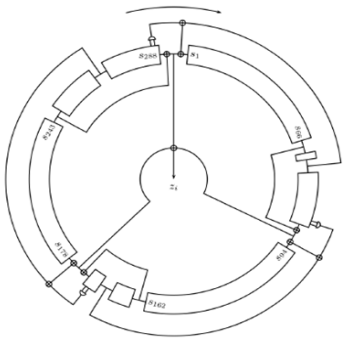
En pratique, pour du chiffrement à flot où le débit doit être important, on utilise des générateurs pseudo-aléatoires qui ne sont pas prouvés sûrs, mais qui ont été soumis à la communauté cryptographique et ont résisté aux attaques. Différents exemples de chiffrements à flot sont présentés dans la figure IV.1 :




a Sosemanuk




b Grain



(C) Trivium

**Figure IV.1 : Trois finalistes de eSTEEAM**

L'un des éléments communément utilisé pour construire de tels générateurs est le registre à décalage linéaire (Linear Feedback Shift Registrer ou LSFR). Il est constitué de mémoire et a une fonction de transition linéaire. Dans le cas binaire, il ne nécessite que des portes OU exclusif pour être implémenté (**figure IV.2**). Il produit des suites avec une large période et de bonnes propriétés statistiques.

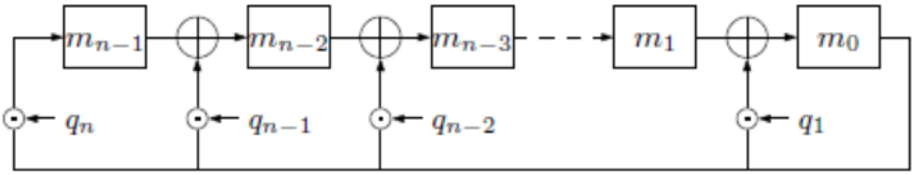


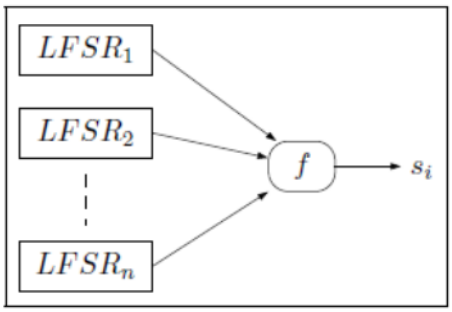

**Figure IV.2 : Exemple de LFSR binaire**

Cependant, les LFSRs ne peuvent pas être utilisés seuls, car l'algorithme de Berlekamp-Massey [25] permet de retrouver l'état d'un LFSR composé de n mémoires et sa fonction de transition à partir de 2n éléments consécutifs de la suite. Trois constructions classiques existent pour casser la structure linéaire (**figure IV.3**) :

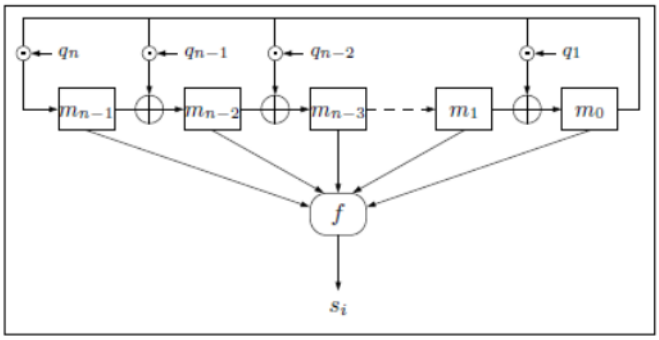
**Les générateurs à combinaison non-linéaire :** Ces générateurs sont composés de plusieurs LFSRs en parallèle, et d'une fonction de combinaison f non-linéaire. La fonction f doit vérifier différentes propriétés comme avoir un haut degré, être équilibrée, etc.

**Les générateurs à filtre non-linéaire :** Ces générateurs appliquent une fonction non-linéaire f à l'ensemble de l'état d'un LFSR. Comme pour les générateurs à combinaison linéaire, la fonction f doit avoir un haut degré, être équilibrée, etc.

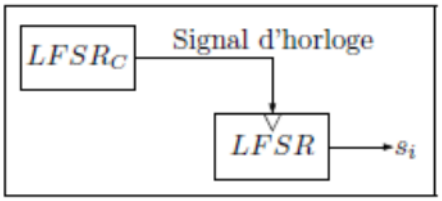
**Les générateurs à horloge contrôlée :** Ces générateurs utilisent au moins deux LFSRs. LFSRC est un LFSR binaire classique qui contrôle la façon dont le second est clocké, i.e. en fonction du bit produit par LFSRC, le second LFSR met à jour son état ou pas.




(a) Générateurs à combinaison non linéaire




(b) Générateur à filtre non linéaire




(c) Générateurs à horloge contrôlée

**Figure IV.3 : Trois constructions classiques basées sur des LFSRs**

Les générateurs à combinaison non-linéaire et à filtre non-linéaire sont les plus courants. Dans ces deux cas, la fonction f est souvent coûteuse à implémenter, car elle nécessite de nombreuses portes logiques et une grande profondeur de circuit. De plus, ces générateurs ne sont maintenant plus utilisés, car les attaques algébriques, par corrélation, par corrélation rapide et par compromis temps-mémoire permettent de les casser.

**IV.5 Générateur de Blum-Blum-Shub (BBS) :**

Actuellement, le générateur le plus simple et le plus efficace est appelé le générateur **Blum Blum Shub** d'après les noms de ses inventeurs. Nous utilisons l'abréviation **BBS**. Il s'appelle aussi « générateur à résidu quadratique ». Ce générateur illustré dans la (figure 1) fonctionne ainsi.

Trouvez deux nombres premiers p et q qui soient congrus à 3 modulo 4. Le produit de ces nombres $n=p*q$ est un entier de **Blum**. Choisissez un autre entier aléatoire *S* qui soit premier par rapport à *n* Calculez :

$s_0 = s^2 \bmod n$ C'est le **semence** du générateur

Les nombres de ce générateur donné par la relation suivante :

$s_i = s_{i\_l}^2 \ mod\ n$

Et le $i^{éme}$ bit pseudo-aléatoire de **BBS** est le bit le moins significatif de $s_i$ où

$z_i = s_i \ mod\ 2$

Le générateur de **Blum-Blum-Shub** est présenté sur la (figure 1). Son fonctionnement est simple. Etant donné une semence $s_0 \epsilon QR(n)$ (ensemble des résidus quadratiques modulo *n*), on calcule la suite $s_1, s_2, \ldots s_l$ par élévations au carré successive *S* modulo n , et l'on réduit les $s_i$ modulo *2* pour obtenir les $z_{i,}$ on a donc :

$z_i = (s_0^{2i} \mod n) \bmod 2, \qquad 1 \leq i \leq 1$

Algorithme de générateur Blum- Blum-Shub

Soit $p$ et $q$ deux nombres premiers de $k/2$ bits tels que

$P = q = 3(mod4)$, et soit $n = pq$, $QR(n)$ représente l'ensemble des résidus

Quadratiques modulo $n$.

Une semence $S_0$ est un élément de $QR(n)$. Pour $i \geq 0$, on

Définit :

$$S_{i+1} = S_i^2 mod\ n$$

Puis :

$$f(S_{0)} = (z_1, z_2, \dots, z_l)$$

Où :

$$Z_i = S_i mod\ 2$$

**Figure IV.4 : générateur BBS**

**Remarque :**

On remarque que, nous pouvons calculer le bit de générateur BBS. Sans calculer les $(i-1)^{éme}$ bits précédent, qu'on utilise la formule :

$$z_i = s_0^{2i} \mod 2$$

On peut utiliser le générateur **BBS** comme un crypto système de chiffrement en continu pour des fichiers à accès aléatoire.

## IV.6 Sécurité du générateur BBS :

La sécurité de ce générateur dépend de la difficulté de factoriser n. Vous pouvez rendre n public.

Le générateur **BBS** est imprévisible à gauche et imprévisible à droite. Cela signifie que, étant donné une suite engendrée par le générateur, les cryptanalyses ne peuvent pas prédire le bit suivant ou le bit précédent de la suite. Ce qui n'est pas de la sécurité basée sur un générateur de bits compliqué que personne ne comprend, mais bien sur les mathématiques sous-jacentes à la factorisation de n. Pour ceux qui veulent des suites pseudo-aléatoires de bits crypto graphiquement sûres, c'est le meilleur choix.

### IV.8 Conclusion :

Le générateur BBS est relativement lent et n'est pas utilisé pour le chiffrement en continu. Toute fois, pour des applications de haute sécurité, telles que la génération de clés. Ce générateur est le meilleur. Comme nous allons le voir dans le chapitre suivant qui concerne le chiffrement sélectif en utilisant le générateur BBS.

# Chapitre V :

# Chiffrement sélectif en utilisant le générateur BBS

## V.1. Introduction :

Le trafic de données numériques a augmenté rapidement dans les larges réseaux. La protection de données numériques et particulièrement les images médicales, devient importante pour beaucoup de raisons comme la confidentialité et la sécurité. De nos jours, le moteur le plus important pour fournir la confidentialité est le cryptage. Donc, les systèmes classiques et modernes ne sont pas appropriés pour une telle quantité énorme de données en temps réel. Le chiffrement sélectif est une approche à crypter une partie des données pour réduire des exigences informatiques et fournir une vie privée proportionnel. Ce chapitre présent une nouvelle méthode de cryptage sélectif des images médicales basé sur le générateur pseudo aléatoire BBS. La méthode proposée aboutit à une réduction significative du temps de traitement pour l'opération de cryptage et décryptage.

## V.2. Description de la méthode :

Dans ce travaille une méthode simple basée sur le générateur pseudo aléatoire BBS pour le cryptage et décryptage d'image est proposée. Figure 5.1 montre le bloc diagramme de la méthode proposée. Par $x_i$ on désigne la suite chiffrante. Par $c_{(i)=}E_k(m_i) = xor(m(i); x(i))$ et $m_i = D_k(C_i) = xor(C(i); x(i))$ on note respectivement le processus de chiffrement de flux binaire original $m_i$ avec la clé secrète *k* à chaque instant *i* et le processus de déchiffrement de flux binaire crypté $C_i$ avec la clé secrète $k$ à chaque instant $R_j(n_i)$ une région sélectionné de taille $n_j$ .

Le processus de chiffrement et de déchiffrement fonctionne comme suit : $R_1(n_1), R_2(n_2), \dots R_j(n_j)$.

Soit : $R_1(n_1), R_2(n_2), \dots R_j n_j$ les régions sélectionnées pour le chiffrement, mettre les données des régions dans un vecteur *A* de taille $L = n_{1+}n_{2+\dots+}n_j$ pixels.

Convertir les données du vecteur A en flux binaire, ensuite crypter le flux binaire en utilisant la relation :

$$C(i) = E_k(m_i) = xor\ (m(i), x(i)),$$

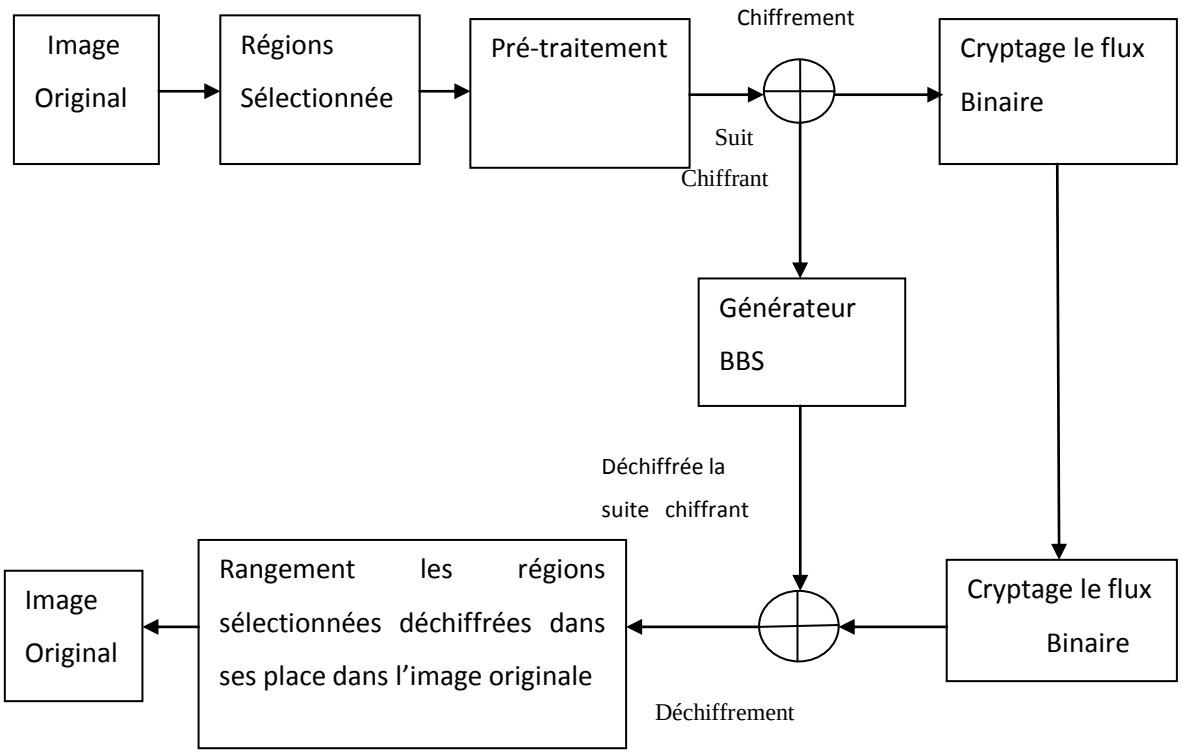
*pour* $i \geq 0$. La **figure V.2** montre l'organigramme de chiffrement.

Le flux binaire chiffré c (i) est envoyé au récepteur à travers un canal non sécurisé. Le

récepteur déchiffre le flux binaire chiffré c (i) en utilisant la relation :

$$m(i) = D_k(C_i) = xor\ (C(i), x(i))$$

La **figure V.3** montre l'organigramme de déchiffrement.




**FigureV.1: Bloc diagramme de l'approche proposée**

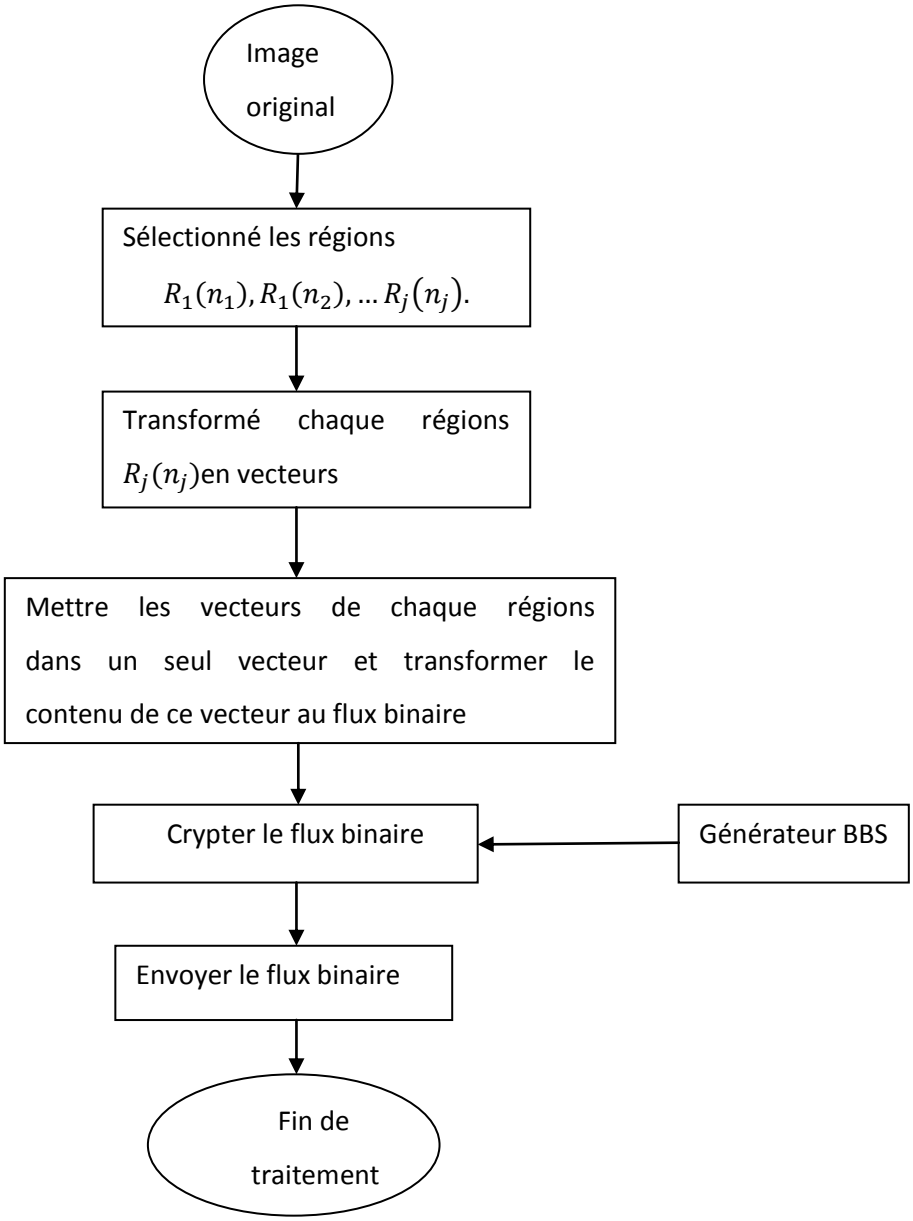
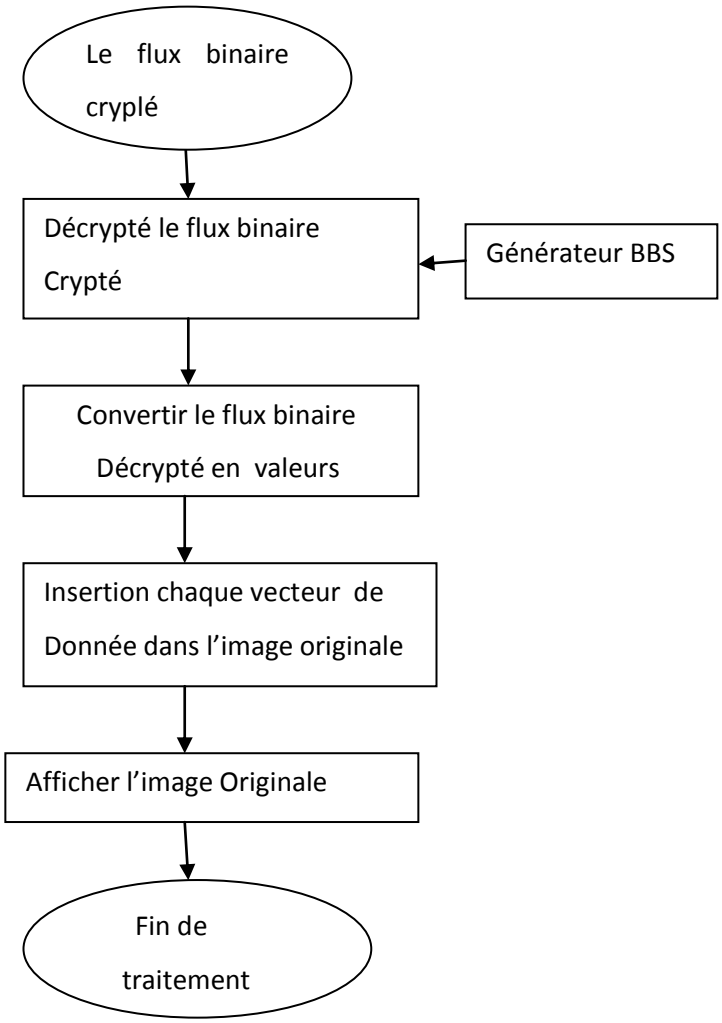



**Figure V.2 : Organigramme de Chiffrement**




**FigureV.3 : Organigramme de Déchiffrement**

## V.3. Algorithme de chiffrement et déchiffrement d'image :

### V.3.1 : Chiffrement

1. Lire l'image originale ;
2. Sélectionné les régions $R_1(n_1), R_2(n_2), \dots R_j(n_j)$ ;
3. Transformé chaque régions $R_j(n_j)$ en vecteurs de données $v_i$ ;
4. Mettre les données de $v_i$ dans un seul vecteur $A$ ;
5. Transformer les donnée de $A$ en valeurs binaires et les stokers dans fichier $m$ ;
6. M la taille de $m$ ;
7. Générer la suite pseudo aléatoire $x_i$ en utilisant l'algorithme 5.4.3 ;

8. Pour $i$ =1 à M faire

9. Crypter le flux binaire $m$ en utilisant la relation : $C_{(i)} = E_k(m_i) = xor\big(m(i), x(i)\big)$;

10.Fin faire ;

11. Envoyer le flux binaire crypté c ;

**V.3.2 : Déchiffrement**

1. lire le flux binaire crypté c ;

2. $M$ ⟵ la taille de c ;

3. Générer la suite pseudo aléatoire $x_i$ comme l'algorithme 5.4.3 ;

4. Pour i=1 à $M$ faire ;

5. Décrypté le flux binaire crypté en utilisant la relation :$m(i) = D_k(C_i) = xor(C(i), x(i))$;

6. Fin faire ;

7. Transformer le flux $m$ en valeurs décimaux et les stokers dans $A$;

8. Mettre chaque bloc de $A$ de taille $n_j$ dans leur place dans l'image originale ;

9. Afficher l'image originale ;

**V.4.3 : Algorithme de calcul la suite chiffrante engendrée par le générateur BBS** :

Générer la suite chiffrante $x_1, x_2 \ldots, x_M$ de taille $M$

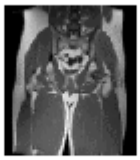
1. lire $M$ la taille de m ;
2. sélectionner deux nombres aléatoires premiers p et q , et calculer n= p*q
3. sélectionner un entier 0< $S < n$ .
4. Calculez $S_O = S^2 \ mod \ n$ C'est le semence du générateur
5. Pour $i$=1à $M$ faire :
6. $S_i = S_{i-1}^2 \ mod \ n$
7. $x_i = S_i mod \ 2$
8. fin faire

**V.5. Simulation et résultat :**

La simulation a été porté de l'utilisation MATLAB7.8 .Une image est crypté par la méthode proposé et le texte visuel est exécuté. On montre un exemple dans la figure5.4.Dans ce travaille p=7603, q=7487,s=7817. on utilisé respectivement pour calculer n=p*q=56923661.$s_0$ Représente la clé secrète.

## V.6. Test visuel :

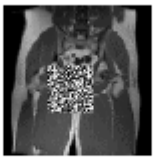
### V.6.1 Test 1 : une seule région



a : L'image original

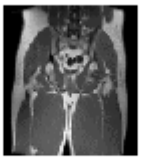
b : la région sélectionnée

c : la région chiffrée



d : insertion la région chiffrée dans l'image

e: la région déchiffrée



f : insertion la région déchiffrée dans l'image origénal

**Figure V.4 :** test 1 pelvis.gif

## V.6.2 :Teste2: Deux régions :

a 1 : image original

b 1,b 2 : les région sélectionnées

c 1

e1

c 2

c 1 ;c 2 : les régions chiffrées

d 2

d 1,d 2 : insertion les régions chiffrées dans l'image originale

e 2

e 1,e 2 :les régions déchiffrées

f 2

f1, f2 : insertion les régions déchiffrées dans l'image originale

**Teste3: Plusieurs régions**

b 1

b 2

b 3

b1 ,b2 ,b3 : les région sélectionnées

c 1

d 1

c 2

d 2

c 3

d 3

c 1,c 2,c 3 :les régions chiffrées

d 1, d 2, d 3 : insertion les régions chiffrées dans l'image original

e 1

f 1

e 2

f 2

e 3

f 3

e 1,e 2, e3 :les régions déchiffrées

f 1, f 2, f 3 : insertion les régions déchiffrées dans l'image original

**FigureV.4 :** test 3 cameramen. tif

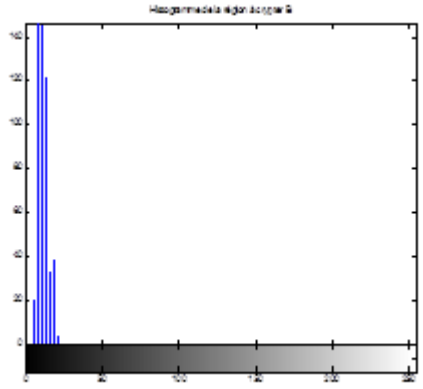
## V.7. Analyse de la sécurité :

Dans ce chapitre, la performance du crypto système d'image proposée et analysée en détaille nous discutons de l'analyse de sécurité de cryptage d'image proposée en introduisant quelques analyses importantes comme la sensibilité statistique, l'analyse de la sensibilité de clé.

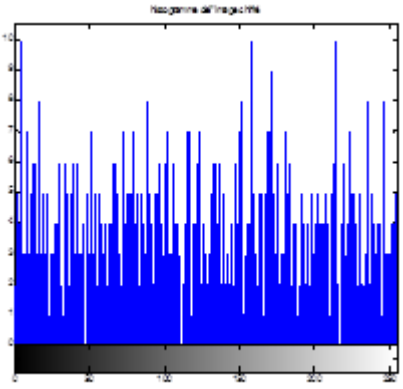
### V.7.1. Analyse de l'histogramme :

Les régions originales et leurs régions chiffrées correspondant sont illustrées dans les **figures V.4**, leurs histogrammes sont présentés dans la figure 5.6. Il est clair que l'histogramme de la région chiffrée est presque uniformément distribué, et différent de l'histogramme de la région originale. Donc, la région chiffrée ne fournit aucun indice qui permette de faciliter l'utilisation d'une attaque statistique sur le crypto système proposé, ce qui rend les attaques statistiques difficile.

Ces propriétés indiquent que le crypto système d'image proposé présente une haute sécurité contre les attaques statistiques. Dans la région originale, quelques valeurs de niveau de gris dans l'intervalle [0 ,225] n'existent pas, mais des valeurs de niveau de gris dans l'intervalle [0,225] existe et sont uniformément distribuées dans la région chiffrée. Différentes images ont été examinées par le procédé de chiffrement proposé.



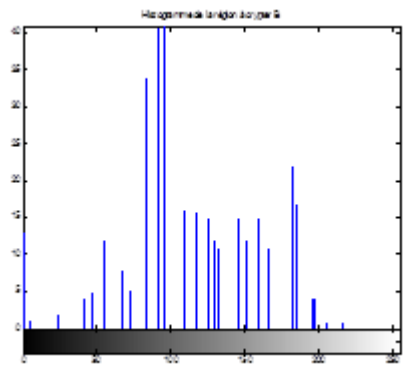
a. l'histogramme de la région sélectionnée



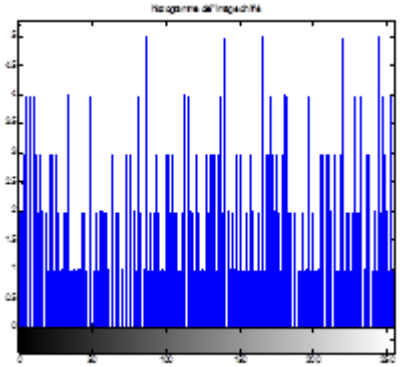
b.l'histogramme de la région chiffrée

**figureV.7 :** les histogrammes de test 1

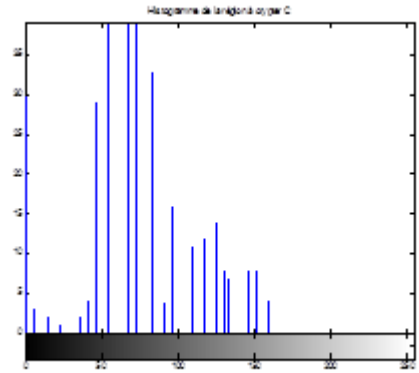
## Test 2



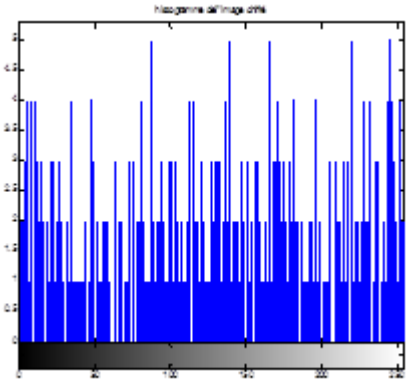
c.l'histogramme de la$1^{ére}$ région sélectionnée



d.l'histogramme de la$1^{ére}$ région chiffrée



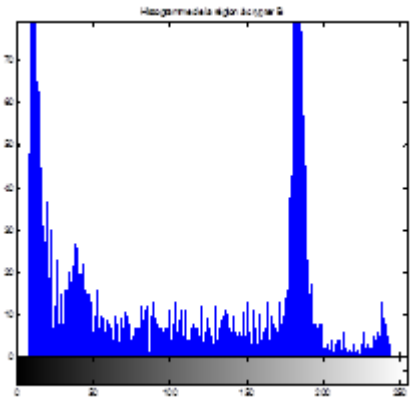
e .l'histogramme de la $2^{éme}$région sélectionnée



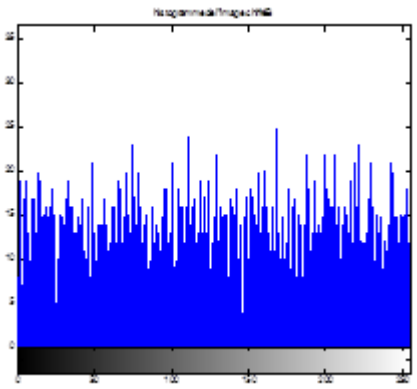
f. l'histogramme de la $2^{éme}$ région chiffrée

**Figure V.8 :** les histogrammes de test 2

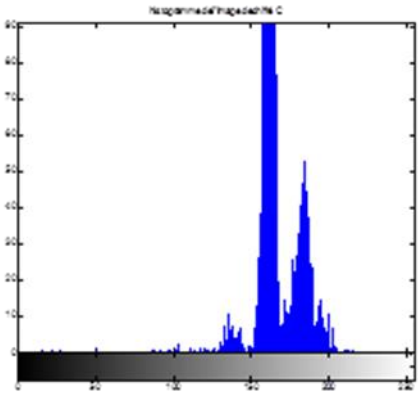
**Test 3**



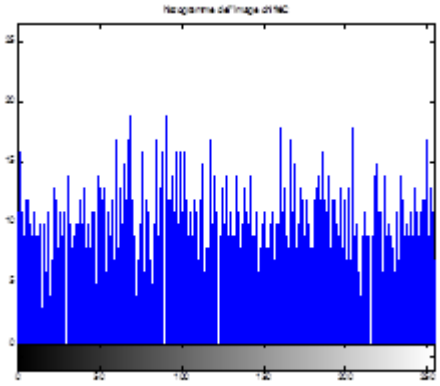
g.L'histogramme de la $1^{ére}$ région sélectionnée



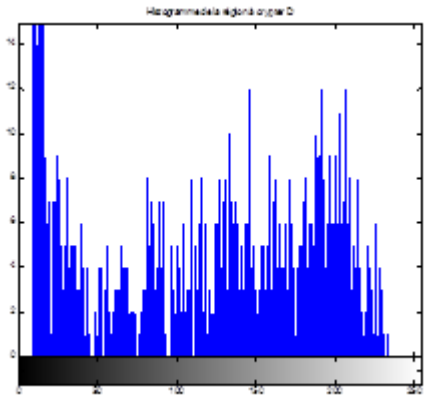
h.L'histogramme de la $1^{ére}$ région chiffrée



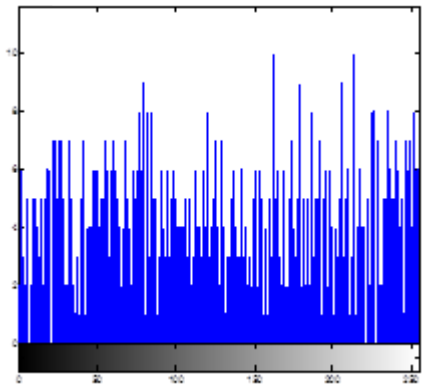
i.L'histogramme de la $2^{éme}$ région sélectionnée



j.L'histogramme de la $2^{éme}$ région chiffrée



k.L'histogramme de la $3^{éme}$ région sélectionnée



i.L'histogramme de la $3^{éme}$ région chiffrée

**FigureV.9 :**les histogramme de test 3

### V.7.2. Analyse de coefficient de corrélation :

Le coefficient de corrélation simple est un indice de mesure de l'intensité d'un lien qui peut exister entre deux variables. Le coefficient de corrélation peut prendre une valeur comprise entre -1 et +1. Si les deus variables sont la région originale et son région chiffrée alors sont en corrélation si et seulement si le coefficient de corrélation est égale à 1. Dans ce cas la région chiffrée et la région originale sont identiques et la procédure de chiffrement a échoué en cachant les détails de la région originale. Si le coefficient de corrélation est égale à zéro, alors la région originale et sa région chiffrée sont totalement différentes c.à.d. que la région chiffrée est fortement indépendante de la région originale. Si le coefficient de corrélation est égal a -1, alors la région chiffrée est un négatif de la région originale.

Le tableau V.1 donne le coefficient de corrélation entre les régions originales et leurs régions chiffrées représentées dans le test 1, test 2 et test 3. On observe que le coefficient de corrélation est une petite corrélation entre la région originale et la région chiffrée.

| | **Coefficient de corrélation** | |
|---|---|---|
| | **Coor 1** | **Corr 2** |
| Test 1 | 0,0048 | 1 |
| Test 2 | 0,0159 | 1 |
| Test 3 | 0,01292 | 1 |
| | ),0117 | 1 |
| | -0,0159 | 1 |
| | _0,0670 | 1 |

**TableauV.1 :** Analyse du Coefficient Corrélation.

**Corr1**=différence entre la région originale et la région chiffrée.

**Corr2**= différence entre la région originale et la région déchiffrée.

## V.7.3. Analyse de l'entropie :

Le tableau (V.2) , (V.3) donne les résultats de l'entropie des régions originales, les régions chiffrées et les régions déchiffrées. Les valeurs de l'entropie des régions chiffrées obtenus sont très proches de la valeur théorique de 8 .Cela signifie que la fuite de l'information dans la procédure de chiffrement est négligeable ce qui rend l'attaque statistiques moins efficace.

| | Entropie | |
|---|---|---|
| | E1 | E2 |
| Test | 3,7172 | 7,7837 |

**TableauV.2: Analyse de l'entropie de test 1**.

E1 : l'entropie de la région sélectionnée.

E2 : l'entropie de la région chiffrée

| | Entropie | | | |
|---|---|---|---|---|
| | E1 | E2 | E3 | E4 |
| Test 2 | 3,7438 | 7,4959 | 3,4875 | 7,5760 |

**Tableau V.3 :** analyse de l'entropie de test 2

E1 :l'entropie de la $1^{ére}$ région sélectionnée.

E2 : l'entropie de la $1^{ére}$ région chiffrée

E3 : l'entropie de la $2^{éme}$ région sélectionnée.

E4 : l'entropie de la $2^{éme}$ région chiffrée

| | Entropie | | | | | |
|---|---|---|---|---|---|---|
| | E1 | E2 | E3 | E4 | E5 | E6 |
| Test 3 | 6,7582 | 7,9517 | 5,0324 | 7,9301 | 7,3822 | 7,8074 |

**Figure V.4 : Analyse de l'entropie de test 3**

E1 : l'entropie de $1^{ére}$ la région sélectionnée.

E2 : l'entropie de la$1^{ére}$ région chiffrée

E3 : l'entropie de la$2^{éme}$ région sélectionnée.

E4 : l'entropie de la$2^{éme}$ région chiffrée

E5 : l'entropie de la$3^{éme}$ région sélectionnée.

E6 : l'entropie de la $3^{éme}$ région chiffrée

## V.8. Conclusion :

Dans ce chapitre, une méthode de cryptage d'image sn utilisant un algorithme de chiffrement basé sur le générateur pseudo aléatoire BBS. Les simulations ont été portées de deux messages différents. Le teste indique que le message crypté était très différent que le message originale. Cette méthode est très simple, pour mettre en œuvre le chiffrement et déchiffrement de message.

Ici les aspects de sécurité comme l'analyse d'histogramme, l'analyse d'entropie et l'analyse de coefficient de corrélation sont discutés avec des exemples.

[1] A Menezes, P. Van Oorchost, S Vanstone “Handbook of Applied Cryptography”; CRC press 1996.

[2] Nada REBHI, Mohamed Amine BEN FARAH, Abdennadeur KACHOURRI & Mounir SAMET, Analyse de sécurité d’une Nouvelle Méthode de cryptage Chaotique Laboratoire d’Electronique et des Technologie de L’information (LETI) Ecole Nationale d’Ingénieure de Sfax B.P.W. Sfax ,Tunisie.

[3] A. Kirchhoff ; ’’La cryptographie militaire ’’ ; Joural des sciences militaires, IX ;1883 .

[4]C.E. Shannon; ‘Communication theory of secrecy systems’’; Bell System Technique journal volume 28 n°10 pages 656-715; October 1949.

[5] Herve Schauer, Introduction à la cryptographie Herve Schauer Consultants Support de cours du cabinet consultant 1999/2001.

[6] : mémoire de fin d’étude d’ingénieur d’état en électronique titre : Cryptanalyse d’un système de la parole. Encadre par : Dr kahil Djamel-promotion : 2008 / 2012.

[7] Mémoire de fin d’étude Master 2 électronique biomédicale titre : Cryptage des images médicales encadrer par : Mr. BELMEGUENAI AISSA. 2011/2012.

[8] Mémoire de fin d’étude D’ingénieur d’état en électronique segmentation des images couleur par des techniques statistiques. Encadrer par: Dr. GROUCH-Promotion: 2008 / 2009.

[9] Habutsu, T. Nishio; Y Sasase, I, ‘A secret cryptosystem bay iterating a chotic map’,In: Advantage in cryptography EUROCRYPT’91, Berlin, springer-verlag,1991,pp.127-140.

[10] M .A. Bani Younes and A Jantan, ‘image encryption using block-based transformation algorithm, ‘IANG International journal of computer science, 35:1,IJcs_35_1_03,fev 2008.

[11] M. Podesser, H-P Schmidt, A Uhl;’’ Selective biplane encryption for secure transmission of image data in mobibe environments’’; CD-ROM in: Proceedings of the Fifth IEEE Nordic Signal Processing Symposium (NORSIG 2002); Tromso-Trondheim. Norway; Oct. 2002.

[12] T. Lookbaugh;”Signals, Systems and Computers”, Conference Record of the Thirty Eighth Asilowar Conference; pp. 373-376 vol 1; Nov.2004.

[13] R. Norcen, M. Podesser, A Pommer, H-P. Schmidt, A. Uhl ; ’’Confidential storage and transmission of modical image data’’ ; Computers in Biology and Medicine 33 ; 2003 ;pp.277-292.

[14] http/www.picsi.org/parcours_48_235.html (2014).

[15] G.S Vernam:’’Secret signaling system’’, 1919.US Patent1, 310 ,719.

[16] G.S Vernam. ‹‹Cipher printing telegraph systems for secret wire and radio telegraph communications››.Jornal of the American Institute for Electrical Engineers,(55),1926.

[17] C.E Shannon. ‹‹A mathematical theory of communication›› *Bell Syst. Tech J., 27,*

*1948.*

[18] A. Joux et F. Muller: Chosen-ciphertext attacks against Mosquito. In Fast Software Encryption, pages 390_404.Springer, 2006.

[19] T. Siegenthaler. ‹‹Decrypting a class of stream ciphers using ciphertext only ››.IEEE Trans. Computers, C-34(1):81-84,1985.

[20] N. Courtois. ‹‹fast algebraic attacks on stream ciphers with linear feedback ››. Advances in Cryptology-CRYPTO 2003, 2729 Lecture Notes in Computer Science, 177-194. Springer-Verlag 2003.

[21] P Hwkes, G.G.Rose. ‹‹Rewring variables: the complexity of fast algebraic attacks on stream ciphers ››. Advances in Cryptology - CRYPTO 2014, 3152 Lecture notes in Computer Science, 390-406. Springer-Verlag, 2004.

[22] N. Courtois, w Meier. ‹‹Algebraic attacks on stream ciphers with linear feedback ››. Advances in Cryptology- EUROCRYPT 2003, 2656 Lecture Notes in Computer Science,345-359. Springer-Verlag, 2003.

[23] W. Meier, E.Pasalic, C .Carlet. ‹‹Algebraic attacks and decomposition of Boolean function ››.Advances in Cryptology- EUROCRYPT 2004, 3027 Lecture Notes in Computer Science, 474-491.Springer-Verlag, 2004.

[24] J. Massey: Shift-register synthesis and BCH decoding IEEE Transaction on Information Theory, 15 (1):122_127,1969.

[25] N. Coutois et W. Meier: Algebraic Attacks on Stream Ciphers with Linear Feedback. Advances in cryptology-EUROCRYPT 2003.Lecture Notes in Computer Science, 2656: 345_359, 2003.