République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique

Université de Ghardaïa

N° d'ordre :
N° de série :

Faculté des Sciences et Technologies
Département d'automatique et électromécanique

Mémoire présenté en vue de l'obtention du diplôme de

MASTER

Domaine : *Sciences et Technologies*
Filière : *Automatique*
Spécialité : *Automatique et Système*

Par : ***Massoun Imad Eddine et Chikh Salah Idriss***

Thème

Amélioration de la sécurité de transmission des images biométriques utilisant un cryptage chaotique en cascade

Soutenu publiquement le 19/06/2023

Devant le jury :

Chenini Keltoum	Grade	Université	**Président**
Kifouche Abdessalam	Grade	Université	**Examinateur**
Ladjel Boumediene	Grade	Université	**Examinateur**
Arif Mohamed	Grade	Université	**Encadreur**

Année universitaire 2022/2023


بسم الله الرحمن الرحيم

Dédicace

Je dédie ce mémoire à mes chers parents qui m'ont toujours soutenu et encouragé dans mes études. Leur présence a été essentielle dans ma réussite académique et je leur suis reconnaissant pour leur soutien constant. Cette dédicace leur est humblement dédiée.

Je souhaite également exprimer ma gratitude à mes frères et sœurs, qui ont toujours été présents pour moi et ont fait preuve de dévouement et de sacrifices. Leur amour et leur soutien ont été une source d'inspiration tout au long de mon parcours.

J'adresse mes remerciements sincères à mon encadrant, M. ARIF Mohammed, pour sa guidance et ses précieux conseils tout au long de ce travail.

Mes remerciements vont également à tous les enseignants qui m'ont accompagné tout au long de ma scolarité et ont contribué à ma réussite académique.

Enfin, j'aimerais exprimer ma reconnaissance à mes amis et à tous les membres de MNEA qui ont toujours été présents pour moi et m'ont soutenu tout au long de cette aventure.

Votre soutien inconditionnel a été d'une grande importance pour moi et je vous en suis profondément reconnaissant.

MSSOUN Imad Eddine

Dédicace

Je souhaite exprimer ma profonde gratitude à mes parents bien-aimés, qui ont toujours été là pour moi et m'ont donné un merveilleux exemple de travail et de persévérance. J'espère qu'à travers ce travail, ils ressentiront toute ma reconnaissance et mon amour.

Je tiens à exprimer ma gratitude à toute ma famille pour leur appui, leurs sacrifices, leur patience et leurs conseils précieux. Que Dieu les garde en sécurité et les regorge de bénédictions.

Un grand merci à tous mes amis et collègues, ainsi qu'à tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail. Votre soutien et votre assistance ont été très bénéfiques.

CHIKH Salah Idriss

Remerciements :

Nous voulons exprimer nos sincères remerciements à Dieu, qui nous a donné la santé, le courage et la patience tout au long de notre parcours, nous permettant ainsi d'arriver à ce stade.

Nous exprimons nos plus sincères remerciements à Dr. ARIF Mohammed, notre superviseur, pour sa direction et sa supervision de nos travaux. Nous apprécions vos échanges scientifiques, vos conseils utiles et votre rigueur.

Nous souhaitons exprimer notre profonde gratitude à tous les professeurs de notre spécialité pour leur contribution à notre formation et leur soutien continu.

Nos remerciements vont également à tous les membres du jury qui ont été présents et ont accepté d'évaluer notre travail.

Nous voulons exprimer notre gratitude à nos parents, frères, amis et membres du MNEA pour leur soutien indéfectible tout au long de ce voyage.

Enfin, nous voulons exprimer notre gratitude à tous ceux qui, de près ou de loin, ont contribué à l'achèvement de ce travail. Votre soutien et votre participation ont été essentiels.

Résumé :

Les cartes chaotiques sont largement utilisées dans différentes applications. Motivé par la structure en cascade des circuits électroniques, cet memoire présente un cadre chaotique général appelé le système chaotique en cascade (CCS). En utilisant deux cartes chaotiques unidimensionnelles comme cartes initiales, le CCS est capable de générer un grand nombre de nouvelles cartes chaotiques. Des exemples et des évaluations montrent la robustesse du CCS. Comparées aux cartes initiales correspondantes, les nouvelles cartes chaotiques générées sont plus imprévisibles et présentent de meilleures performances chaotiques, davantage de paramètres et des propriétés chaotiques complexes. Pour étudier les applications du CCS, nous introduisons un générateur de nombres pseudo-aléatoires (PRNG) et un système de cryptage de données utilisant une carte chaotique générée par le CCS. Des simulations et des analyses démontrent que le PRNG proposé présente une grande qualité d'aléatoire et que le système de cryptage de données est capable de protéger différents types de données avec un niveau de sécurité élevé.

Termes clés :

Système chaotique en cascade (CCS), carte chaotique, cryptage de données, générateur de nombres pseudo-aléatoires (PRNG).

Abstract:

Chaotic maps are very useful in many different fields. This dissertation offers the cascade chaotic system (CCS), a broad chaotic framework that takes into account the cascading pattern seen in electrical circuits. With only two 1-D chaotic maps acting as seed maps, CCS is able to produce a plethora of brand-new chaotic maps. The strength of CCS is supported by examples and assessments. The newly created chaotic maps show enhanced unpredictability, enhanced chaotic performance, an expanded parameter set, and complicated chaotic properties in contrast to the comparable seed maps. We present a pseudo-random number generator (PRNG) and a data encryption system using a chaotic map produced by CCS to investigate the practical uses of CCS. The suggested PRNG demonstrates high-quality randomness, according to simulation and analysis, and the data encryption system provides high levels of security for a variety of data types.

Index Terms:

Data encryption, chaotic map, cascade chaotic system (CCS), and pseudo-random number generator (PRNG).

ملخص :

تُستخدم الخرائط الفوضوية على نطاق واسع في تطبيقات مختلفة. مستوحاة من الهيكل التتابعي في الدوائر الإلكترونية، تقدم هذه المذكرة إطار فوضوي عام يُسمى "نظام الفوضى التتابعي (CCS) ". باستخدام خريطتي فوضى أحادية البعد كخرائط بذرة، يستطيع CCS توليد عدد هائل من الخرائط الفوضوية الجديدة. تُظهر الأمثلة والتقييمات قوة CCS. بالمقارنة مع الخرائط البذرية المقابلة، تكون الخرائط الفوضوية الجديدة المولدة أكثر عدم التنبؤ وتتمتع بأداء فوضوي أفضل ومعلمات أكثر وخصائص فوضوية معقدة. لاستكشاف تطبيقاتCCS ، نقدم مُولّد أعداد عشوائية شبه عشوائي (PRNG) ونظام تشفير بيانات باستخدام خريطة

فوضوية تم إنشاؤها بواسطة CCS. تُظهر المحاكاة والتحليل أن PRNG المقترح لديه جودة عالية من العشوائية وأن نظام تشفير البيانات قادر على حماية أنواع مختلفة من البيانات بمستوى أمان عالي.

كلمات مفتاحية :

نظام الفوضى التتابعي(CCS) ، خريطة فوضوية، تشفير البيانات، مُولّد أعداد عشوائية شبه عشوائي.(PRNG)

Liste des figures

Liste des tableaux

Sommaire

Chapitre 03 :Cryptage et cryptographie

Chapitre 04 : Resultats et discussion

Glossaire :

CBC : Cipher Block Chaining

CCS : Système Chaotique en Cascade.

CEI : Commission électrotechnique internationale.

ECB : Electronique Code Book.

ECG : Electrocardiogramme.

FISMA : Federal Information Security Management Act.

KE : L'entropie de Kolmogorov.

LE : L'exposant de Lyapunov.

NCM : New Chaotique Map.

NCMs : New Chaotique Maps.

NIST : National Institute of Standards and Technology.

NPCR : Le taux de changement du nombre de pixels.

NPWLCM : New Piecewise Linear Chaotic Map.

PCG : Phonocardiogram.

PDCA : Plan–Do–Check–Act.

PRNG : Pseudo random Number Generator.

PWLCM : Piece Wise Linear Chaotic Map.

PWLCM : Piecewise Linear Chaotic Map.

RNG : Random Number Generator.

TL-DEA : Tent-Logistic map-based Data Encryption Algorithm.

TL-PRNG : Tent-Logistic Pseudo Random Number Generator.

UACI : L'intensité moyenne modifiée unifiée.

XOR : Exclusive OR.

Introduction Générale :

Dans le monde numérique d'aujourd'hui, où les informations personnelles sont de plus en plus accessibles et les menaces de sécurité sont omniprésentes, la protection des données sensibles est devenue une préoccupation majeure. Parmi ces données, les informations biométriques occupent une place particulière en raison de leur nature unique et de leur rôle crucial dans l'identification et l'authentification des individus.

De nombreuses solutions ont été proposées pour prévenir les attaques et protéger la liberté et les informations personnelles. Les pares-feux et la cryptographie font partie de celles-ci. La cryptographie comprend une variété de méthodes, y compris la cryptographie à clé publique, la cryptographie à clé privée, la cryptographie quantique et la cryptographie basée sur le chaos.

Un état spécifique d'un système dont le comportement ne se répète jamais, est extrêmement sensible aux conditions initiales et est imprédictible à long terme est défini sous le nom de "chaos". Au contraire, le chaos est défini par le comportement des systèmes dynamiques déterministes qui sont instables et non linéaires. La relation entre l'instabilité et la chaoticité est alors que le système est très sensible aux changements.

Effectivement, l'histoire de la cryptographie remonte à plus de 1000 ans en Égypte, où l'on trouve les premières utilisations connues de cette discipline. À l'époque, les méthodes utilisées étaient souvent très primitives. De plus, la cryptographie était principalement utilisée pour répondre aux besoins de l'armée et de la diplomatie, limitant ainsi sa mise en œuvre à ces domaines spécifiques. Cependant, c'est pendant la Seconde Guerre mondiale que la cryptographie et la cryptanalyse ont connu un développement majeur et ont exercé une influence profonde.

Le cryptage chaotique en cascade présente des avantages significatifs en termes de sécurité et de robustesse. En exploitant les propriétés du chaos déterministe, il offre une méthode efficace pour crypter les données sensibles et garantir leur confidentialité. Avec sa sensibilité aux conditions initiales, sa diffusion élevée et sa complexité accrue, le cryptage chaotique en cascade se positionne comme une solution prometteuse pour protéger les informations confidentielles dans divers domaines tels que les communications sécurisées, les systèmes de paiement électronique et la protection des données biométriques.

Le cryptage chaotique en cascade améliore la sécurité de la transmission d'images biométriques. La confidentialité et l'intégrité des données sensibles sont assurées grâce à la transformation des images en un format crypté qui ne peut être lu par les personnes non autorisées. Le cryptage en cascade augmente la complexité et la résistance aux attaques de cryptanalyse en raison de ses systèmes chaotiques interconnectés. La sensibilité aux conditions initiales et aux paramètres est assurée par les propriétés du chaos déterministe, ce qui rend le processus de cryptage plus sûr. De plus, ce cryptage garantit une diffusion élevée des données, élimine toute corrélation potentielle et protège contre les attaques par canaux bruités ou les pertes de données. Les images biométriques sont mélangées et perturbées à l'aide de séquences pseudo-aléatoires créées par des systèmes chaotiques, ce qui renforce la sécurité. En résumé, l'utilisation du cryptage chaotique en cascade sur les images biométriques améliore considérablement leur sécurité lors de la transmission, préservant ainsi la confidentialité et l'intégrité des données biométriques sensibles.

En utilisant les idées des systèmes chaotiques en cascade, notre objectif principal est de créer un système de sécurité avancé.

Le premier chapitre de ce mémoire traite des techniques biométriques. Le deuxième chapitre traite de la sécurité des données. Le cryptage et la cryptographie sont abordés dans le troisième chapitre et La méthode de chiffrement basée sur chaotique cascade est présentée dans le dernier chapitre.

CHAPITRE 01
LES TECHNIQUES BIOMETRIQUES

1.1 Introduction :

La biométrie est un ensemble des technologies appelées les technologies biométriques qui exploitent des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche, et l'empreinte palmaire pour différencier des personnes.

Ces caractéristiques sont traitées par certains ordres des processus automatisés à l'aide des dispositifs comme des modules de balayage ou des appareils-photo.

À la différence des mots de passe ou des numéros d'identification personnelle (PINs) qui sont facilement oubliés ou exposés à l'utilisation frauduleuse, ou des clefs ou des cartes magnétiques qui doivent être portées par l'individu et sont faciles à être volées, copiées ou perdues, ces caractéristiques biométriques sont uniques à l'individu et il y a peu de possibilités que d'autres individus puissent remplacer ces caractéristiques, donc les technologies biométriques sont considérées les plus puissantes en termes de sécurité.

En plus les mesures biométriques sont confortables parce qu'elles n'ont pas besoin d'être portées séparément. De telles caractéristiques peuvent être bien employées pour obtenir l'identification/authentification pour accéder à des systèmes tels que les guichets automatiques.

La biométrie se prouve également comme outil puissant d'identification/vérification aux scènes de crime dans le secteur juridique.

1.2 Définition de la biométrie :

La biométrie est une mesure des caractéristiques biologiques pour l'identification, où l'authentification d'une personne à partir de certaines de ses caractéristiques est possible.

Le mot "biométrie" provient de deux mots grecs, "bios" signifiant "vie" et "Metrikos" signifiant "mesure". [1]. Il fait référence à l'ensemble des procédés par lesquels une personne est reconnue automatiquement en fonction de certaines de ses caractéristiques. C'est la rencontre entre les techniques numériques, les caractéristiques du corps humain et un besoin de la société moderne : "identifier facilement et sûrement des personnes" [2]. Il est également possible de la décrire comme l'analyse mathématique de toutes les caractéristiques physiques ou traits personnels

automatiquement mesurables, permanents et distincts qui peuvent être utilisées pour identifier une personne ou pour vérifier l'identité prétendue d'une personne.

La biométrie consiste à vérifier ou à déterminer l'identité d'une personne à partir des caractéristiques de cette personne.

1.3 Différentes techniques biométriques :

Actuellement, il existe plusieurs techniques biométriques différentes permettant d'identifier ou de vérifier une personne [3], [4], [5]. Celles-ci sont répertoriées dans trois catégories.

1.3.1 Techniques physiologiques (statiques) :

Forme de la main ou des doigts de la main :

La géométrie de la main est une caractéristique unique à chaque individu. Des paramètres tels que la taille de la paume, la longueur et la largeur des doigts, leur épaisseur et leur position relative sont extraits à partir de l'image de la main acquise grâce à un scanner spécialisé qui est encore encombrant [1]. La biométrie de la main est toutefois sujette.

Aux modifications de la forme de la main liées au vieillissement. Le taux d'erreurs dans la reconnaissance est assez élevé, en particulier pour des personnes appartenant à une même famille en raison d'une forte ressemblance. De ce fait, la fiabilité des systèmes biométriques basés sur l'empreinte palmaire est affectée [27].

Avantages :

- Bonne acceptation des usagés ;
- Très simple à utiliser ;
- Le résultat est indépendant de l'humidité et de l'état de propreté des doigts.

Inconvénients :

- Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille ;
- Trop encombrant pour un usage sur le bureau ou dans une voiture.

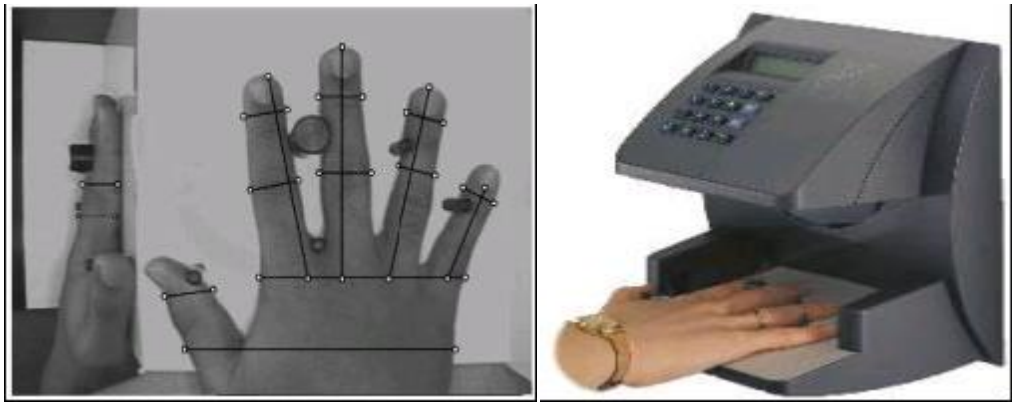


Figure 1-1 : Identification de la forme de la main[27].

Les veines :

Il s'agit ici d'analyser le dessin (configuration) formé par le réseau des veines sur une partie du corps d'un individu (la main ou les doigts) pour en garder quelques points caractéristiques [27]. Cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main.

Avantage :

- Il n'existe aucun moyen de frauder, car on ne peut pas "photographier" les veines de la main. Le réseau vasculaire est propre à chaque individu : même les vrais jumeaux en ont un différent.

Inconvénient :

- La méthode est encore trop récente pour être correctement évaluée. Le scanner est relativement encombrant comparer aux capteurs d'empreintes digitales.

Figure 1-2 : Le réseau veineux de la main[27].

Empreintes digitales :

Les systèmes de reconnaissance d'empreintes digitales exploitent la forme géométrique des parties (surfaces) inférieures des bouts des doigts pour effectuer la reconnaissance des personnes.

Cette technique utilisait au départ par la police scientifique, la reconnaissance par empreinte digitale est aujourd'hui la technique la plus largement utilisée [7].

Avantages :

- Technique évoluée et éprouvée
- Grande précision ;
- Peuvent être installés dans divers milieux ;
- Dispositifs ergonomiques et faciles à utiliser ;
- Permettent d'enrôler plusieurs empreintes (plus grande précision et fiabilité) ;

Inconvénients :

- Enrôlement impossible pour un faible pourcentage ;
- Performance pouvant se détériorer avec le temps ;
- Association psychologique à une enquête criminelle.

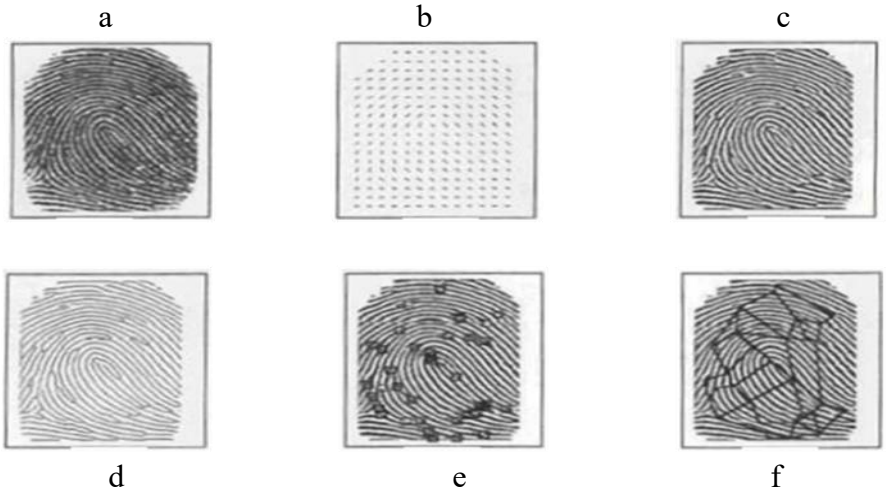


Figure 1-3 : Etapes de traitement d'une empreinte digitale : a) originale, b) orientation, c) image binarisée, d) image affinée, e) points caractéristiques, f) graphe des minuties[27].

Visage :

C'est la technique la plus simple et la moins contraignante. Mais elle a encore de gros progrès à faire. En mode vidéo, les résultats ne sont pour l'instant pas très probants.

L'utilisation d'une caméra permet de capter la forme du visage d'un individu et d'en dégager certaines particularités telles que l'écartement des yeux, narines, largeur de la bouche. Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Un système utilisant une telle technique doit être capable de reconnaître un individu malgré les différents artifices physiques tels que pilosité, chirurgie esthétique, vieillissement, maquillage, variation de l'éclairage et expression faciale inhabituelle [8].

Avantages :

- Peuvent s'appuyer sur l'équipement d'acquisition des images actuel ;
- Peuvent comparer des images statiques, comme des photos de permis de conduire ;
- Seule technique biométrique offerte sur le marché capable de fonctionner sans la collaboration du sujet.

Inconvénients :

- Les changements dans l'environnement d'acquisition des images (principalement la lumière et l'angle de l'appareil photo) peuvent avoir une incidence sur l'exactitude de la concordance ;
- Les changements physiques peuvent tromper le système ;
- Fortes préoccupations relatives au respect de la vie privée en raison de leurs capacités d'enrôlement et d'identification sans la collaboration des sujets.

Figure 1-4 : Points clés dans la reconnaissance faciale[27].

Rétine :

Cette technique se base sur le fait que le dessin formé par les vaisseaux sanguins de la rétine (Figure I-6), paroi interne de l'œil, est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. Mais, elle est moins bien acceptée par les utilisateurs à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques millimètres), l'image de la rétine est numérisée par un laser à faible intensité en effectuant un balayage de celle-ci [27].

Avantages :

- Extrêmement précis.
- Très difficiles à mystifier.

Inconvénients :

- Relativement difficiles à utiliser.
- Pas largement distribués sur le marché.

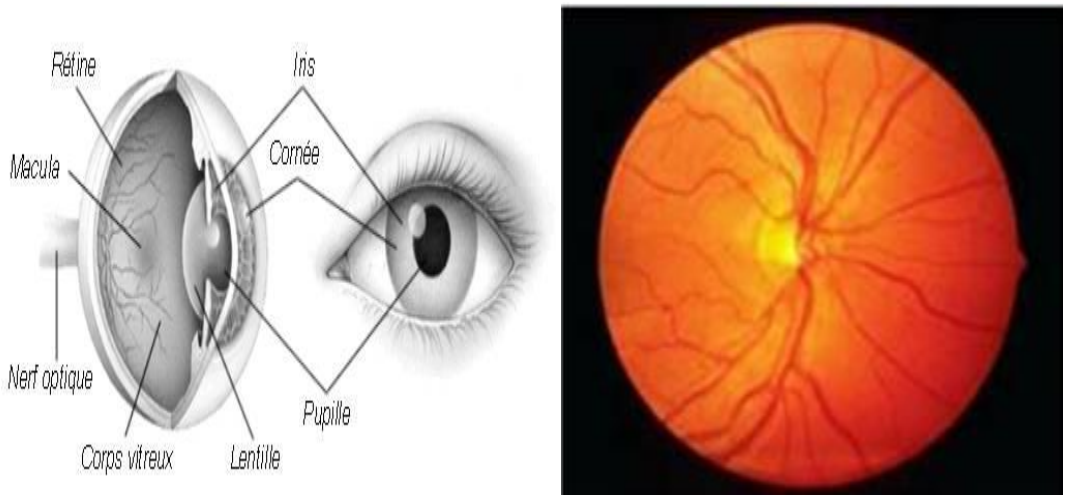


Figure 1-5 : Image d'une rétine[34].

L'iris :

En ce qui concerne l'iris (Figure I-7), l'individu se place en face du capteur (caméra) qui scanne son iris. Cette technique est relativement désagréable pour l'utilisateur car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct. La fraude est aussi possible par le port de lentilles. Néanmoins, la texture de l'iris est riche et unique (même

entre jumeaux et entre l'œil gauche et droit) de laquelle des paramètres caractéristiques sont extraits formant une configuration unique le caractérisant [9].

Avantages :

- Potentiel de très grande précision.
- Peuvent être utilisés pour l'identification et la vérification.
- Les structures de l'iris restent stables durant toute la vie.

Inconvénients :

- L'acquisition des images exige une certaine formation et de la pratique.
- L'acquisition des images crée un certain inconfort chez l'utilisateur, ce qui peut empêcher l'enrôlement de certaines personnes.
- Le nombre de faux rejets est plus élevé que pour les autres techniques.

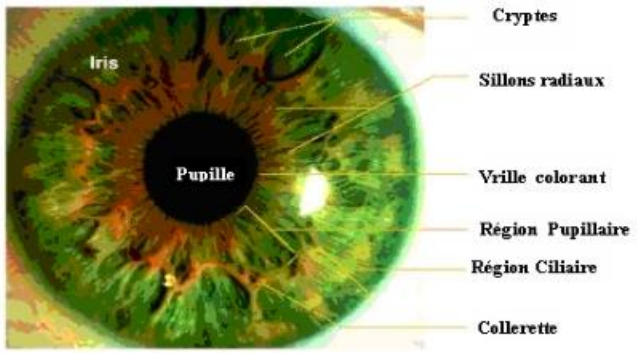


Figure 1-6 : Reconnaissance d'iris [27].

1.3.2 Techniques comportementales (dynamiques) :

La voix :

Un son (voix) se caractérise par une fréquence, par une intensité et par une tonalité qui sont dues à la forme des cordes vocales qui elles-mêmes sont suffisamment distinctes d'un individu à l'autre. Il faut faire une distinction entre les systèmes dépendants et indépendants du texte. En système dépendant, le texte prononcé lors de l'authentification est le même que celui préalablement enregistré. Par contre, en mode indépendant, le locuteur prononce la phrase qu'il désire. La reconnaissance vocale est le seul moyen pour authentifier une conversation téléphonique [27]. Pour autant, ce moyen n'est pas complètement fiable puisque la fatigue, le stress ou la maladie peuvent altérer la voix. Enfin, la fraude est possible par enregistrement.

Avantages :

- Peuvent exploiter la vaste infrastructure téléphonique.
- Se fondent bien avec la reconnaissance de la parole et les mots de passe vocaux.
- Aucune connotation négative, contrairement à d'autres techniques biométriques.

Inconvénients :

- Leur conception les rend vulnérables à la fraude à l'aide d'enregistrements.
- Les dispositifs de capture de piètre qualité et le bruit ambiant limitent souvent leur précision.
- Les gabarits sont généralement très volumineux comparativement à ceux des autres techniques biométriques.

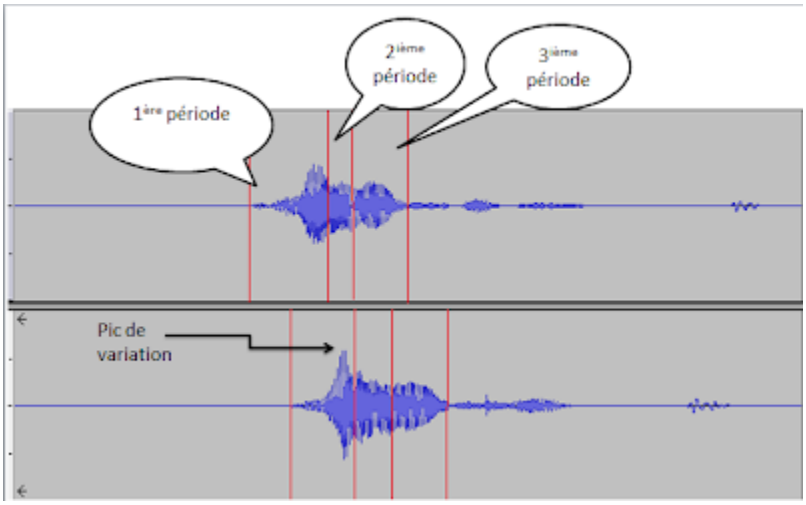


Figure 1-7 : Spectre de la voix [35].

Techniques de frappe au clavier :

Cette technique, qui utilise les statistiques, est aussi appelée dactylographie dynamique. Elle mesure la façon dont l'utilisateur appuie sur les touches (temps d'appui et temps entre chaque frappe). Étant donné qu'une personne peut améliorer sa vitesse et sa technique de frappe sur un clavier, le système doit sans cesse renouveler son fichier référence [10].

Avantages :

- Exploitent le matériel existant.
- Exploitent le processus d'authentification par mot de passe.
- Un mot de passe peut être changé au besoin.
- Perçus comme non contraignants.

Inconvénients :

- Technique récente.
- Renforcent la sécurité, mais ne sont pas plus pratiques pour autant.
- Conservent bien des défauts de l'authentification par mot de passe.

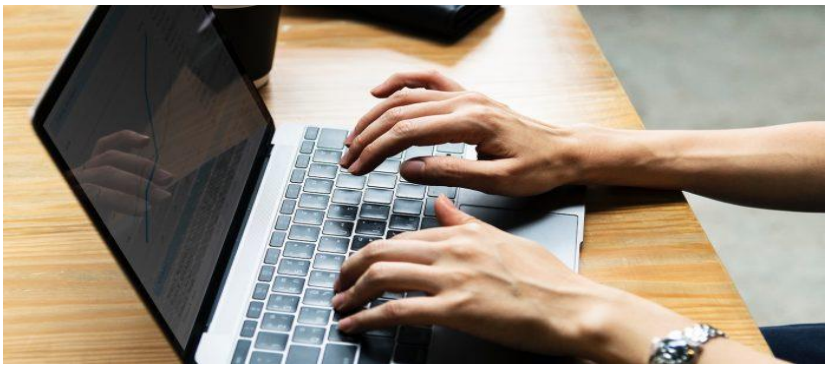


Figure 1-8 : Dynamique de frappe au clavier [36].

Analyse de fréquence cardiaque :

La reconnaissance par la forme du pouls sanguin de l'électrocardiogramme (ECG) ou phonocardiogram (PCG) a été proposée, mais il y a peu d'activité dans ce domaine, et ce n'est toujours pas une méthode qui a fait ses preuves [11].

ECG : ECG mesure le changement du potentiel électrique du cœur avec le temps. Puisque les signaux commencent au cœur, ECG décrit une mesure de battement. La durée d'un battement de cœur change avec l'effort, inquiétude, et même avec l'heure. Cependant, la structure du battement de cœur contient seulement des différences scalaires avec des changements d'effort [12].

PCG : L'introduction récente des stéthoscopes électroniques, qui fournissent les signaux numériques de l'excellente qualité PCG, a réveillé l'intérêt considérable pour les techniques pour l'analyse automatique des signaux de PCG, qui contiennent une grande quantité d'informations sur l'état du système cardio-circulatoire d'un individu. L'idée est que les signaux de PCG ont de différentes caractéristiques spécifiques qui peuvent être prises en compte comme signe physiologique utilisé dans un système biométrique [13].

Mouvement des lèvres :

Les lèvres ne sont pas très connues en tant qu'éléments anthropomorphiques, et n'ont été guère étudiées. Cependant, elles sont intéressantes à plusieurs égards [11] :

- **L'empreinte des lèvres** est connue en médecine légale pour être spécifique à chaque individu, comme le sont les empreintes.
- **Le mouvement des lèvres** aide l'identification utilisant la voix.
- **La forme des lèvres** peut être utilisée seule pour l'authentification.

Les systèmes de biométrie basés sur l'identification de forme de lèvre sont des matières intéressantes à peine, non développée dans la littérature scientifique. C'est peut-être dû à la croyance généralisée des recherches de sa puissance à peine distinctive. Cependant, une étude soigneuse prouve que la différence parmi le contour de la lèvre des personnes est plus grande que la différence parmi la forme à différentes images de lèvre de la même personne. Ainsi, l'identification biométrique par le contour de lèvre est possible [14].

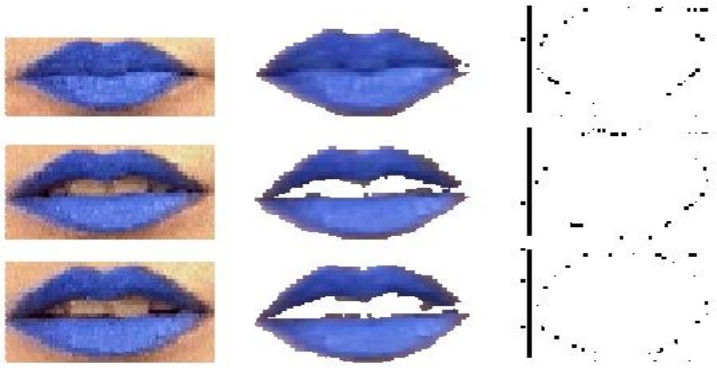


Figure 1-9 : Extraction de la forme de lèvre [27].

Reconnaissance de l'écriture :

La reconnaissance optique des caractères (ROC, OCR) est presque aussi vieille que le champ de l'origine remonte aux années 1900 [1 journalières. Le lecteur de code à barres adapte les supermarchés et les magasins généraux. Augmentation d productivité dans beaucoup de bureaux. S'adresser aux lecteurs assortit automatiquement des morceaux de courrier dans le courrier stations [16].

A. Reconnaissance de caractère et analyse de documents :

La structure du texte est limitée à quelques lignes ou mots. La lecture consiste en un simple repérage des mots dans les lignes, puis à un découpage de chaque mot en caractère. Dans le second cas, il s'agit de données bien structurées dont la lecture nécessite la connaissance de la typographie et de la mise en page du document (structure physique et logique de contenu) [15].

La reconnaissance l'industrie et les secteurs de caractères manuscrits a de nombreuses applications dans de service où une grande masse des documents de roulement des textes doit être interprétée et est aujourd'hui traité par les opérateurs humains qui agissent selon ce qui a été écrit ou simplement verrouiller ce qu'ils lisent sur un système informatique qui effectuera une transformation plus ultérieure de L'identification des adresses manuscrites dans les morceaux de l'information acquise. Courriers postaux est un exemple typique de cet arrangement. Pourtant là existent d'autres applications qui adaptent le même moule, comme la banque de lecture ou les contrôles postaux, traitant les feuilles d'impôt manuellement remplies dehors, analysant documents qui incluent le texte aussi bien que des images ou des graphiques et accumulation d'une lecture machine pour l'abat-jour [17].

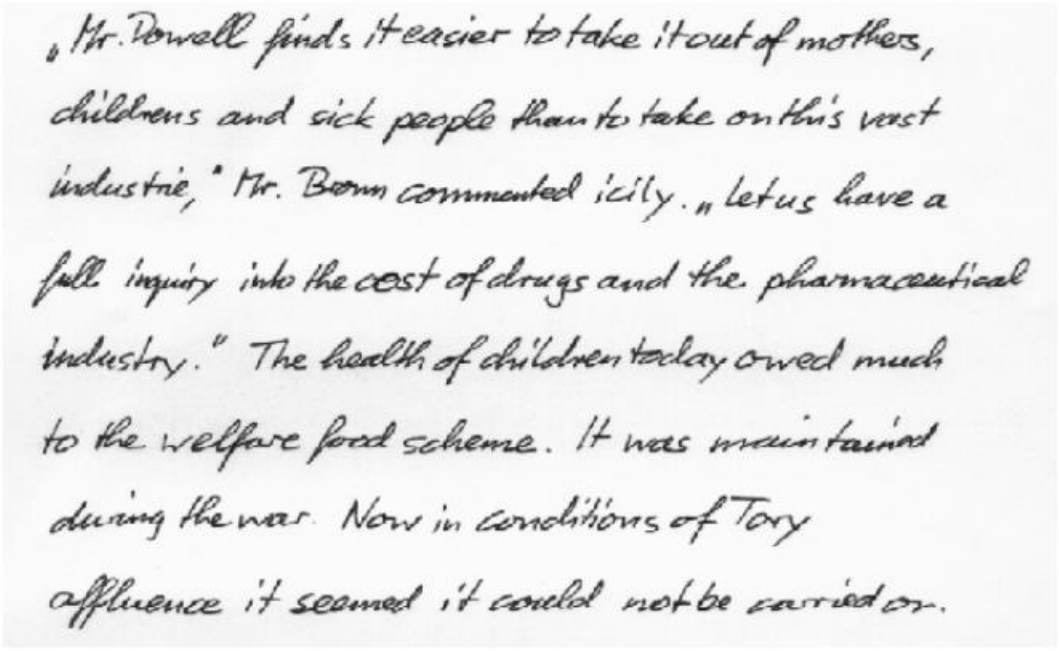


Figure 1-10 : Exemple d'un document manuscrit [27].

La signature manuscrite :

La vérification de signature est le processus utilisé pour identifier les signatures manuscrites d'un individu [18]. Elle a été pratiquée pendant des siècles, et l'acte de signer un document a été longtemps accepté par presque chaque culture dans le monde en tant que son identification. De nos jours, il est généralement employé et accepté comme une manière de vérifier l'identité des personnes dans une grande variété de buts, particulièrement dans légal, les banques, le film publicitaire, et même les documents éducatifs [19].

Figure 1-11 : Exemple de signature de base de données MCYT [27].

L'application de la vérification de signature est principalement employée dans les secteurs où la vérification de l'identité d'un individu est exigée pour être établie avant d'effectuer une transaction confidentielle. Certains des secteurs où c'est applicable sont [20] :

- Applications bancaires : la signature sur le chèque à ordre est vérifiée avant le dégagement des transactions monétaires.
- Applications aux cartes de crédit : le monde s'est déjà déplacé à une société cashless (sans cache) là où la plupart des transactions monétaires sont faites en utilisant des cartes de crédit au lieu de l'argent comptant ou des contrôles. Les possibilités de vérification de la signature peuvent être utilisées pour vérifier des disques de crédit d'un client.
- Agences d'application de loi : Ceux-ci emploient la vérification de signature pour arranger des cas légaux impliquant des contesté des documents. Une branche spécialisée de la science légale est consacrée afin d'étudier l'écriture et les signatures.
- Agences de sécurité : La signature peut être employée comme code personnalisé pour accorder l'entrée dans des secteurs exigeant l'autorisation.

1.3.3 Techniques émergentes :

La marche :

Chaque individu marche avec des mouvements de bras, de jambes et un déhanchement qui lui sont propres.

La démarche est définie comme la manière dont une personne marche. On peut étendre cette définition en parlant de dynamique des mouvements liés à la marche à pied d'une personne [21].

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps…), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle. Mais des vêtements amples, par exemple, peuvent compromettre une bonne identification .

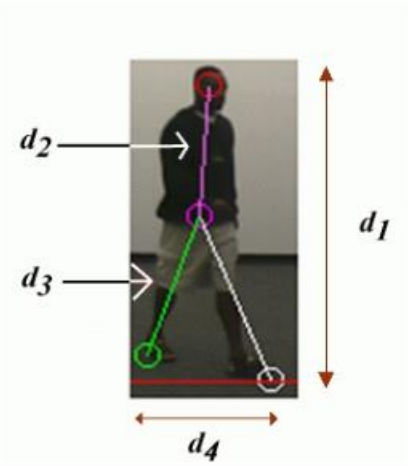


Figure 1-12 : Caractéristiques de la marche [27].

Avantages :

- Alternative à la reconnaissance faciale
- Peuvent fonctionner sans la collaboration du sujet

Inconvénients :

- Pas bien développés et pas offerts sur le marché.
- Des changements comportementaux de la démarche peuvent tromper le système.
- Fortes préoccupations relatives au respect de la vie privée en raison de leurs capacités d'enrôlement et d'identification sans la collaboration des sujets.

L'empreinte génétique (ADN) :

L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN) [22], [23]. Cette technique est complexe, coûteuse et lente à réaliser compte tenu des nombreuses manipulations biologiques (amplification + électrophorèse). Ceci explique ce fait qu'il n'existe toujours pas de solution technologique grand-public qui permette de réaliser automatiquement cette analyse, d'autant plus qu'elle nécessite un prélèvement d'échantillon (sang, salive, sperme, cheveux, urine, peau, dents, etc.) qui rend cette technique très intrusive [27].

Figure 1-13 : Illustration de l'acide désoxyribonucléique « ADN » [37].

Oreille :

En raison du fait qu'il n'existe pas deux formes d'oreilles identiques, la technique serait à priori efficace. Cependant, aucune application commerciale n'a encore été créée.

Selon certaines études scientifiques, même les jumeaux n'ont pas deux oreilles identiques sur Terre. En effectuant plus d'une centaine de mesures très précises, il serait donc possible de reconnaître une personne par son oreille. Les proportions de l'oreille sont conservées, bien qu'elle se développe jusqu'à 20 ans, se stabilise et recommence à grandir après 45 ans [27]. Ainsi, la reconnaissance pourrait être effectuée à tout âge.

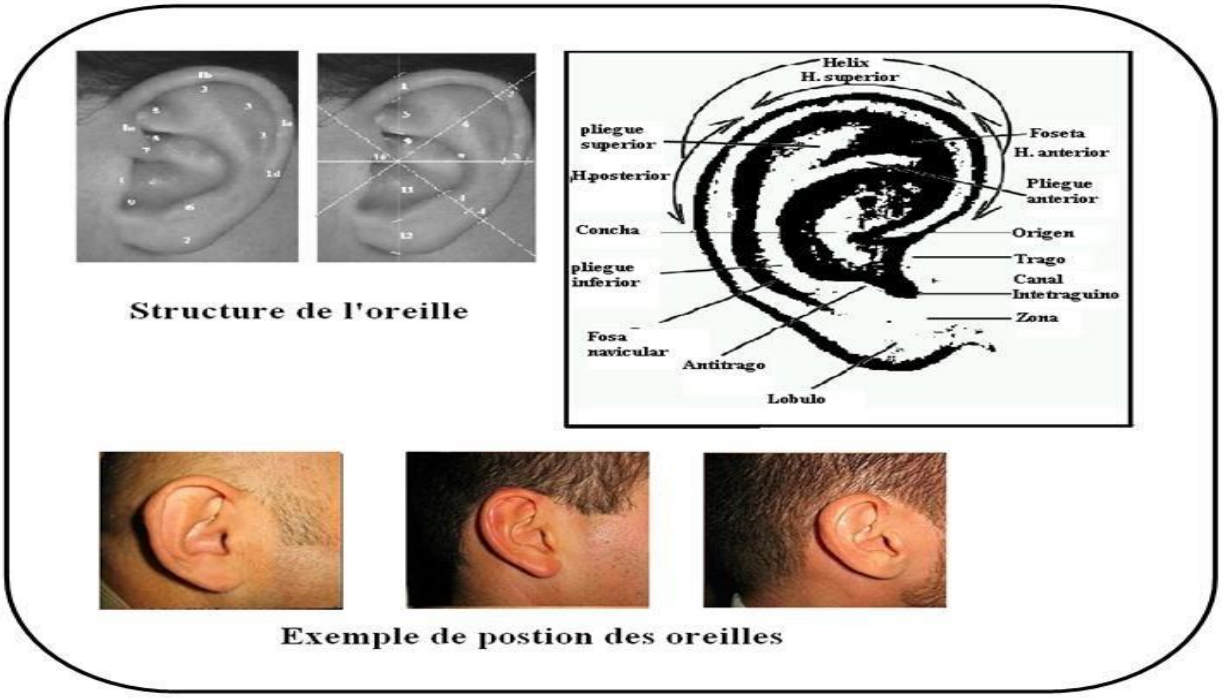


Figure 1-14 : Forme d'oreille [38].

L’odeur :

Chaque individu répand une odeur distincte. Le vivant est plus fort que la machine. Même si des "nez électroniques" existent, les chiens sont toujours les meilleurs pour reconnaître les odeurs individuelles. Peu de gens sont disposés à accepter de se faire renifler chaque matin! Par conséquent, cette méthode est principalement employée dans le secteur de l'agroalimentaire [27].

La thermographie faciale :

Le principe est que chaque corps an une température différente. Une caméra thermique prend une photo infrarouge du visage. Il est possible de montrer une distribution spécifique de la chaleur pour chaque personne, voire de tracer le réseau veineux du visage qui est invisible à l'œil nu. L'avantage est qu'il est possible de différencier de vrais jumeaux. Ainsi, contrairement à la reconnaissance faciale, il peut être utilisé même dans l'obscurité ou dans des conditions de mauvaise visibilité. Cependant, les conditions de vue peuvent entraîner des erreurs [27]. Ce système est très coûteux et est encore en phase de test.

1.4 Les types de systèmes biométriques :

1.4.1 Mono-modalité :

La biométrie monomodale est une technologie d'authentification par modalité biométrique unique. Avant de proposer un système biométrique, il est nécessaire de déterminer la modalité la plus adaptée à l'application [28].

1.4.2 Multi-modalité :

La biométrie multimodale consiste à combiner plusieurs systèmes biométriques, ce qui permet l'identification d'une plus grande quantité d'informations discriminantes dans les personnes. Effectivement, cela permet de réduire certaines contraintes des systèmes biométriques monomodaux. Une alternative est la multimodalité, qui peut améliorer de manière systématique les performances d'un système biométrique [29].

1.5 Quelle méthode biométrique est la plus efficace?

La comparaison des différentes biométries est généralement effectuée en fonction dequatre critères à savoir **l'effort, l'intrusion, le coût, et la précision** [30].

- **L'effort (Effort) :** l'effort de l'utilisateur lors de la vérification du système biométrique.
- **L'intrusion (Intrusiveness) :** niveau d'acceptation de l'utilisateur du test.
- **Le coût (Cost) :** investissement dans la technologie (capteurs, lecteurs...).
- **La précision (Accuracy) :** efficacité du processus.

Selon l'analyse Zephyr (Figure 1-15), il n'existe pas de méthode biométrique idéale car chaque méthode a ses avantages et ses inconvénients. Le choix dépend essentiellement de la nature de l'application. Par exemple, la voix et la signature sont des méthodes peu intrusives, peu coûteuses, mais pas assez performantes. Bien que l'iris et la rétine soient fiables, leurs prix sont élevés et le grand public les considère mal. Il convient de noter que le choix de la modalité biométrique dépend également de la culture locale des utilisateurs. En Asie, les méthodes nécessitant un contact physique, comme l'empreinte digitale, sont rejetées pour des raisons d'hygiène, tandis que les méthodes qui ne nécessitent pas de contact sont bien acceptées [31].

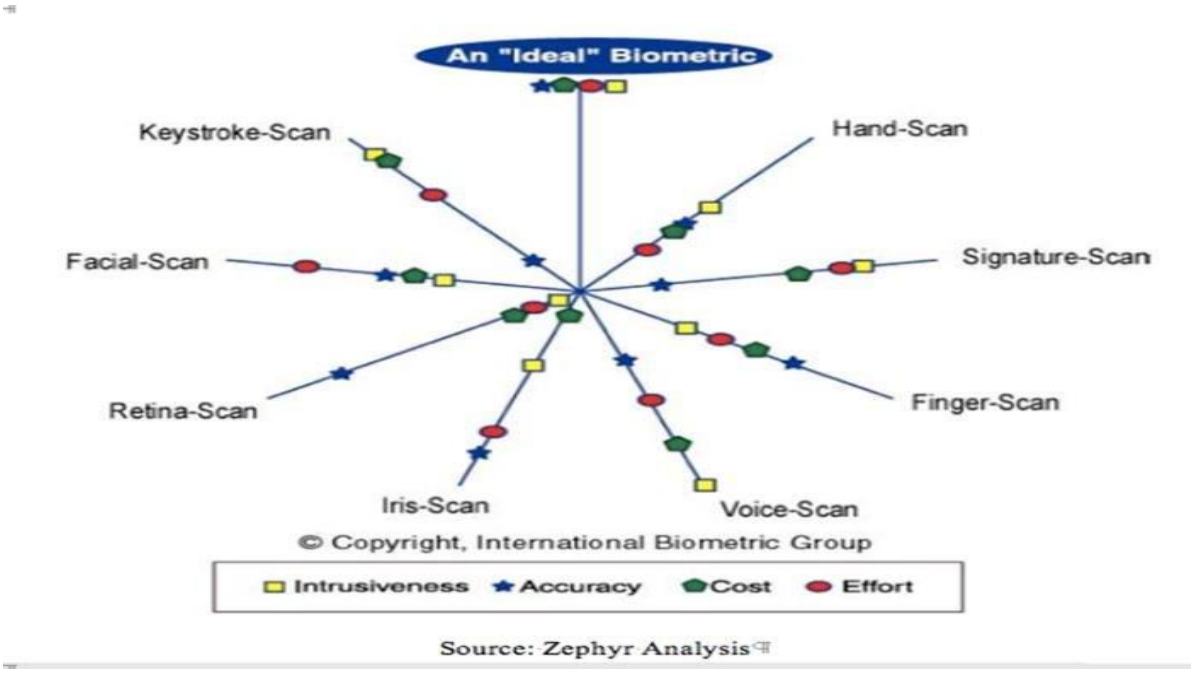


Figure 1-15 : L'analyse Zephyr compare différentes modalités en fonction de quatre critères fondamentaux : l'intrusion, la précision, le coût et l'effort [39].

1.6 Comparaison entre quelques techniques biométriques :

Identifiant biométrique	Universalité	Caractère distinctif	Permanence	Facilité de saisie	Performance	Acceptabilité	Facilité de contournement
ADN	E	E	E	F	E	F	F
Oreille	M	M	E	M	M	E	M
Visage	E	F	M	E	F	E	E
Empreinte digitale	M	E	E	M	E	M	M
Démarche	M	F	F	E	F	E	M
Géométrie de la main	M	M	M	E	M	M	M
Veines de la main	M	M	M	M	M	M	F
Iris	E	E	E	M	E	F	F
Dynamique de la frappe	F	F	F	M	F	M	M
Empreinte palmaire	M	E	E	M	E	M	M
Rétine	E	E	M	F	E	F	F
Signature	F	F	F	E	F	E	E
Voix	M	F	F	M	F	E	E

Tableau 1 : Tableau comparatif des différentes techniques biométriques. (E : Elevé, F : faible et M : Moyen) [32].

1.7 Conclusion :

Ce chapitre a fourni une présentation générale de la biométrie, ainsi que des méthodes biométriques différentes, avec les avantages et les inconvénients de chaque méthode. Nous avons également comparé différentes méthodes biométriques. Nous avons défini le mode de fonctionnement du système biométrique, son domaine d'application, son architecture, ses types et ses performances.

Bibliographie

[1] : A. K. Jain, A. Ross et S. Prabhakar. “An introduction to biometric recognition”, IEEE transactions on circuits and systems for video technology, Vol. 14, no. 1, pp. 4-20 Janvier 2004.

[2] : D. Maltoni, D. Maio, A. K. Jain et S. Prabhakar, “Handbook of Fingerprint Recognition”, Springer Verlag, New York, NY, USA, Juin 2003.

[3] : A. Jain, R. Bolle et S. Pankanti, "BIOMETRICS: Personal Identification in Networked Society", Kluwer Academic Publishing, 1999 (quatrième édition 2002).

[4] : D. Polemi, "Biometrics techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable", Rapport interne, Institute of communication and computer systems, National technical university of Athens, 1997.

[5] : E. Sender, "Le corps pour tout passeport", Revue Sciences et Avenir, pages 64-67, Septembre 2004.

[6] : M. Adán , A. Adán, A. S. Vázquez, R. Torres, "Biometric verification/identification based on hands natural layout", Image and Vision Computing 26 (2008), pp 451–465.

[7] : Guide de sécurité des technologies de l'information, "Les technologies biométriques : une évaluation d'applications pratiques", Sous direction de la sécurité technique, Opérations techniques, Gendarmerie royale du Canada, juin 2002.

[8] : W. Zhao, R. Chellappa, P.J. Phillips et A. Rosenfeld, "Face recognition: A literature survey", ACMComputing Surveys (CSUR), Volume 35, Issue 4, Décembre 2003.

[9] : J. G. Daugman, "High Confidence Recognition of Persons by a Test of Statistical Independence", IEEE

Trans. Pattern Anal. and Machine Intell., Vol. 15, No.11, pp. 1148-1161, 1993.

[10] : P. Mroczkowski, "Identity Verification using Keyboard Statistics", Thèse Master, Linköping University, Linköping, Suède, 2004.

[11] : http:/pagesperso-orange.fr/fingerchip/biometrics/types.htm

[12] : J. M. Irvine, S. A. Israel, W. T. Scrugg, W. J. Worek, "eigenPulse: Robust human identification from cardiovascular function", Pattern Recognition 41 (2008) 3427 – 3435.

[13] : F. Beritelli, S. Serrano, "Biometric Identification Based on Frequency Analysis of Cardiac Sounds", IEEE Transactions on information forensics and security, vol 2, N° 3, September 2007.

[14] : E. Gomez, C. M. Travieso, J. C. Briceno et M. A. Ferrer, "Biometric Identification System By Lip Shape", Proceedings of, 36th Annual International Carnahan Conference, 20-24 Oct. 2002, IEEE, pp 39-42.

[15] : A. Belaïd, Y. Belaïd, "Reconnaissance des formes, méthodes et applications", Inter Edition, Paris,1992.

[16] : L. Pavlidis, “Physics-Based Methodologies for Recognizing, Handwritten Signatures, Words, and Line Drawings”, thèse de PhD, Faculty of the Graduate School of the University of Minnesota, novembre 1996. [17]. KE HAN, « Handwriting Identification and Recognition”, thèse de PhD, The Graduate School of Wayne State University, Detroit, Michigan, 1995

[18] : “Biometrics Information Resource: Signature Recognition”, http://www.biometricsinfo.org/signaturerecognition.htm

[19] : L. K. Kwong, “A New Statistical Stroke Recovery Method and Measurement for Signature Verification”, thèse de PhD, Hong Kong Baptist University, Septembre 2005.

[20] : B. G. Rajaram, “Characterization and automated verification of handwritten signatures”, thèse de masters,the university of Texas at Arlingston, 1992.

[21] : G. Johansson, “Visual perception of biological motion and a model for its analysis”, Perception& Psychophysics revue, 1973.

[22] : M. H. Cherpin, “Identification biologique des personnes”, Revue de l'ACOMEN, Vol.5, n°3, 1999

[23] : A. J. Jeffreys, V. Wilson et S. L. Thein, “Hypervariable minisatellite ragions in human DNA”, Nature, 314, pp 67-73, 1985.

[24]: H. Guesmi » Identification de personne par fusion de différentes modalités biométriques » ’Université européenne de Bretagne, Janvier 2014

[25] : Alismail MohamedRaouf, Ourchani NorElhouda., "Fusion multimodale des scores pour la reconnaissancedes personnes", Université Mohamed Khider Biskra, 2011.

[26] : S. Hocquet, “Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite”, Thèse de doctorat, Université François Rabelais Tours, 2007.

[27] : M.ARIF Mohammed " Hybridation des Données On/Off-line pour la Vérification des Signatures Manuscrites ", ECOLE MILITAIRE POLYTECHNIQUE, février 2009

[28] : Y.Wang, T. Tan, and A. Jain. “Combining face and iris biometrics for identity verification”. In: Proceedings of Fourth International Conference on Audio- and Video-Based Authentication (AVBPA), pp. 805–813, Guildford, U.K., June 2003.

[29] : J. Kittler, M. Hatef, R. Duin, and J. Matas. “On Combining Classifiers”. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 3,pp. 226–239, 1998.

[30] : Modèles acoustiques à structure temporelle renforcée pour la vérification du locuteur

Embarquée. Par Anthony LARCHER

[31] : Boussafeur Yousra, Yeddiou Idriss., " La biométrie multimodale basée sur la fusion de la reconnaissance de visage et l'empreinte palmaire". Université Larbi Ben M'hidi Oum El Bouaghi, juin 2017.

[32] : R.P. Wilds, « A system for automated iris recognition », Proc. Of 2nd IEEE Workshop on Applications of Computer Vision, pp. 121-128, December 1994.

[34] : https://www.biometrie-online.net/technologies/retine visite le 04-04-2023.

[35] : https://sites.google.com/site/tpelabiometrie/home/biometrie-par-reconnaissance-vocale visite le 04-04-2023

[36] : https://ecolebranchee.com/ameliorer-methode-frappe-au-clavier-conseils/ visite le 04-04-2023

[37] : https://www.chusj.org/fr/soins-services/G/Genetique-medicale/comprendre-genes visite le 04-04-2023

[38] : https://www.researchgate.net/figure/Reconnaissance-biometrique-de-loreille-2930_fig12_289700249 visite le 04-04-2023

[39] : https://www.researchgate.net/figure/Biometric-Zephyr-analysis-http-biometricspbworkscom_fig2_343608500 visite le 04-04-2023

CHAPITRE 02
SECURITE D'INFORMATION

2.1 Introduction :

Aujourd'hui, l'information est la pierre angulaire de l'entreprise. C'est ce qui fait à la fois son existence et sa force. Les informations qui composent la structure et la base d'une entreprise comprennent des fichiers, des bases de données, des méthodes de travail et de fabrication, des fiches de salariés et des informations industrielles. C'est son capital intellectuel, ou plus précisément son capital informationnel. Toute perte d'information peut être mortelle pour une entreprise ou même pour un pays.

La donnée n'aurait plus de raison d'exister car elle ne serait plus exclusive si ces informations venaient à être perdues, volées ou tombées dans les mains d'une autre entreprise. L'information an aujourd'hui de la valeur pour une entreprise en raison de son caractère unique et exclusif. Ainsi, il est dans l'intérêt de l'entreprise de protéger sa propriété intellectuelle. Nous allons essayer de définir et de décrire la sécurité des données.

2.2 Outil de la sécurité de l'information :

Pour définir la sécurité de l'information, il faut étudier ses deux facettes :

- **L'information,** qui peut être présenté en fonction de sa forme de stockage, de traitement ou de transmission. Il peut s'agir d'un morceau de papier, d'un échange oral, d'un classeur, d'une structure numérique combinée à un moyen de transmission par télécommunications.
- **La sécurité,** qui est évaluée à l'aide de différents critères établis qui permettent de qualifier la sécurité d'une information.[1]

2.3 Concept lies à la sécurité :

La sécurité est "la protection de l'information et des systèmes d'information contre tout accès et utilisation non autorisés, divulgation, perturbation, modification ou destruction", selon la définition de S. Zevin dans [3], p. 7. Selon C. Alberts, "la sécurité revient à déterminer ce qui doit être protégé et pourquoi, ce qui a besoin d'être protégé et comment le protéger tant qu'il existe". [5] page 5. Ces définitions démontrent que la sécurité d'un système dépend de sa définition et de son identification de la portée de sécurité sur tous ses composants.

Dès ce qui suit, les besoins de sécurité créent des objectifs de sécurité à atteindre et conduisent à la mise en place de mesures pour améliorer la sécurité d'un système. Les objectifs de sécurité, les mesures de sécurité et les stratégies de développement de systèmes sécurisés sont tous abordés ici.

2.3.1 Les principaux objectifs de sécurité :

- **La confidentialité**

L'objectif de sécurité de la confidentialité est de protéger les informations au repos et lors de l'échange contre toute divulgation et accès non autorisés. Afin de ne donner l'accès qu'à ceux qui sont autorisés, la confidentialité doit être assurée techniquement (mécanismes de chiffrement et de contrôle d'accès) et non techniquement (classification des informations et mise en place de politiques de contrôle d'accès). Cet objectif peut porter sur la protection d'un message élémentaire ou d'un champ spécifique dans un message en utilisant l'objectif support d'authentification et de contrôle d'accès.

Le niveau de confidentialité des informations peut varier. Si certaines informations ne sont pas protégées (informations publiques accessibles à tout le monde), d'autres doivent être plus strictement contrôlées et partagées uniquement avec les partenaires commerciaux, voire n'être accessibles que pour les informations les plus sensibles.

La protection du flot de trafic contre l'analyse est un autre aspect de la confidentialité. Cela signifie qu'un attaquant ne peut pas surveiller le trafic sur un équipement de communication.[5]

- **La disponibilité**

L'objectif de la disponibilité est de garantir à tout moment l'accès à un service, à une information ou à une ressource aux personnes autorisées. La disponibilité est assurée techniquement en garantissant la protection des ressources et des biens (tels que les applications, les systèmes d'hébergement et les équipements réseau) et en garantissant que ces biens fonctionnent correctement. Il est important de garder à l'esprit que la mise en place de procédures et de politiques de sécurité garantit également la disponibilité. En effet, les attaques malveillantes, qui peuvent résulter de la non-respectation des politiques et des procédures de sécurité, peuvent provoquer des dénis de service, ce qui signifie que le service n'est pas disponible. [5]

- **L'intégrité**

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'intégrité désigne la caractéristique qui garantit qu'une information ou un traitement n'a pas été altéré ou détruit de manière non autorisée. Afin d'assurer l'intégrité des informations en transit, il est possible d'utiliser des mécanismes de signature électronique. Quant à l'intégrité des informations au repos, elle est assurée en utilisant des mécanismes de signature appliqués à ces informations, ainsi qu'en vérifiant, par le biais de mécanismes de détection d'intrusion, que les systèmes hébergeant les informations fonctionnent de manière fiable [6].

2.3.2 Les objectif support de sécurité :

Les objectifs de sécurité concernant les supports nécessaires à la réalisation des objectifs de sécurité de base sont succinctement présentés dans le Tableau 2-1. En mettant en place des mécanismes tels que l'identification, l'authentification, l'autorisation et le chiffrement, la confidentialité est garantie. De même, les mécanismes d'authentification, d'audit, de non-répudiation et de signature assurent l'intégrité. Par ailleurs, en implémentant des mécanismes de contrôle d'accès, d'audit, de redondance, de filtrage (pare-feu), etc., la disponibilité est assurée.

Objectifs de sécurité	Description
Identification	Cet objectif permet d'attribuer des identifiants aux utilisateurs ou aux services. En particulier, la fédération d'identité permet à un utilisateur d'utiliser le même identifiant pour divers domaines de confiances. L'identification sert à l'audit et la traçabilité des activités d'un utilisateur ou d'un service.
Authentification	Cet objectif permet de valider l'identifiant d'un utilisateur ou d'un service. Ceci est réalisé en présentant la preuve de possession de l'identité (soumission d'un mot de passe, d'une clé secrète, d'une signature numérique, etc.)
Contrôle d'accès (Autorisation)	Cet objectif permet de contrôler l'accès à l'information et aux systèmes. Pour réaliser ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée avant que les droits d'accès puissent être calculés.
Non-répudiation	Cet objectif empêche aussi bien l'expéditeur que le receveur de nier le fait D'avoir transmis ou reçu une information. Lorsqu'un message est envoyé, le récepteur peut prouver que le message a été bien envoyé par l'expéditeur. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le receveur.
Audit	Cet objectif permet de contrôler le fonctionnement d'un système et de Contrôler les mécanismes de sécurité et de conformité afin de détecter leurs défaillances et les corriger.

Tableau 2-1 : Les objectifs de sécurité de support [5].

2.3.3 Les mesures de sécurité :

Les différentes solutions de sécurité qui pourront être mises en place pour atteindre les objectifs de sécurité sont appelées mesures de sécurité. Les protocoles, les mécanismes et les politiques de sécurité sont les trois catégories de mesures de sécurité selon l'ontologie de sécurité NRL-SO. [7]

1. Les protocoles de sécurité sont définis comme une série d'étapes nécessaires à la réalisation d'une tâche spécifique. Les protocoles fonctionnels qu'ils supportent peuvent être liés à ces protocoles, tels que les protocoles de sécurité liés aux protocoles de routage (IPsec lié

à IP), de transport (SSL/TLS lié à TCP) et d'application (DNSsec lié à DNS). [8]

2. Les mécanismes de sécurité sont les moyens par lesquels les protocoles sont mis en œuvre. Les mécanismes de sécurité réseaux (VPN), des mécanismes systèmes (Safehost) et des mécanismes de services (Parefeu SOAP) sont disponibles. [7]
3. En spécifiant les règles de sécurité à respecter, les politiques gouvernent les mécanismes et les protocoles. Il existe plusieurs types de politiques de sécurité qui peuvent être définis :
   - ✓ Les responsables du secteur établissent les politiques de sécurité du secteur. Les lois sur les droits d'accès à l'information font partie de cette catégorie.
   - ✓ Les architectes logiciels sont responsables de la définition des règles de sécurité pour les applications et les conceptions. Les applications sont conçues en utilisant ces politiques. Par exemple, ces politiques incluent la définition des rôles qui autorisent l'appel d'opérations dans une application.
   - ✓ Les administrateurs du réseau sont responsables de l'établissement des règles de sécurité opérationnelles. Ces politiques sont utilisées dans la gestion de l'infrastructure technique, comme la définition du nombre de tentatives de connexion sur un système informatique. [9]

Il est nécessaire de faire une veille sur les mesures de sécurité existantes et de sélectionner celles qui sont les plus adaptées au contexte métier et technologique de l'entreprise afin de décider quelles mesures de sécurité sont les plus appropriées à mettre en place. Pour protéger la confidentialité des données, par exemple, les mesures de sécurité suivantes pourraient être mises en place :

- ❖ Des réglementations qui définissent les droits d'accès aux données.
- ❖ Des systèmes d'authentification et d'autorisation, tels que le contrôle d'accès mandataire ou le contrôle d'accès basé sur la fonction, tels que le contrôle d'accès mandataire ou le contrôle d'accès basé sur la fonction, sont disponibles.
- ❖ Pour les données en transit, il existe des protocoles de chiffrement tels que les protocoles SSL/TLS. Pour garantir la confidentialité des données, une ou plusieurs de ces instances doivent être choisies et combinées en fonction des contextes métier et technologiques de l'entreprise.

Les techniques de développement de systèmes sécurisés sont abordées dans ce qui suit. En particulier, nous soulignons le concept de patron de sécurité. Un patron de sécurité illustre les différentes mesures de sécurité à prendre pour résoudre un problème connu.

2.3.4 Les stratégies dans le développement de systèmes sécurisés :

La sécurité d'un système dépend de sa conception. Les méthodologies d'analyse des risques, les modèles de conception et les patrons de sécurité peuvent être utilisés pour développer des systèmes sécurisés, qu'ils soient des systèmes d'information, des architectures à base de services ou des applications monolithiques. Le concept de patrons de sécurité est présenté ci-dessous.

De manière générale, un patron fournit une base de connaissances et de compétences pour résoudre des problèmes fréquents dans un domaine spécifique. La description de ces connaissances qui peuvent être réutilisées

1. Permet d'identifier le problème à résoudre en capitalisant et en organisant les connaissances tirées de l'expérience.
2. Propose une solution pour y répondre qui est possible, correcte, générale et consensuelle.
3. Fournit des moyens d'adapter cette solution à une situation particulière [12].

Les patrons obtiennent des informations et des connaissances organisationnelles pour résoudre un problème récurrent en fonction des spécifications du problème. Les patrons de sécurité aident les architectes et les développeurs à partager des connaissances sur la sécurité, à définir un nouveau paradigme de conception ou un style d'architecture et à identifier les risques qui ont été traditionnellement identifiés par prototypage ou par expérience intégrant les visions métier et technologiques de la sécurité [13]. Les exemples de patrons de sécurité sont présentés dans le Tableau 2-2 :

Nom du patron	**Standards and Technologies**	**Description**
Communication sécurisée	HTTPS; SSL (TLS), IP sec	Ce patron de sécurité décrit l'utilisation d'une couche de Transport sécurisée dans le cadre de la communication client-serveur ou serveur-serveur.
Log d'évènements de sécurité	JMX ; Java API for Login	Ce patron de sécurité décrit la traçabilité des Évènements de sécurité pour des raisons d'audit.
Passerelle de sécurité SOA	Intégration de services de sécurité au sein d'un ESB	Pour centraliser la sécurité, des services de sécurité peuvent être connectés à une ESB. En utilisant ce patron, nous pouvons simplifier la propagation des identités, renforcer les politiques, mettre en place des mécanismes d'audit, etc.

Tableau 2-2 : Exemples patterns de sécurité [5].

2.4 Gestion de la sécurité :

La gestion de la sécurité est un processus qui intègre à la fois les aspects organisationnels et technologiques dans le but d'assurer la sécurité. Ce processus permet d'identifier les actifs à protéger et de développer des stratégies de protection contre les menaces potentielles. L'objectif principal de la gestion de la sécurité est d'aligner les besoins de sécurité et de définir une stratégie globale pour garantir le niveau de sécurité requis pour les informations et les systèmes

d'information de l'entreprise. Dans son cadre général de sécurité, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France a établi six principes fondamentaux pour la gestion de la sécurité des systèmes d'information. [2] :

1. **Adapter une démarche globale**

L'objectif est que la stratégie de sécurisation des systèmes d'information soit cohérente dans son ensemble. Pour éviter toute faille qui compromettrait la sécurité globale du système d'information, il convient à ce titre de garder à l'esprit tous les aspects pertinents.

2. **Adapter la sécurité du système d'information selon les enjeux**

Il est préconisé d'adapter la sécurité du système d'information en fonction des enjeux spécifiques du système et des besoins de sécurité, de manière à allouer les ressources financières et humaines nécessaires, mais également suffisantes.

3. **Gérer les risques**

Il est nécessaire de mener une approche consistant à :

1) Déterminer l'ensemble des risques qui pèsent sur le système.
2) Fixer des objectifs de sécurité pour répondre proportionnellement aux besoins de protection du système et des informations face aux risques identifiés.
3) Déterminer les fonctions de sécurité et leur niveau de mise en œuvre nécessaires à l'atteinte de ces objectifs.

4. **Elaborer une politique de sécurité du système d'information (SSI)**

La création d'une stratégie de sécurité globale vise à définir les conditions d'utilisation du système d'information. Les rôles et les responsabilités des différents acteurs, les règles d'utilisation des systèmes et des informations, les mesures de contrôle d'accès à l'information, les règles de protection des données privées, les directives d'audit et de sauvegarde, et bien d'autres sont définis par les politiques.

5. **Utiliser les produit et prestataires labellises pour leur sécurité**

La certification des produits ou des prestataires permet de garantir la confiance accordée aux produits de sécurité et à la compétence des professionnels en matière de sécurité des systèmes d'information (SSI). Elle atteste que les produits répondent à des normes de sécurité établies et démontre la compétence des prestataires dans ce domaine.

6. **Viser une amélioration continue**

Il est suggéré d'améliorer constamment la sécurité des systèmes d'information (SSI). Un "système de gestion de la sécurité des données" (SMSI) est généralement utilisé pour planifier, mettre en œuvre, vérifier et améliorer les mesures de sécurité. Le SMSI permet de renforcer la sécurité en suivant un processus évolutif de gestion des risques et en s'adaptant aux évolutions technologiques et aux nouvelles menaces.

2.4.1 Les standards dans la gestion de sécurité :

Le standard ITSEC dl 'Union Européenne :

Le critère d'évaluation standard de la sécurité de l'information technologique (ITSEC) de l'Union européenne a été créé en 1991 dans le but de renforcer les processus de certification de sécurité des États partenaires [14]. Huit groupes de critères décrivent les exigences en termes de "cible de sécurité" (c'est-à-dire le niveau de certification visé) : identification et authentification, contrôle d'accès, imputabilité, réutilisation d'objets, fidélité, continuité de service, échange de données (incluant l'authentification, le contrôle d'accès, la confidentialité des données, l'intégrité des données et la non- Afin de créer un système d'information sécurisé, ces critères sont classés en neuf familles en fonction du cycle de vie du projet : étude des besoins, conception de l'architecture, conception détaillée, mise en œuvre, configuration et contrôle, langages de programmation et compilateurs, sécurité pour les développeurs, documentation "opérationnelle" et environnement opérationnel.

Cependant, ce standard ne prend pas réellement en compte les aspects organisationnels, malgré le but de l'ITSEC de fournir une analyse globale du système de support du système d'information. L'accent est principalement mis sur les contraintes de conception, de développement et de mise en œuvre des ressources informatiques plutôt que sur l'adaptation de l'organisation aux exigences de la politique de sécurité. De plus, ces normes ne tiennent pas compte des éléments de sécurité d'un réseau ou d'un système informatique [15].

Les 'Common citerai' :

Le standard "Common Criteria" (CC) définit à la fois des critères et une méthode d'évaluation afin d'assurer une certification cohérente au niveau international du niveau de sécurité atteint par les systèmes des partenaires dans un environnement distribué. Ce standard est basé sur deux idées principales :

Le profil de protection (PP) représente tous les besoins et objectifs de sécurité d'une catégorie de produits ou de systèmes.

La cible de sécurité (Security Target : ST) décrit les objectifs de sécurité et les exigences liées à une "cible d'évaluation".

Ce standard est innovant parce qu'il repose sur un modèle de gestion des risques qui intègre plusieurs idées. Les risques sont liés aux biens et sont identifiés en combinant les menaces et les vulnérabilités. La réduction des risques consiste à mettre en place des contre-mesures pour

diminuer les vulnérabilités et ainsi réduire la possibilité qu'elles soient exploitées par des menaces. Ce modèle met également l'accent sur la responsabilité des propriétaires dans la définition de la valeur des biens et des contraintes, ce qui permet d'intégrer les contraintes organisationnelles dans la définition des objectifs de sécurité. La conformité de la cible (ST) par rapport à un ou plusieurs profils de sécurité (PP) est vérifiée par la méthode d'évaluation proposée.

Cependant, ce standard ne tient pas compte de la dimension organisationnelle et se concentre principalement sur la certification des composants.[16]

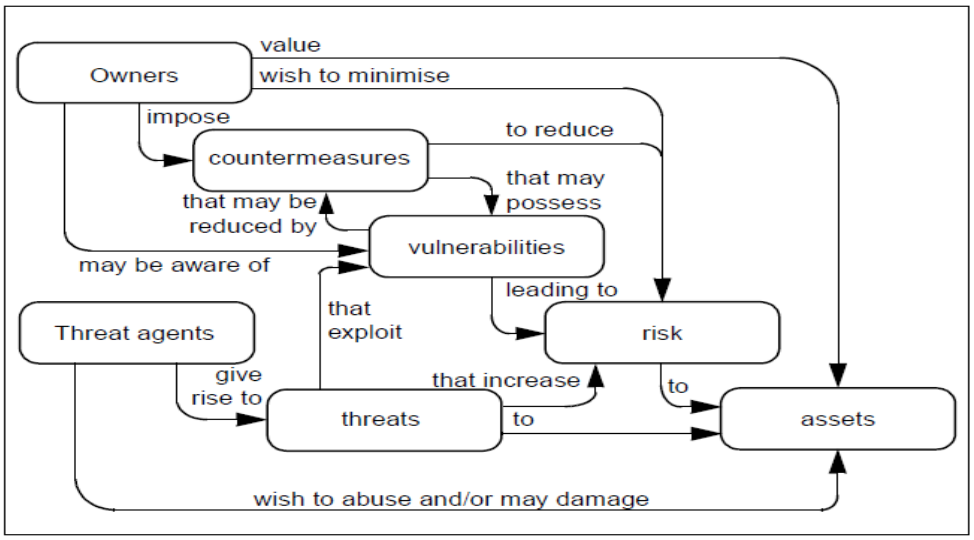


Figure 2-1 : Modèle de concepts de sécurité [16] p. 13

Les standards de l'ISO :

La CEI et l'ISO (Commission électrotechnique internationale) ont publié les normes ISO27001/ISO27002 (anciennement ISO 17799) [17]. Ces normes définissent les principes et les lignes directrices pour la création, la mise en œuvre, la maintenance et l'amélioration de la gestion de la sécurité. Contrairement aux spécifications précédentes, la sécurité est désormais considérée au niveau organisationnel et technologique. Les fonctions offertes par ces normes sont répertoriées dans le Tableau 2-3 :

ISO 27001	Gestion de la responsabilité
	Audit Interne
	Amélioration de l'ISMS (Information Security Management System)
	Elaboration d'une politique de sécurité

	Organisation de la sécurité des informations
	Gestion des biens et des actifs
	Sécurité physique et environnementale
	Communications et la gestion des opérations
	Contrôle d'accès
	Systèmes d'acquisition de l'information
	Développement et maintenance
	Gestion des incidents de sécurité des informations
	Gestion de la continuité
	Conformité

Tableau 2-3 : Fonctions ISO 27001 / ISO 27002 [17].

Les normes ISO27001/ISO27002 font partie d'une série de normes ISO sur la gestion de la sécurité :

- ✓ Les directives pour l'évaluation d'un système de gestion de sécurité sont fournies par le standard ISO27004.
- ✓ Les directives pour la gestion des risques dans une entreprise sont fournies par le standard ISO27005.
- ✓ Les règles d'accréditation des organismes de certification ISO sont fournies par le standard ISO27006.

Le cadre FISMA du NIST

Le FISMA (Federal Information Security Management Act) et d'autres normes de mise en œuvre de la gestion de la sécurité similaires ont été créées dans une approche similaire par le NIST (National Institute of Standards and Technology) [18].

Le FISMA, un cadre de gestion composé de plusieurs documents, a été créé par NIST pour protéger les systèmes d'information. La création d'un plan de gestion de la sécurité est l'objectif principal du cadre FISMA. La portée de ce cadre est résumée dans le Tableau 2-4 :

Standards pour la catégorisation de l'information et des systèmes d'information.
Standards des exigences de sécurité minimales pour l'information et les systèmes d'information.
Directives pour la sélection des contrôles de sécurité appropriés aux systèmes d'information.
Guide pour l'évaluation des contrôles de sécurité dans les systèmes d'information et de la détermination de l'efficacité du contrôle de sécurité.
Directives pour la certification et l'accréditation des systèmes d'information.

Tableau 2-4 : Portée du cadre FISMA [18]

Parmi les références du cadre FISMA, voici les documents centraux :

- NIST 800-30 : Guide de gestion des risques pour les systèmes d'information.
- NIST 800-53 : Guide des contrôles de sécurité dans les systèmes d'information.
- FIPS 199 (Federal Information Processing Standard 199) : Normes pour la catégorisation de l'information et des systèmes d'information.

Bien que le cadre FISMA soit axé sur les systèmes en développement et que les normes ISO soient davantage destinées aux systèmes en production, nous avons constaté que ces deux cadres présentent des similitudes significatives dans la gestion de la sécurité :

- Les deux cadres reposent sur un processus de développement : l'ISO recommande le processus PDCA (Plan - Do - Check - Act), tandis que le FISMA propose un cycle de développement plus traditionnel (initialisation, développement, acquisition/implémentation, opération et maintenance).
- Les deux cadres accordent une importance centrale à la gestion des risques.
- Les deux cadres soulignent l'importance de l'implication des responsables métier dans l'étude, la mise en œuvre et le suivi de la gestion de la sécurité.

Les cadres ITSec, ISO et FISMA sont reconnus pour la gestion de la sécurité des systèmes d'information, mais ils ne conviennent pas à la gestion de la sécurité dans un environnement de services distribués et collaboratifs. Ils ne fournissent pas de plateforme intégrée pour intégrer les exigences de sécurité dans les modèles de processus de l'entreprise. En mettant l'accent sur la collaboration et l'intégration entre les partenaires, il est nécessaire de développer de nouveaux cadres pour relever les défis spécifiques de la sécurité dans les environnements de services distribués. Pour garantir la sécurité des échanges et des transactions entre les différentes parties prenantes, ces nouvelles méthodes doivent fournir des mécanismes et des outils appropriés.

2.4.2 Les processus d'implémentation de la gestion de la sécurité :

La gestion de la sécurité implique des études et des processus sur la gouvernance de la sécurité, la gestion des risques et l'organisation. Cela inclut la création d'un plan de continuité des activités pour répondre aux besoins de sécurité tout au long du cycle de vie du système d'information et des projets associés. Ces efforts visent à garantir la disponibilité et l'intégrité des données et des processus critiques, ainsi que la protection et la résilience des systèmes d'information. La gestion de la sécurité est une approche holistique qui nécessite une collaboration et une coordination étroites entre les différentes parties prenantes, y compris les responsables métier, les experts en sécurité et les équipes techniques.[20]

La gouvernance de la sécurité :

Le processus de gestion d'une stratégie de sécurité globale est appelé gouvernance de la sécurité. La planification et la détermination des priorités dans l'utilisation des ressources de

l'entreprise sont parmi ses fonctions principales. Cela comprend l'établissement du budget, l'allocation des ressources et le soutien aux décisions prises dans le processus de gestion des risques. Selon la spécification 800-39 du NIST, le processus de gestion des risques est composé des éléments suivants :

- L'alignement stratégique des décisions de gestion des risques sur la mission et les objectifs organisationnels de l'entreprise
- Vérifier l'application du processus de gestion des risques et attribuer les ressources nécessaires.
- Vérifier que la mise en œuvre du processus de gestion des risques respecte les objectifs organisationnels et commerciaux.

La gouvernance de la sécurité permet de garantir que la gestion des risques est alignée sur les objectifs de l'entreprise et soutenue par les ressources nécessaires. De plus, elle garantit que les décisions prises dans le processus de gestion des risques sont cohérentes avec les objectifs commerciaux et organisationnels.

Le plan pour suite d'activité :

En préparant à l'avance la continuité des activités stratégiques, le plan de poursuite d'activité vise à garantir la survie de l'entreprise. Il comprend un plan de secours informatique qui garantit la reprise des systèmes identifiés comme critiques dans un délai minimum et la récupération des données avec une perte minimale.

La direction de l'entreprise et l'analyse des risques sont nécessaires pour créer un plan de secours informatique.

- Analyse de l'impact de l'indisponibilité des activités sur les objectifs de l'entreprise.
- Choisissez des stratégies de récupération en fonction des besoins de l'entreprise en termes de métier et de technologie.
- Créer un plan de reprise des activités et des plans de récupération en réponse aux scénarios de risque.
- Sensibiliser les parties prenantes aux scénarios de risque afin qu'elles puissent agir.
- Vérification du plan d'action pour assurer la continuité des activités.

La préparation de l'entreprise aux incidents et la reprise rapide et efficace des activités essentielles sont les objectifs du plan de poursuite d'activité. Il est basé sur une évaluation approfondie des risques et la mise en place de mesures appropriées pour réduire les perturbations et les pertes en cas d'incident.

2.5 Conclusion :

Le chapitre aborde les concepts de sécurité en soulignant l'importance de comprendre les besoins et objectifs de l'entreprise, car ils influencent grandement les mesures de sécurité mises en place. Il est donc essentiel d'identifier ces objectifs pour pouvoir mettre en œuvre des mesures de sécurité adaptées à la situation spécifique de l'entreprise.

En résumé, la compréhension des concepts de sécurité, l'élaboration d'une stratégie de sécurité adaptée et la gestion des risques sont des éléments essentiels pour assurer la sécurité des systèmes d'information dans différents environnements, y compris les environnements distribués et dynamiques.

Bibliographie

[1] : ANSSI. EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité. [En ligne]. 2010. Disponible sur : < http://www.ssi.gouv.fr/ > (consulté le 5 mai 2023)

[2] : ANSSI. Référentiel généralde la sécurité. [En ligne]. Disponible sur : <http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/ > (consulté le 2 mai 2023)

[3] : NIST. Standards for Security Categorization of Federal Information and Information Systems. [En ligne]. 2004. Disponible sur : < http://csrc.nist.gov > (consulté le 10 mai 2023)

[4] : Alberts C. Managing information security risks : the OCTAVE approach. Boston : Addison-Wesley, 2003. ISBN : 9780321118868.

[5] : Stallings W. Sécurité des réseaux : applications et standards. Paris : Vuibert, 2002. ISBN : 9782711786534.

[6] : ANSSI. Agence nationale de la sécurité des systèmes d'information. [Enligne].Disponible sur : < http://www.ssi.gouv.fr/ > (consulté le 5 mai 2023)

[7] : Kim A., Luo J., Kang M. « Security ontology for annotating resources ». On the Move toMeaningful Internet Systems 2005: CoopIS, DOA, and ODBASE. 2005. p. 1483–1499.

[8] : Schneier B. Applied cryptography : protocols, algorithms, and source code in C. 2nd ed.New York : Wiley, 1996. ISBN : 9780471128458.

[9] : BUECKER A. et al. Understanding SOA Security Design and Implementation. [Enligne2007.Disponible sur : <http://www.redbooks.ibm.com/abstracts/sg247310.html > (consulté le 5 mai 2023)

[10] : Samarati P., De Vimercati S. « Access control: Policies, models, and mechanisms ».Foundations of Security Analysis and Design. 2001. p. 137–196.

[11] : Ferraiolo D., Cugini J., Kuhn D. R. « Role-based access control (RBAC): Features and motivations ». In : Proceedings of 11th Annual Computer Security Application Conference. Washington : IEEE Computer Society Press, 1995. p. 241–48.

[12] : Hachani wafa. Patrons de conception à base d'aspects pour l'ingénierie des systèmes d'information par réutilisation. Thèse Doctorat. GRENOBLE : Université Joseph Fourier,2006.

[13] : Steel C. Core security patterns best practices and strategies for J2EE, Web services, and identity management. Upper Saddle River, NJ : Prentice Hall PTR, 2006. ISBN :9780131463073.

[14] : EEC, Information Technology Security Evaluation Criteria (ITSEC), RapportTechnique. [En ligne]. Disponible sur : <http://csrc.nist.gov/publications/secpubs/itsec.txt> (consulté le 5 mai 2023)

[15] : MATHIEU H. Modélisation conjointe de l'infrastructure et des processus pour l'administration pro-active de l'entreprise distribuée. Thèse Doctorat. Lyon : INSA de Lyon, 2004. 252 p.

[16] : ISO/IEC. Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and generalmodel . [En ligne]. 1998.Disponible sur : < www.commoncriteriaportal.org > (consulté le 5 mai 2023)

[17] : ISO/IEC, The International Organization for Standardization and The International Electrotechnical Commission. ISO/IEC 27002:2005. [En ligne]. 2005. Disponible sur :

[18] : NIST. Federal Information Security Management Act (FISMA) Implementation Project. [En ligne]. Disponible sur :<http://csrc.nist.gov/groups/SMA/fisma/index.html (Consulté le 5 mai 2023)

[19] : Biennier F., Mathieu H. « Technical Solutions vs. Global BPR Investment ». Schedae Informaticae. 2005. Vol. 14, p. 13-34.

[20] : Vacca J. Managing information security. Burlington MA : Elsevier, 2010. ISBN :9781597495332.

CHAPITRE 03
CRYPTAGE ET CRYPTOGRAPHIE

3.1 Introduction :

La cryptographie est effectivement une science ancienne qui remonte à l'Antiquité. Des exemples historiques de l'utilisation de techniques de cryptographie à des fins militaires incluent l'utilisation de hiéroglyphes non conformes à la langue pour écrire des messages secrets en Égypte antique.

De nos jours, la cryptographie est essentielle aux réseaux informatiques. Il sert de mécanisme essentiel pour garantir la confidentialité des données numériques. La cryptographie garantit la confidentialité des données car elle permet de transformer un message en un format illisible pour quiconque n'a pas la clé de déchiffrement appropriée.

Ce chapitre présente les concepts fondamentaux de la cryptographie. Cela comprend des idées comme les algorithmes de chiffrement, les clés de chiffrement, les fonctions de hachage, les signatures numériques et d'autres mécanismes cryptographiques utilisés pour protéger les données dans les environnements informatiques.

La cryptographie est un domaine en constante évolution, avec de nouvelles techniques et algorithmes développés pour faire face aux défis de sécurité croissants. Les professionnels de la sécurité informatique doivent comprendre les bases de la cryptographie afin de concevoir et de mettre en œuvre des solutions de sécurité efficaces dans les réseaux et les systèmes d'information.

3.2 Terminologie :

- **Texte en clair** : Il s'agit du message original à protéger.
- **Texte chiffré** : C'est le résultat obtenu après avoir appliqué un algorithme de chiffrement au texte en clair.
- **Chiffrement** : C'est le processus utilisé pour transformer un texte en clair en texte chiffré, généralement à l'aide d'un algorithme et d'une clé.
- **Déchiffrement** : C'est le processus inverse du chiffrement, utilisé pour récupérer le texte en clair à partir du texte chiffré, en utilisant la clé appropriée.
- **Clé** : Il s'agit d'un secret partagé utilisé dans le processus de chiffrement et de déchiffrement. La clé est nécessaire pour rendre le texte chiffré illisible et pour le ramener au texte en clair. Il peut s'agir d'une série de caractères ou d'un

algorithme spécifique.

- **Cryptographie** : C'est le domaine qui englobe les méthodes et techniques utilisées pour chiffrer et déchiffrer les messages afin de les rendre confidentiels pour ceux qui ne possèdent pas la clé appropriée.
- **Cryptanalyse** : C'est l'art de décrypter un texte chiffré sans avoir connaissance de la clé utilisée. La cryptanalyse consiste à trouver des faiblesses dans les méthodes de chiffrement pour récupérer le texte en clair.
- **Cryptologie** : Il s'agit de la science qui étudie les communications secrètes. Elle comprend à la fois la cryptographie (étude du chiffrement) et la cryptanalyse (étude du décryptage).
- **Décrypter** : C'est l'action de retrouver le texte en clair à partir du texte chiffré sans avoir la clé correspondante. Ce terme est généralement utilisé dans le contexte de la cryptanalyse.
- **Crypter** : Après avoir examiné la définition de décrypter, il est clair que le terme "crypter" n'a pas de sens précis. Il est préférable de l'éviter. De même, le terme "cryptage" n'a pas de sens clair.
- **Coder, décoder** : Ce sont des termes utilisés pour décrire le processus de modification de la structure d'un message sans y introduire d'éléments secrets. [1]

3.3 Définition de la cryptographie :

La cryptographie est une discipline qui comprend le chiffrement et le code des messages et est devenue une discipline complète. En combinant les domaines des mathématiques, de l'informatique et parfois même de la physique, elle permet de répondre à un besoin fondamental des sociétés : la protection du secret. Il est parfois nécessaire de dissimuler des informations sensibles pour éviter les conflits ou protéger une population.[4]

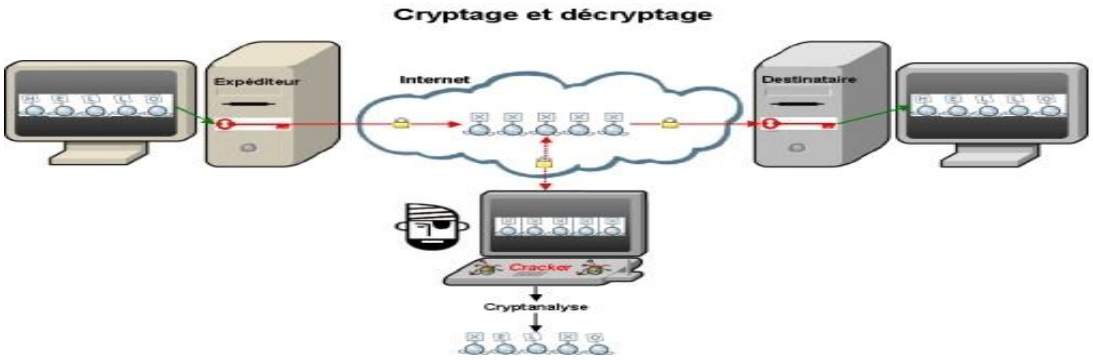


Figure 3-1 : schéma de cryptographie

3.4 But de cryptographie :

Aux yeux de certains utilisateurs, la cryptographie est généralement utilisée pour dissimuler des messages. Aujourd'hui, cette utilisation est d'autant plus importante que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. De nos jours, la cryptographie sert à protéger la confidentialité des données et à garantir leur authenticité et leur intégrité.

- **La confidentialité** : consiste à rendre l'information compréhensible à d'autres que les acteurs de la transaction.
- **L'intégrité** : La vérification de l'intégrité des données consiste à s'assurer que les données n'ont pas été altérées pendant la transmission..
- **L'authentification :** Afin d'assurer l'identité d'un utilisateur, chaque correspondant doit s'assurer que l'interlocuteur qu'il entretient est bien la personne qu'il prétend être. Il est possible de mettre en place un contrôle d'accès, par exemple en utilisant un mot de passe crypté. Ce contrôle d'accès limite l'accès aux ressources aux personnes autorisées.
- **Le non répudiation :** des informations garantit qu'aucune des parties ne peut nier sa participation ou son implication dans une transaction. En fournissant des preuves incontestables de l'implication de chaque correspondant, cela prévient les contestations ultérieures.[4]

3.5 Mécanisme de la cryptographie :

Une fonction mathématique appelée algorithme de cryptographie est utilisée pour chiffrer et déchiffrer des données. Une clé, qui peut être un mot, un nombre ou une phrase, l'accompagne. Les résultats de chiffrement varient selon l'utilisation de différentes clés. L'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé utilisée garantissent la sécurité des données cryptées.

L'algorithme de cryptographie lui-même, ainsi que les clés et les protocoles nécessaires à son fonctionnement, constituent un système de cryptographie.[3]

Qu'entend-on par clé ? :

Une valeur utilisée pour chiffrer des données est appelée clé dans un algorithme de cryptographie. Dans la plupart des cas, elle est représentée par un nombre complexe mesuré en bits. Une clé de taille plus grande protège le système. Cependant, la sécurité dépend d'un mélange d'algorithmes complexes et de clés de grande taille.

Les clés doivent être stockées de manière sécurisée afin que seuls les propriétaires puissent y accéder et les utiliser.[3]

3.6 Les déférents algorithmes de cryptage et décryptage :

Les méthodes de cryptage peuvent être classées en deux catégories.

3.6.1 Méthodes de cryptage Classiques :

3.6.1.1 Cryptage par substitution :

Dans la cryptographie, les substitutions sont la substitution de symboles ou de groupes de symboles par d'autres symboles ou groupes de symboles. La substitution mono-alphabétique et poly-alphabétique sont les deux options disponibles.

1) Substitution mono-alphabétique :

Consiste à remplacer chaque alphabet clair par un autre alphabet codé.

Texte clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Texte codé	W	X	E	H	Y	Z	T	K	C	P	J	I	U	A	D	G	L	Q	M	N	R	S	F	V	B	O

Tableau 3-1 : substitution mono-alphabétique

•Exemple :

Texte claire «la cryptographie»
Texte Crypté «iweqbgndtqwgkcy»

2) Substitution poly-alphabétique :

La substitution poly-alphabétique consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans plusieurs alphabets aléatoires associés. Une clé est utilisée pour déterminer l'ordre séquentiel de lecture des caractères dans la grille poly-alphabétique. En utilisant la clé associée dans l'ordre séquentiel et en répétant la clé si nécessaire, on peut consulter la grille pour chiffrer un caractère. Les algorithmes de chiffrement bien connus utilisent ce principe, tels que les algorithmes de Vigenère et de Beaufort.

L'utilisation d'une fonction de ou exclusif (XOR) est une illustration facile du principe de substitution poly-alphabétique.

3.6.1.2 Cryptage par transposition :

Les transpositions consistent à combiner des symboles ou des groupes de symboles d'un message clair selon des règles préétablies pour créer de la diffusion. La clé de chiffrement fixe ces règles. Une permutation est une succession de transpositions.

3.6.1.3 Cryptage par produit :

Il combine le chiffrement par transposition et le déchiffrement par substitution. Les algorithmes à clés symétriques utilisent généralement le chiffrement par produit. Lorsque les deux transformations (substitution et transposition) sont effectuées une fois, on dit qu'un « tour » est terminé. Les réseaux S-P de Shannon sont également appelés à la suite de ces successions de rondes.[2]

3.6.2 Méthodes de cryptage Modernes :

On distingue deux méthodes majeures de cryptage modernes :

- ✓ Les méthodes clef secrète (symétriques).
- ✓ Les méthodes clef publique/clef privée (asymétriques).

3.6.2.1 Algorithmes symétriques (clef secrète) :

Un algorithme symétrique est un algorithme qui utilise une clé pour chiffrer un texte en clair et la même clé pour déchiffrer le texte chiffré en texte en clair.

La clé utilisée pour chiffrer et déchiffrer les messages dans les algorithmes symétriques est effectivement essentielle pour garantir la confidentialité de la communication. Le secret se trouve dans la clé, tandis que l'algorithme lui-même est généralement connu du grand public. Étant donné que la même clé est utilisée symétriquement pour chiffrer et déchiffrer un message, on les appelle des algorithmes symétriques.

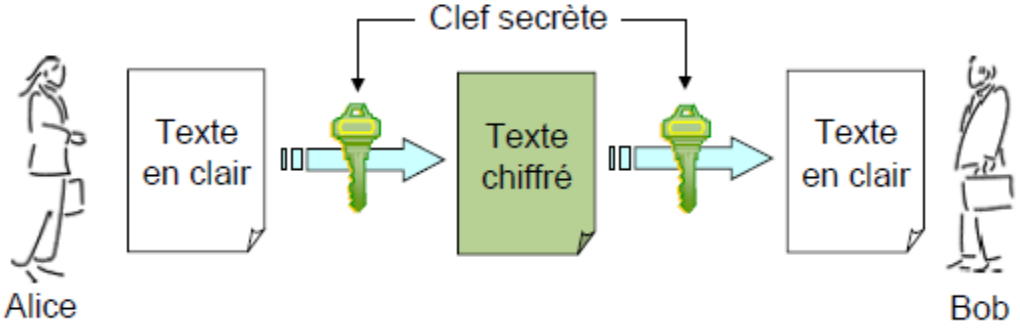


Figure 3-2 : principe de l'algorithme symétrique [7]

Les algorithmes symétriques sont de deux types :

- Les algorithmes de chiffrement en continu, qui agissent sur le message en clair un bit à la fois.
- Les algorithmes de chiffrement par bloc, qui opèrent sur le message en clair par groupes de bits appelés bloc. [3]

Algorithmes de chiffrement en continu :

qui travaillent sur le message à la fois. L'opération XOR est utilisée pour générer un flux pseudo aléatoire et le combiner avec les informations bit à bit. L'information est restituée par le même mécanisme à la réception.

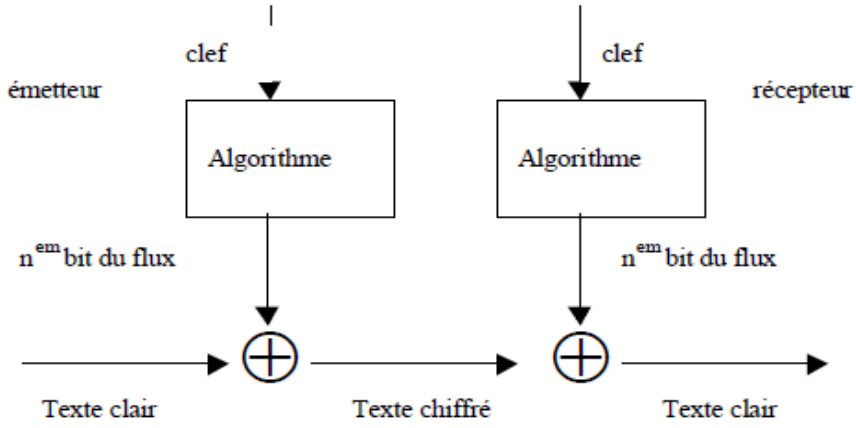


Figure 3-3 : chiffrement en continu

– **Algorithmes de chiffrement par bloc :**

Qui opèrent sur le message en clair par groupe de bit. La taille typique des blocs est 64 bits, ce qui est assez grand pour interdire l'analyse et assez petit pour être pratique

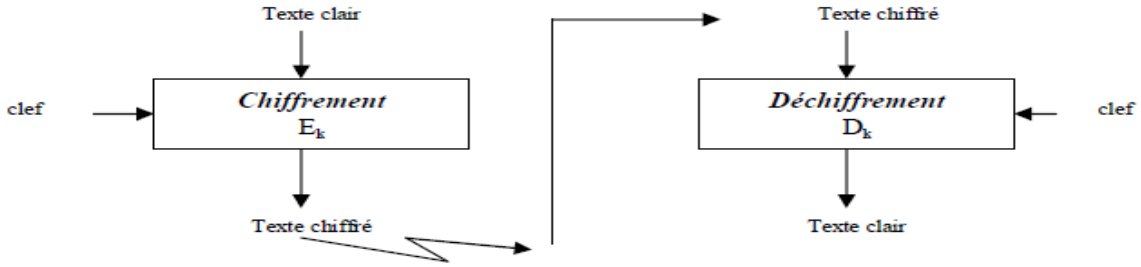


Figure 3-4 : chiffrement par bloc

Les algorithmes de chiffrement par blocs peuvent être utilisés suivant différents modes, dont les deux principaux sont le mode ECB (Electronique Code Boock) et le mode CBC (Chipher Block Haining).[3]

1-Le mode ECB (Electronique Code Book) :

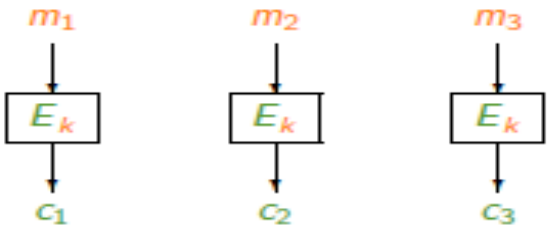


Figure 3-5 : le mode ECB

- **Chiffrement :** Chaque bloque clair m_i est chiffré indépendamment et donne un bloc chiffré

$$c_i = E_k(m_i)$$

- **Déchiffrement :** Chaque chiffré est déchiffré indépendamment pour donner le clair correspondant

$$m_i = D_k(c_i)$$

Avantage : Ce mode permet le chiffrement en parallèle des différents blocs composant un message.

Inconvénient : Même bloc de message en clair sera toujours chiffré en un même bloc de message chiffré. Or, dans le chiffrement sur un réseau par exemple, les données à chiffrer ont des structures régulières facilement repérables par un cryptanalyse, qui pourra donc obtenir beaucoup d'informations. D'autre part, un attaquant actif pourra facilement manipuler les messages chiffrés en retirant, répétant ou inter changeant des blocs. Un autre inconvénient qui s'applique au chiffrement par blocs en général, est l'amplification d'erreur : si un bit du message chiffré est modifié pendant le transfert, tout le bloc de message en clair correspondant sera faux.[5]

2-Le mode CBC (Cipher Block Chaining) :

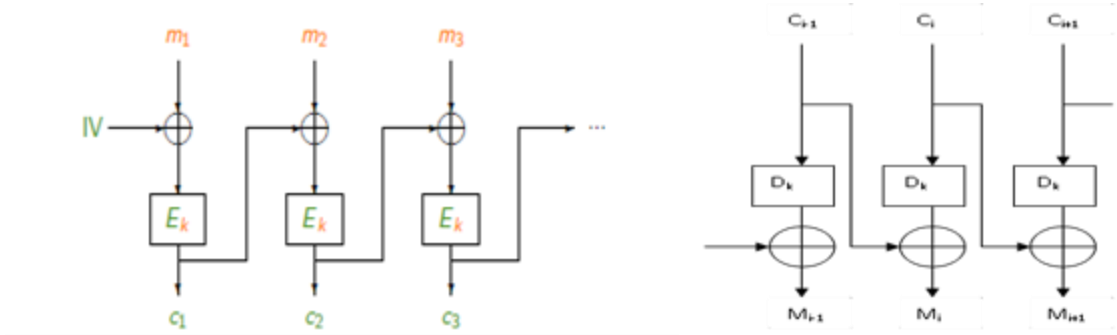


Figure 3-6 **:** Chiffrement et Déchiffrement CBC

- **Chiffrement :** Un vecteur d'initialisation IV est généré aléatoirement

$$Ci = Ek\ (Mi + Ci\text{-}1).$$

Le vecteur IV est transmis avec les blocs chiffrés.

- **Déchiffrement :** $M_i = C_{i-1} + D_k(C_i)$.

Avantage : La structure du message en clair est masquée par le chaînage. Un attaquant ne peut plus manipuler le cryptogramme, excepté en retirant des blocs au début ou à la fin. Un inconvénient est qu'il n'est plus possible de paralléliser le chiffrement des différents blocs (le déchiffrement reste parallélisé blé).

Inconvénient : On pourrait craindre que le chaînage de bloc n'entraîne une propagation d'erreur importante. De fait, une erreur d'un bit sur le message en clair affectera tous les blocs

chiffrés suivants. Par contre, si un bit du message chiffré est modifié au cours du transfert, seul le bloc de message en clair correspondant et un bit du bloc de message en clair suivant seront endommagés : le mode CBC est dit auto réparatrice.[5]

Exemple algorithmes symétrique :

Chiffrement par bloc :

		DES	3DES	IDEA	RC4	RC5 et RC6	Blowfish	AES
Nom réel		Data Encryption Standard	Triple Data Encryption Standard	International Data Encryption Algorythm	Rivest Cipher 4	Rivest Cipher 5/6	Blowfish	Advanced Encryption Standard
Date		1973	1978	1992	1987	1994	1993	1998
Longueur	**Clé**	64 bits (56 effectifs)	192 bits (168 effectifs)	128 bits	jusqu'a 256 bits	entre 0 et 2040 bits	entre 40 et 448 bits	128, 192, 256 bits
	Bloc	64 bits	64 bits	64 bits	Flux	32, 64, 128 bits	64 bits	128 bits

3.6.2.2 Algorithme asymétriques (clef publique) :

Bien que les algorithmes symétriques observés soient fiables, il existe un problème lié à l'échange de clé : comment puis-je transmettre de manière fiable la clé de chiffrement utilisée pour chiffrer le message que je lui envoie? Bien sûr, il y a le téléphone, mais il y an aussi les écoutes.

Les algorithmes asymétriques ont été créés pour résoudre le problème de la transmission sécurisée de la clé.

Étant donné que la clé utilisée pour le chiffrement et le déchiffrement n'est pas la même, on parle d'algorithmes asymétriques. Les algorithmes utilisent des clés privées et publiques. Une fonction mathématique complexe relie les deux clés, la clé privée et la clé publique.

Les algorithmes asymétriques possèdent 2 modes de fonctionnement :

- Le mode chiffrement dans lequel l'émetteur chiffre un fichier avec la clé publique du destinataire pour chiffrer. Le destinataire utilise sa clé privée pour déchiffrer le fichier.
- Dans ce mode, l'émetteur est sûr que seul le destinataire peut déchiffrer le fichier.

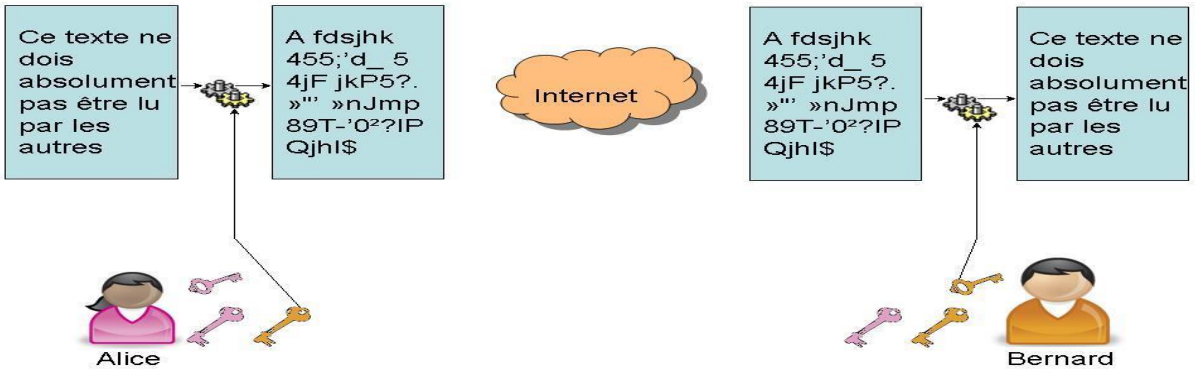


Figure 3-7 : chiffrement avec l'algorithme asymétrique [2]

- Le mode signature dans lequel l'émetteur signe un fichier avec sa propre clé privée. Le destinataire utilise la clé publique de l'émetteur pour vérifier la signature du fichier. Dans ce mode, le destinataire est sûr que c'est bien l'émetteur qui a envoyé le fichier.

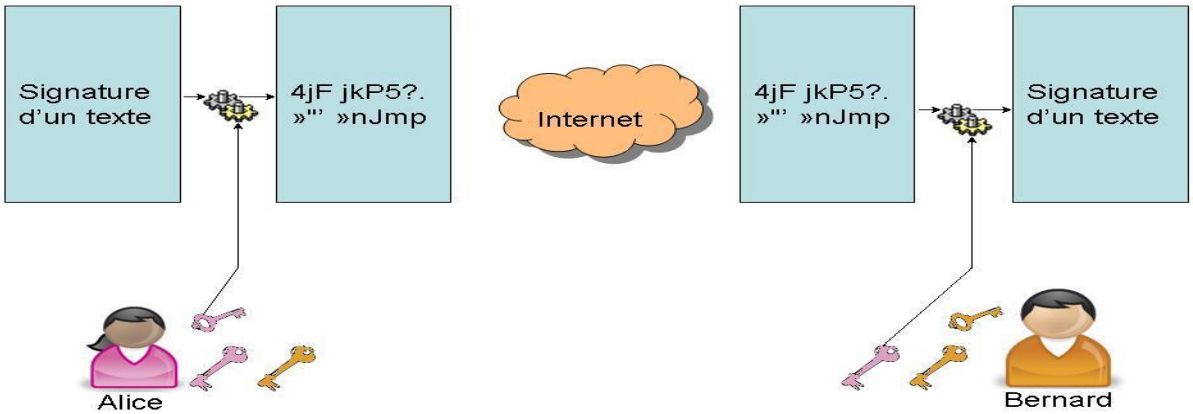


Figure 3-8 : signature avec l'algorithme asymétrique [2]

Donc pour résumer :

- L'émetteur chiffre avec la clé publique du destinataire, le destinataire déchiffre avec sa clé privée.
- L'émetteur signe avec sa clé privée, le destinataire vérifie la signature avec la clé publique de l'émetteur.[3]

3.7 Introduction aux système chaotique en cascade (CCS) :

Le système chaotique en cascade (CCS) est une approche innovante utilisée dans le domaine de la cryptographie pour renforcer la sécurité des communications. Ce concept repose sur l'utilisation de plusieurs systèmes chaotiques interconnectés, formant une cascade de chiffrement. Chaque système chaotique génère une séquence de nombres aléatoires complexes et imprévisibles, qui est utilisée pour chiffrer les données [9].

L'avantage principal du CCS réside dans sa capacité à produire des résultats hautement chaotiques et à rendre les données chiffrées résistantes aux attaques cryptographiques. En combinant les sorties de plusieurs systèmes chaotiques, le CCS crée un niveau supplémentaire de complexité et de non-linéarité, ce qui rend extrêmement difficile pour un attaquant de récupérer les données originales sans la clé de déchiffrement appropriée [9].

De plus, le CCS offre une forte sensibilité aux conditions initiales et aux paramètres de chaque système chaotique, ce qui signifie qu'une légère modification de ces valeurs peut entraîner une modification significative de la séquence de chiffrement. Cela renforce la sécurité du système en rendant les attaques par force brute ou par recherche exhaustive inefficaces [9].

En outre, le CCS offre une bonne diffusion et dispersion des données, ce qui signifie que des modifications mineures dans les données d'entrée se propagent de manière aléatoire et complexe dans les données chiffrées, rendant toute corrélation ou modèle difficile à détecter [9].

Cependant, il est important de noter que la mise en œuvre d'un système chaotique en cascade nécessite une attention particulière aux aspects de synchronisation et de gestion des clés [9]. La synchronisation précise des systèmes chaotiques et la gestion adéquate des clés sont essentielles pour garantir la sécurité et la fiabilité du CCS.

3.8 Les cartes chaotiques traditionnelles :

Plusieurs systèmes chaotiques différents sont utilisés pour créer des cartes chaotiques :

3.8.1 La Carte Logistic :

La carte Logistic est une carte chaotique discrète 1-D largement utilisée dans de nombreuses applications. Il a été prouvé qu'il avait de bonnes performances chaotiques [6] et peut générer

des séquences chaotiques avec une plage de [0,1] en étirant et en retirant une valeur d'entrée initiale dans [0,1]. Mathématiquement, la carte logistique est définie :

$$x_{n+1} = ax_n(1 - x_n) \quad (1)$$

Où **a** est un paramètre ayant une plage de valeurs de [0, 4].

Le diagramme de bifurcation trace les séquences de sortie d'une carte chaotique en fonction de la variation de son (ses) paramètre(s). L'exposant de Lyapunov (EL) [7], [8] est une mesure utilisée pour décrire les comportements chaotiques d'un système dynamique. Une valeur d'EL positive indique que le système dynamique est chaotique.

Le diagramme de bifurcation et les valeurs d'EL de la carte logistique sont présentés dans la figure 3-9 (a) [9]. À partir de son diagramme de bifurcation, on peut observer que la carte logistique est chaotique lorsque a ∈ [3,57, 4], et qu'elle présente de meilleurs comportements chaotiques lorsque a est proche de 4.

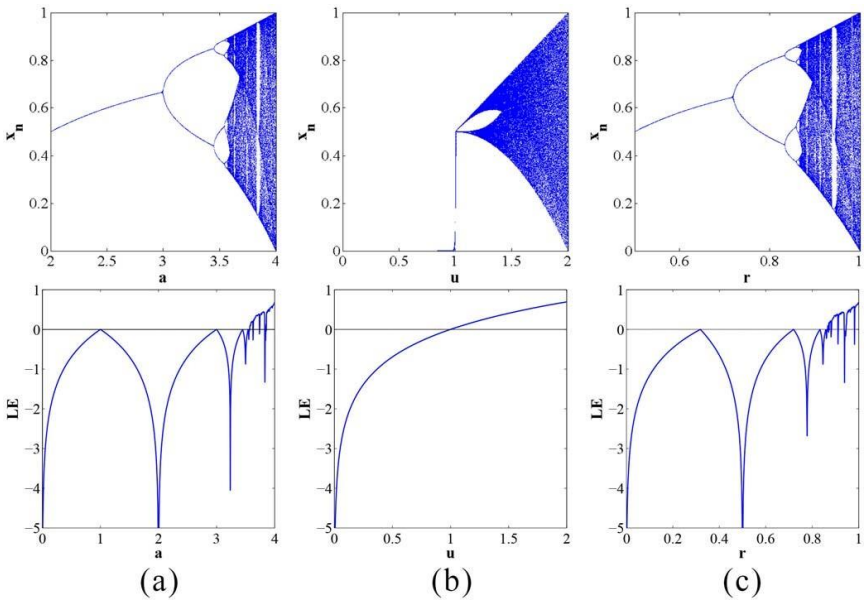


Figure 3-9 : La performance chaotique des trois cartes chaotiques. Les première et deuxième lignes représentent les diagrammes de bifurcation et les exposants de Lyapunov des (a) carte logistique, (b) carte tente et (c) carte sinus [9].

3.8.2 La Carte Tent :

La carte Tent est une autre carte chaotique discrète en une dimension qui effectue des opérations d'étirement et de pliage. Lorsque son entrée est inférieure à 0,5, elle étire la sortie dans la plage de [0, 1]. En revanche, lorsque son entrée est supérieure ou égale à 0,5, la carte Tente plie sa valeur d'entrée dans la plage de [0, 0,5], puis l'étire dans la plage de [0, 1] pour générer sa sortie. Sa représentation mathématique est définie par [9]:

$$x_{n+1} = \begin{cases} ux_n & \text{for} x_n < 0.5 \\ u(1 - x_n) & \text{for} x_n \geq 0.5 \end{cases} \quad (2)$$

Où le paramètre **u** se situe dans la plage de [0, 2].

Figure 3-9 (b) montre le diagramme de bifurcation et les valeurs d'EL de la carte Tent. Comme on peut le voir, la carte Tent présente de bonnes performances chaotiques lorsque le paramètre u ∈ (1, 2]. Lorsque u est proche de 2, ses séquences de sortie se répartissent presque dans toute la plage de données de [0, 1] [9].

3.8.3 La carte sine :

La carte sine est une autre carte chaotique couramment utilisée qui présente des comportements chaotiques similaires à la carte Logistic. Cependant, sa définition mathématique est totalement différente, comme indiqué ci-dessous :

$$x_{n+1} = r \sin(\pi x_n) \quad (3)$$

Où le paramètre **r** est compris entre 0 et 1 et Xn représente les sorties/entrées itératives avec une plage de [0, 1].

Lorsque r ∈ [0,867, 1], la carte sine présente des comportements chaotiques. Son diagramme de bifurcation et les valeurs d'EL sont présentés dans la Figure 3-9 (c). À partir de son diagramme de bifurcation, la carte sine présente de meilleurs comportements chaotiques lorsque le paramètre r est proche de 1 [9].

3.9 Le système chaotique en cascade (CCS) :

Figure 3-10 montre la structure de CCS, où G (x) et F (x) sont deux cartes de semences. CCS relie deux cartes de semences en série. La sortie de G (x) est introduite dans l'entrée de

F(x) et les entrées de F (x) la sortie est ensuite renvoyée dans l'entrée de G(x) pour récursive itérations [9].

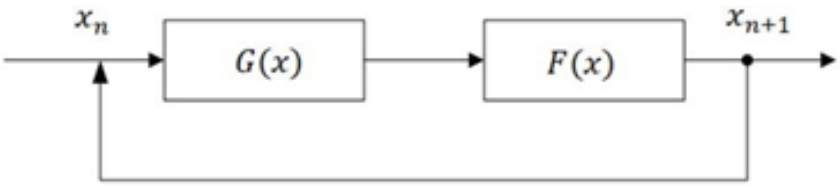


Figure 3-10 : Structure du CCS [9].

Mathématiquement, le CCS proposé est défini dans le suivant, où G (x) et F (x) sont deux cartes de semences :

$$\boldsymbol{x_{n+1} = \Gamma(x_n) = F(G(x_n))}. \quad (4)$$

Effectivement, tout 1-D carte chaotique existante peut être utilisée comme carte de départ (seed map) du CCS. Les utilisateurs ont la flexibilité de choisir les cartes de départ F(x) et G(x) comme étant les mêmes ou différentes cartes chaotiques [9].

1) Lorsque F(x) et G(x) sont les mêmes cartes chaotiques 1-D, c'est-à-dire F(x) = G(x), le CCS (cascade chaotic system) de l'équation (4) se simplifie en :

$$\boldsymbol{x_{n+1} = F(F(x_n))} \textbf{ ou } \boldsymbol{x_{n+1} = G(G(x_n))}. \quad (5)$$

Le CCS devient une structure dans laquelle une carte chaotique 1-D est en cascade avec elle-même. Par exemple, lorsque F(x) et G(x) sont deux cartes Sine, le CCS est appelé "Double-Sine map".

2) Lorsque F(x) et G(x) sont sélectionnées comme des cartes chaotiques différentes, c'est-à-dire F(x) ≠ G(x), le CCS devient une autre structure chaotique 1-D définie par l'équation (4) ou par :

$$\boldsymbol{x_{n+1} = G(F(x_n))}. \quad (6)$$

En modifiant les paramètres de F(x) et G(x) ou même en changeant l'ordre des deux cartes sources, le CCS génère une carte chaotique 1-D différente. Par exemple, les cartes Tent-Logistic et Logistic-Tent sont totalement différentes [9].

Le CCS offre aux utilisateurs une grande flexibilité pour générer un grand nombre de NCMs en utilisant différents paramètres de F(x) et G(x). Comparées à leurs cartes sources correspondantes, les cartes chaotiques générées par le CCS sont complètement différentes, et présentent plus de paramètres et des comportements chaotiques plus complexes [9].

De plus, la structure du CCS dans la Figure 3-10 peut être étendue à trois seed maps en cascade ou plus. Cela offre aux utilisateurs encore plus de flexibilité dans le choix des seed maps. Les cartes chaotiques résultantes présentent des comportements chaotiques beaucoup plus complexes et offrent davantage de réglages de paramètres, ce qui peut améliorer considérablement leur performance chaotique et générer des séquences de sortie plus aléatoires et imprévisibles. Cependant, la cascade de plusieurs seed maps peut entraîner certains effets secondaires, tels qu'un retard significatif, des difficultés de mise en œuvre matérielle et une complexité accrue de l'analyse des performances [9].

3.10 Analyse du comportement chaotique :

En connectant deux cartes chaotiques G(x) et F(x) en série, les séquences de sortie du CCS ont la structure de G(x), F(x) ou des deux. D'après la définition en (4), le CCS contient tous les paramètres de ses seed maps. Ainsi, il possède plus de paramètres et des propriétés plus complexes que ses seed maps [9].

Étant donné que le CCS est un cadre généralisé des systèmes chaotiques, en utilisant différentes cartes chaotiques en tant que seed maps, ou même en changeant l'ordre de ses seed maps, le CCS produit des cartes chaotiques totalement différentes. L'analyse ou la démonstration directe de la performance chaotique du CCS devient extrêmement difficile. Comme le LE [7], [8] donne une description quantitative des changements entre deux valeurs de sortie voisines d'un système dynamique, il peut être utilisé pour décrire les comportements chaotiques d'un système chaotique. Nous utilisons donc le LE pour analyser la performance chaotique du CCS proposé.

Supposons que $\boldsymbol{x_0}$ et $\boldsymbol{y_0}$ soient deux valeurs initiales extrêmement proches du CCS dans (4). Après la première itération, la différence $|\boldsymbol{x_1} - \boldsymbol{y_1}|$ est définie par :

$$|\boldsymbol{x_1} - \boldsymbol{y_1}| = |\boldsymbol{\Gamma}(\boldsymbol{x_0}) - \boldsymbol{\Gamma}(\boldsymbol{y_0})| = \frac{|\boldsymbol{F}(\boldsymbol{G}(\boldsymbol{x_0})) - \boldsymbol{F}(\boldsymbol{G}(\boldsymbol{y_0}))|}{|\boldsymbol{G}(\boldsymbol{x_0}) - \boldsymbol{G}(\boldsymbol{y_0})|} \frac{|\boldsymbol{G}(\boldsymbol{x_0}) - \boldsymbol{G}(\boldsymbol{y_0})|}{|\boldsymbol{x_0} - \boldsymbol{y_0}|} |\boldsymbol{x_0} - \boldsymbol{y_0}|.$$

Pour $x_0 \rightarrow y_0$, nous avons G $(x_0) \rightarrow$ G (y_0), puis :

$$\begin{aligned} |\frac{dF}{dx}|_{G(x_0)}| &\approx \lim_{G(x_0)\rightarrow G(y_0)} \frac{|F(G(x_0)) - F(G(y_0))|}{|G(x_0) - G(y_0)|} \\ |\frac{dG}{dx}|_{x_0}| &\approx \lim_{x_0 \rightarrow y_0} \frac{|G(x_0) - G(y_0)|}{|x_0 - y_0|}. \end{aligned}$$

De même, après la deuxième itération, la différence $|x_2 - y_2|$ est définie par :

$$\begin{aligned} |x_2 - y_2| &= |\Gamma(x_1) - \Gamma(y_1)| \\ &= \frac{|F(G(x_1)) - F(G(y_1))|}{|G(x_1) - G(y_1)|} \frac{|G(x_1) - G(y_1)|}{|x_1 - y_1|} |x_1 - y_1| \\ &\approx |\frac{dF}{dx}|_{G(x_1)}||\frac{dG}{dx}|_{x_1}||\frac{dF}{dx}|_{G(x_0)}||\frac{dG}{dx}|_{x_0}||x_0 - y_0|. \end{aligned}$$

Après la nième (n $\rightarrow \infty$) itération, la différence entre x_n et y_n est définie par :

$$\begin{aligned} |x_n - y_n| &= |\Gamma(x_{n-1}) - \Gamma(y_{n-1})| \\ &\approx |\prod_{i=0}^{n-1} \frac{dF}{dx}|_{G(x_i)}||\prod_{i=0}^{n-1} \frac{dG}{dx}|_{x_i}||x_0 - y_0|. \end{aligned}$$

Ensuite, le changement moyen à chaque itération de $|x_0 - y_0|$ à $|x_n - y_n|$ est donné par :

$$\Delta_{\Gamma(x)} \approx \{|\prod_{i=0}^{n-1} \frac{dF}{dx}|_{G(x_i)}||\prod_{i=0}^{n-1} \frac{dG}{dx}|_{x_i}|\}^{\frac{1}{n}}.$$

Par conséquent, le LE de $\Gamma(x)$ est défini par :

$$\begin{aligned} \lambda_{\Gamma(x)} &= \ln(\Delta_{\Gamma(x)}) \\ &= \lim_{n\rightarrow\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |\frac{dF}{dx}|_{G(x_i)}| + \lim_{n\rightarrow\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|\frac{dG}{dx}|_{x_i}| \end{aligned} \quad (7)$$

De manière similaire, les LE de F(x) et G(x) sont définis par :

$$\lambda_{F(x)} = \lim_{n\rightarrow\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |\frac{dF}{dx}|_{x_i}| \quad (8)$$

$$\lambda_{G(x)} = \lim_{n\rightarrow\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |\frac{dG}{dx}|_{x_i}|. \quad (9)$$

Alors, (7) devient :

$$\boldsymbol{\lambda_{\Gamma(x)} = \lambda_{F(x)} + \lambda_{G(x)}}. \quad (10)$$

Par conséquent, le LE de CCS est une combinaison des valeurs de LE de ses deux seed maps. Lorsque $\boldsymbol{\lambda_{\Gamma(x)}} > 0$, les trajectoires des deux séquences de sortie de CCS divergent de manière significative à mesure que le nombre d'itérations augmente, et CCS devient chaotique. Une valeur de LE positive plus grande indique une divergence plus rapide des deux trajectoires, ce qui se traduit par de meilleures performances chaotiques [9]. Les comportements chaotiques de CCS peuvent être résumés comme suit :

1) Lorsque $\boldsymbol{\lambda_{F(x)}} > 0$ et $\boldsymbol{\lambda_{G(x)}} > 0$, $\boldsymbol{\lambda_{\Gamma(x)}} > 0$, $\boldsymbol{\lambda_{\Gamma(x)}} > \boldsymbol{\lambda_{F(x)}}$ et $\boldsymbol{\lambda_{\Gamma(x)}} > \boldsymbol{\lambda_{G(x)}}$. Lorsque les deux seed maps sont chaotiques, CCS est chaotique et présente de meilleures performances chaotiques que ses seed maps.
2) Lorsque $\boldsymbol{\lambda_{G(x)}} \leq 0$ et $\boldsymbol{\lambda_{F(x)}} \leq 0$, $\boldsymbol{\lambda_{\Gamma(x)}} \leq 0$. CCS n'a aucun comportement chaotique lorsqu'aucune des seed maps n'est chaotique.
3) Lorsque $\boldsymbol{\lambda_{G(x)}} > 0$ et $\boldsymbol{\lambda_{F(x)}} \leq 0$, ou $\boldsymbol{\lambda_{F(x)}} > 0$ et $\boldsymbol{\lambda_{G(x)}} \leq 0$, nous avons :

$$\boldsymbol{\lambda_{\Gamma(x)}} \begin{cases} > \mathbf{0 if} \boldsymbol{\lambda_{F(x)} + \lambda_{G(x)} > 0} \\ \leq \mathbf{0 if} \boldsymbol{\lambda_{F(x)} + \lambda_{G(x)} \leq 0} \end{cases}$$

Lorsqu'il y a une seule seed map qui est chaotique, CCS sera chaotique si et seulement si $\boldsymbol{\lambda_{F(x)}} + \boldsymbol{\lambda_{G(x)}} > 0$.

En général, CCS est chaotique lorsqu'au moins une des seed maps est dans la plage chaotique [9]. Il présente de meilleures performances chaotiques lorsque les deux seed maps sont chaotiques.

3.11 Conclusion :

Dans ce chapitre, nous avons exploré les fondements de la cryptographie. Nous avons tout d'abord introduit les termes clés associés à ce domaine. Ensuite, nous avons examiné les divers algorithmes de chiffrement, tant classiques que modernes. Nous avons mis en évidence les capacités et les limitations propres à chaque type d'algorithme de chiffrement. Finalement on a

présenté le (CCS) système chaotique en cascade et leur cartes chaotiques traditionnelles et la structures de ce dernier, puis l'analyse de comportement chaotiques.

Dans le chapitre suivant, nous aborderons en détail les différentes méthodes de cryptage chaotiques. Nous examinerons les principes et les concepts fondamentaux du cryptage chaotique, ainsi que les différentes approches utilisées pour créer des systèmes de cryptage basés sur le chaos. Nous étudierons les avantages et les limites de chaque méthode, en mettant l'accent sur leur pertinence dans l'amélioration de la sécurité de la transmission des images biométriques. Cette exploration nous permettra de mieux comprendre comment les techniques de cryptage chaotiques peuvent contribuer à renforcer la sécurité et la confidentialité des données biométriques lors de leur transmission.

Bibliographie

[1] : http://ram0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2
< Visité le :07/03/2023>
[2] : http://www.bart-konieczny.com/fr/blog/securite-des-applications-web/cryptage-symetrique-et-asymetrique. < consulté le 5 mai 2023>
[3] : Gada Zaibi. Thèse doctorats , sécurisation par dynamiques chaotiques des réseaux locaux sans _l au niveau de la couche mac. autre [cs.oh]. Universités Toulouse le Mirail -Toulouse ii, 2012. français.
[4] : A. Menezes, P. VanOorschot, S. Vanstone, Handbook of applied cryptography, 1997 by CRC Press
[5] : Touradj Ebrahimi, Franck Leprévost, Bertrand Warusfel, Cryptographie et sécurité des systèmes et réseaux, Hermès -Lavoisier 2006.
[6] : Y. Zhou, L. Bao et C. L. P. Chen, «Cryptage d'image en utilisant un nouveau système de commutation paramétrique, "Signal Process., volume 93, numéro 11, pp. 3039-3052, 2013.
[7] : G. Jakimoski et K. P. Subbalakshmi, «exposant discret de Lyapunov et cryptanalyse différentielle, "IEEE Circuits Circuits II, Exp. vol. 54, no. 6, pages 499-501, juin 2007.
[8] : J. Amigo, L. Kocarev et J. Szczepanski, "exposant discret de Lyapunov". et la résistance à la cryptanalyse différentielle, "IEEE Trans. Circuits Syst. II, Exp. Mémoires, vol. 54, no. 10, pages 882 à 886, oct. 2007
[9] : Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," IEEE Transactions on Cybernetics, vol. 45, no. 9, pp. 2001–2012, 2015.

CHAPITRE 04
RESULTATS ET DISCUSSION

4.1 Introduction :

Un système dynamique est un concept en mathématiques où une règle fixe décrit la dépendance temporelle d'un point dans un espace géométrique [1]. Au cours des dernières décennies, les chercheurs ont accordé une attention croissante aux systèmes dynamiques [2], en particulier aux applications des cartes chaotiques [3] qui sont des systèmes dynamiques traditionnels. Les cartes chaotiques ont des propriétés d'ergodicité et d'imprévisibilité. Elles peuvent générer des séquences chaotiques totalement différentes en utilisant différents paramètres ou valeurs initiales. Grâce à ces propriétés significatives, les cartes chaotiques sont des outils utiles dans les applications des mathématiques, de l'informatique et de l'ingénierie. En particulier, dans les applications de sécurité, les cartes chaotiques présentent d'excellentes performances dans les générateurs de nombres pseudo-aléatoires (PRNG) [4], [5], le chiffrement de données et d'images [6] – [8].

Récemment, des nombreuses cartes chaotiques ont été développées [9], [10]. Elles peuvent être classées en deux catégories :

1) les cartes chaotiques unidimensionnelles (1-D) :

Les cartes chaotiques 1-D sont des systèmes mathématiques qui simulent l'évolution d'une seule variable sur des pas discrets dans le temps. Parmi les exemples, on trouve la carte logistique, la carte tente, la carte de Gauss et la transformation dyadique [9]. Ces cartes chaotiques 1-D ont généralement des structures simples et sont faciles à mettre en œuvre. Elles présentent d'excellentes propriétés chaotiques et ont été utilisées dans différentes applications de sécurité [7]. Cependant, elles présentent plusieurs faiblesses en termes de sécurité :

1) Leurs plages chaotiques sont limitées [8].
2) Elles ont un petit nombre de paramètres.
3) Leurs sorties sont faciles à prédire avec des coûts de calcul faibles [11] – [13].

2) les cartes chaotiques en haute dimension (HD) :

D'autre part, les cartes chaotiques en haute dimension modélisent l'évolution d'au moins deux variables. Parmi les exemples, on trouve la carte de Hénon[14], le système de Lorenz[14], le système de Chen et Lee [15] et les systèmes hyper-chaotiques [16]. Comparées aux cartes chaotiques 1-D, les cartes chaotiques en haute dimension ont généralement de meilleures performances chaotiques et leurs orbites chaotiques sont plus difficiles à prédire [17]. Cependant, les cartes chaotiques en haute dimension ont des coûts de calcul élevés et sont difficiles à mettre

en œuvre dans du matériel. Ces faiblesses limitent leurs performances dans certaines applications basées sur le chaos, en particulier dans les applications en temps réel [37].

Pour surmonter les performances chaotiques limitées des cartes chaotiques 1-D et les difficultés de mise en œuvre des cartes chaotiques en haute dimension, cet memoire propose un système chaotique en cascade (CCS) comme un cadre chaotique général en 1-D. Le CCS connecte deux cartes chaotiques 1-D (cartes de départ) en série. La sortie de la première carte de départ est liée à l'entrée de la deuxième carte de départ. La sortie de la deuxième carte est réinjectée dans l'entrée de la première pour des itérations récursives, et elle est également la sortie du CCS. En tant que cadre de cascade général, le CCS est capable de produire de nouvelles cartes chaotiques (NCM) en utilisant n'importe quelles deux cartes chaotiques 1-D comme cartes de départ. Trois exemples de NCM sont fournis. Les évaluations et les résultats d'analyse montrent que ces NCM ont plus de paramètres et de meilleures performances chaotiques que leurs cartes de départ correspondantes [37].

En utilisant une carte chaotique générée par le CCS comme exemple, nous proposons également un générateur de nombres pseudo-aléatoires (PRNG) et un système de chiffrement de données. Les résultats des tests SP800-22 du National Institute of Standards and Technology (NIST) et TestU01 sont fournis pour démontrer l'excellente aléatoire du PRNG. Des simulations et des analyses de sécurité sont fournies pour démontrer que le système de chiffrement de données peut chiffrer différentes données avec un haut niveau de sécurité et surpasser plusieurs algorithmes de pointe [37].

En résumé, nos principales contributions dans ce chapitre sont les suivantes :

1) Nous introduisons le CCS qui est un cadre chaotique général avec une structure simple et efficace.
2) Les performances chaotiques du CCS sont étudiées de manière théorique et expérimentale.
3) Nous proposons un PRNG basé sur le CCS.
4) Les propriétés aléatoires du PRNG proposé sont évaluées à l'aide de deux normes de test.
5) Nous développons également un système de chiffrement de données utilisant le CCS.
6) L'analyse de la performance de chiffrement et de sécurité du système de chiffrement de données proposé est réalisée.

4.2 Exemples de NCMS :

En utilisant différentes cartes chaotiques 1-D comme cartes de départ, CCS est capable de générer un grand nombre de modèles chaotiques non linéaires (NCMs). Pour illustrer la robustesse de CCS, cette section présente trois exemples de ces NCMs et discute de leurs performances chaotiques [37].

4.2.1 La Carte Tent-Logistic :

Lorsque $G(x)$ est défini comme la fonction de la tente et $F(x)$ est défini comme la fonction logistique dans la figure 3-10, CCS devient un NCM appelé la fonction de la Tent-Logistic [37]. Mathématiquement, la fonction de la tente-logistique est définie par :

$$x_{n+1} = \begin{cases} \mathbf{aux}_n\ (\mathbf{1} - \boldsymbol{ux}_n) & \textbf{for } \boldsymbol{x}_n < \mathbf{0.5} \\ \boldsymbol{au}(\mathbf{1} - \boldsymbol{x}_n)(\mathbf{1} - \boldsymbol{u}(\mathbf{1} - \boldsymbol{x}_n)) & \textbf{for } \boldsymbol{x}_n \geq \mathbf{0.5} \end{cases} \quad (11)$$

Où les paramètres a et u proviennent de ses deux fonctions de départ, la fonction logistique et la fonction de la tente. Ainsi, la plage des deux paramètres est $a \in [0,4]$ et $u \in [0,2]$.

Les diagrammes de bifurcation 2-D et 1-D de la carte Tent-Logistic sont présentés dans la première ligne de Figure 4-1. La figure 3-9 montre que les cartes Logistic et de la Tent ont des comportements chaotiques lorsque $a \in [3{,}57, 4]$ et $u \in (1, 2]$, respectivement. Comme on peut le voir sur Figure 4-1, la carte Tent-Logistic présente des plages chaotiques plus étendues en fonction des paramètres a et u. Cela signifie que les cartes chaotiques générées par CCS peuvent hériter et améliorer les performances chaotiques de leurs cartes de départ [37].

4.2.2 La Carte Logistic-Tent :

Lorsque l'on échange les positions des deux cartes de départ dans la carte Tent-Logistic, c'est-à-dire lorsque $G(x)$ est la carte Logistic et $F(x)$ est la carte de la Tent dans la figure 3-10, une autre carte chaotique est générée, appelée la carte Logistic-Tent [37]. Sa représentation mathématique est définie par l'équation suivante :

$$x_{n+1} = \begin{cases} \boldsymbol{uax}_n(\mathbf{1} - \boldsymbol{x}_n) & \textbf{for } \boldsymbol{ax}_n(\mathbf{1} - \boldsymbol{x}_n) < \mathbf{0.5} \\ \boldsymbol{u}(\mathbf{1} - \boldsymbol{ax}_n(\mathbf{1} - \boldsymbol{x}_n)) & \textbf{for } \boldsymbol{ax}_n(\mathbf{1} - \boldsymbol{x}_n) \geq \mathbf{0.5} \end{cases} \quad (12)$$

Où les paramètres a et u ont également les mêmes valeurs que les cartes Logistic et Tent, à savoir $a \in [0,4]$ et $u \in [0,2]$.

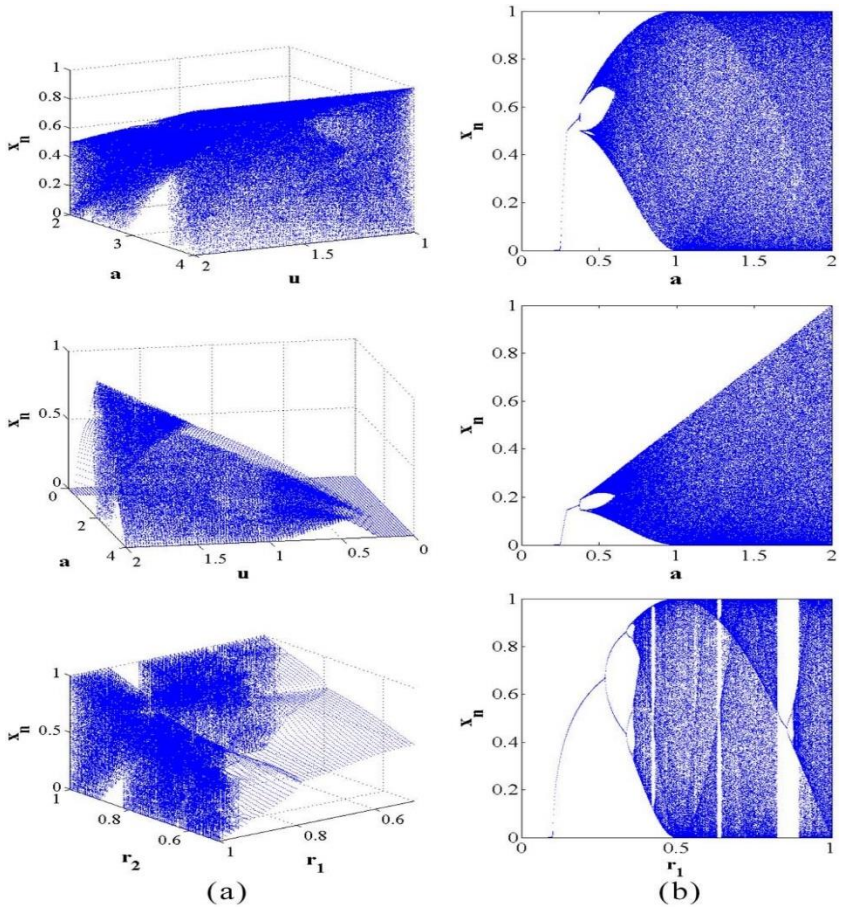


Figure 4-1 : Les diagrammes de bifurcation des trois NCMs. Les première, deuxièmes et troisièmes rangées montrent respectivement les diagrammes de bifurcation 2-D et 1-D des cartes Tent-Logistic, Logistic-Tent et Double-Sine [37].

La deuxième rangée de la figure 4-1 montre les diagrammes de bifurcation 2-D et 1-D de la carte Logistic-Tent. En comparant avec les diagrammes de bifurcation de la carte Tent-Logistic, on peut observer que l'utilisation de deux cartes semences dans des ordres différents produit deux cartes chaotiques avec des comportements chaotiques complètement différents [37].

4.2.3 La Carte Double-Sine :

Dans CCS, les deux cartes de départ peuvent être la même carte chaotique. Dans ce scénario, la carte chaotique se répète. Lorsque les deux cartes de départ sont sélectionnées comme la carte Sine, CCS génère une carte chaotique appelée la carte Double-Sine [37]. Sa représentation mathématique est définie par l'équation suivante :

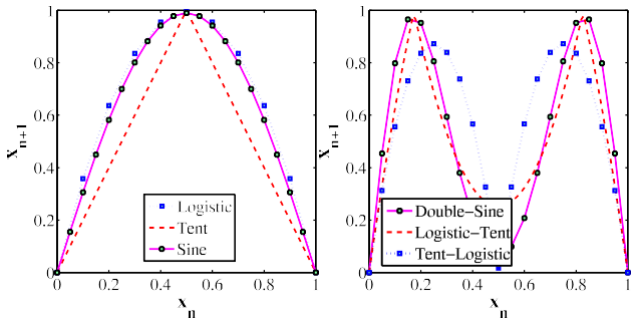
$$x_{n+1} = r_2 \sin(\pi r_1 \sin(\pi x_n)) \quad (13)$$

Où r_1 et r_2 sont deux paramètres, et $r_1, r_2 \in [0,1]$.

Ses diagrammes de bifurcation en 2-D et 1-D sont présentés dans la troisième rangée de la Figure 4-1. Comme on peut le voir, même en reliant simplement deux cartes Sine en série, les comportements chaotiques de la carte Double-Sine sont totalement différents et bien meilleurs que ceux de la carte Sine [37].

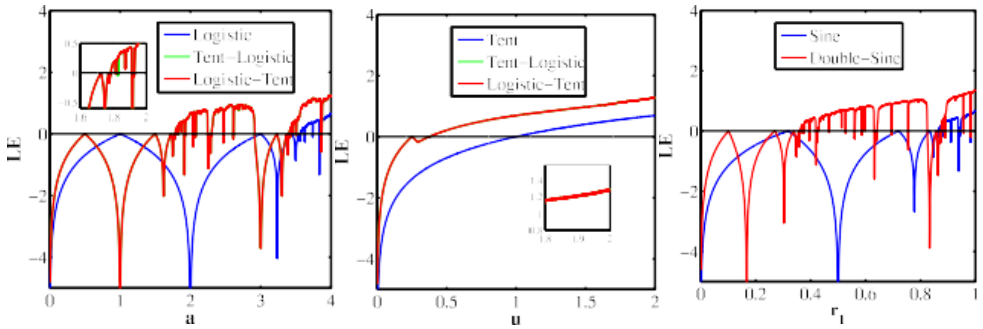
4.3 Analyse des performances :

Cette section analyse les performances chaotiques des trois cartes chaotiques. Les résultats de comparaison montrent que ces NCMs ont de meilleures performances chaotiques que leurs cartes sources correspondantes [37].



(a) (b)

Figure 4-2 : Diagrammes des fonctions d'itération des (a) cartes Logistic, Tent et sine et (b) cartes double-sine, Logistic-Tent et Tent-Logistic [37].



(a) (b) (c)

Figure 4-3 : Comparaison des (LE) des (a) cartes Logistic, Tent Logistic et logistique-tente ; (b) cartes Tent, Tent Logistic et Logistic Tent ; et (c) cartes sine et double-sine, respectivement [37].

4.3.1 Diagramme de la fonction d'itération :

Pour un système dynamique itératif tel que $x_n + 1 = f(x_n)$, le diagramme de la fonction d'itération décrit la sortie $x_n + 1$ en fonction de l'entrée x_n.

Les diagrammes de la fonction d'itération de ces NCMs dans Figure 4-2 (b) présentent des motifs plus complexes que ceux de leurs seed maps dans Figure 4-2 (a). Cela est dû au fait que leurs sorties sont des combinaisons d'orbites chaotiques de deux seed maps. Ces diagrammes de fonction d'itération complexes ont des avantages en termes de sécurité car ils sont difficiles à prédire [37]. Les NCMs sont plus adaptés aux applications de sécurité que leurs seed maps correspondants.

4.3.2 Exposant de Lyapunov :

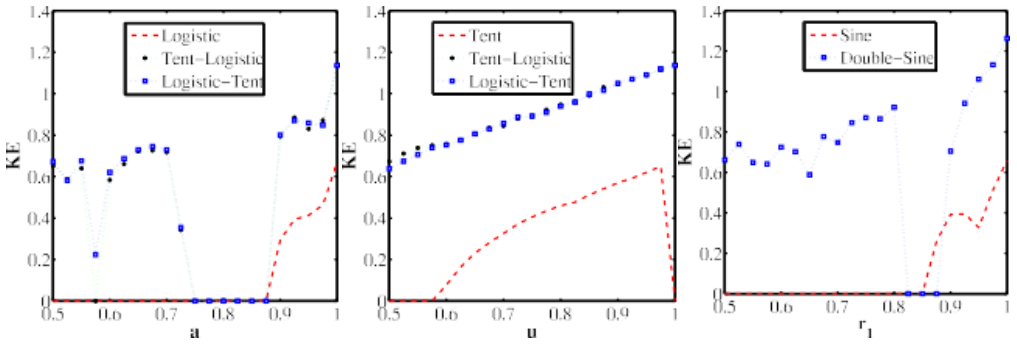
Une valeur positive de l'exposant de Lyapunov d'un système dynamique indique que les trajectoires de ses deux séquences de sortie, générées à partir d'entrées initiales extrêmement proches, divergent considérablement à chaque itération. Des valeurs d'exposant de Lyapunov positif plus élevées indiquent des divergences plus rapides des trajectoires des sorties, et donc une meilleure performance chaotique [37].

Les valeurs d'exposant de Lyapunov des NCMs et de leurs seed maps sont tracées dans la figure 4-3. On peut observer que, avec les mêmes paramètres, les NCMs ont des valeurs d'exposant de Lyapunov plus grandes que leurs seed maps correspondantes dans la plupart des plages de paramètres [37].

Même si les cartes Tent-Logistic et Logistic-Tent sont deux maps chaotiques avec des définitions et des trajectoires différentes, elles ont des caractéristiques chaotiques similaires en raison du fait qu'elles sont dérivées des mêmes seed maps et que leurs distributions d'exposant de Lyapunov sont similaires [37].

4.3.3 Entropie de Kolmogorov :

L'entropie de Kolmogorov (KE), également connue sous le nom d'entropie métrique, d'entropie Kolmogorov-Sinai ou d'entropie K, est une mesure qui décrit la quantité d'information en moyenne nécessaire pour prédire la trajectoire d'un système dynamique à chaque unité de temps [21].



(a) (b) (c)

Figure 4-4 : Comparaison de KE des (a) cartes Logistic, Tent-Logistic et Logistic-Tent ; (b) cartes Tent, Tent-Logistic et Logistic-Tent, et (c) cartes sine et double-sine, respectivement [37].

Mathématiquement, l'entropie de Kolmogorov est définie :

$$\boldsymbol{KE = \lim_{\tau \to 0} \tau^{-1} \lim_{\varepsilon \to 0} \lim_{m \to \infty} K_{m,\tau}(\varepsilon)} \tag{14}$$

Où $\boldsymbol{m}$ est la dimension d'incorporation ; $\boldsymbol{K_{m,\tau}(\varepsilon)}$ est défini par :

$$\boldsymbol{K_{m,\tau}(\varepsilon) = -\sum_{i_1, i_2, \ldots, i_m \leq n(\varepsilon)} p_i \times \log p_i} \tag{15}$$

Où φi_1, $\varphi i\_2, \ldots, \varphi_{im}$ sont des partitions non chevauchantes du plan de phase d'un système dynamique, $p(i_1, i_2, \ldots, i_m)$ est la probabilité conjointe de trouver la trajectoire dans la partition φi_1 au temps τ, dans la partition φi_2 au temps 2τ , ..., dans la partition φ_{im} au temps $m\tau$.

Un système dynamique avec une valeur positive de KE est imprévisible, et une valeur de KE positive plus élevée indique une plus grande imprévisibilité et une meilleure performance chaotique [22].

Dans nos expériences, nous avons choisi 12 000 points continus à partir des trajectoires des NCMs et de leurs seed maps avec les mêmes paramètres. Figure 4-4 représente les résultats de KE calculés selon la méthode décrite dans [23]. Figure 4-4 (a) et (b) montrent que les maps Tent-Logistic et Logistic-Tent ont des valeurs de KE positives beaucoup plus élevées que les maps Tent et Logistic dans toutes les plages de paramètres. Figure 4-4 (c) montre que la map Double-Sine a

des valeurs de KE positives plus élevées que la map Sine dans la plupart des paramètres. Par conséquent, les NCMs ont une plus grande imprévisibilité et une meilleure performance chaotique que leurs seed maps [37].

4.3.4 Test de corrélation :

La distance entre deux séquences de données peut être évaluée par le test de corrélation. Mathématiquement, la corrélation de deux séquences de données est définie comme suit :

$$\boldsymbol{Co = \frac{E[(X_t - \mu_X)(Y_t - \mu_Y)]}{\sigma_X \sigma_Y}} \quad (16)$$

Où $\boldsymbol{X_t}$ et $\boldsymbol{Y_t}$ sont deux séquences de données, μ et σ sont la valeur moyenne et l'écart-type, $E[.]$ est la fonction d'espérance.

Si deux séquences de données $\boldsymbol{X_t}$ et $\boldsymbol{Y_t}$ sont proches l'une de l'autre, la valeur de corrélation est proche de 1 ; si $\boldsymbol{X_t}$ et $\boldsymbol{Y_t}$ sont totalement différentes, la valeur de corrélation est proche de 0, indiquant que les deux séquences ont une relation extrêmement faible.

Paramètres $(\boldsymbol{u}, \boldsymbol{a})$	(1.46, 3.64)		(1.74, 3.96)	
	Corrélation de S_1 , S_2	Corrélation de S_3 , S_4	Corrélation de S_1 , S_2	Corrélation de S_3 , S_4
La carte Logistic (a)	0.833013	0.815053	0.057409	-0.127028
La carte Tent (u, a)	0.066046	0.140041	0.013925	0.022016
La carte Logistic-Tent (u, a)	-0.029632	0.026886	-0.005645	0.014180
La carte Tent-Logistic (u, a)	0.010853	0.104041	-0.006496	0.011341
Paramètres $(\boldsymbol{u}, \boldsymbol{a})$	(0.895, 0.913)		(0.902, 0.948)	
	Corrélation de S_1 , S_2	Corrélation de S_3 , S_4	Corrélation de S_1 , S_2	Corrélation de S_3 , S_4
La carte Sine r_1	-0.050228	0.223317	-0.075275	-0.029231
La carte Sine (r_2)	-0.066046	0.012340	0.220003	0.136564
La carte Double-Sine (r_1, r_2)	0.000578	0.009010	-0.027488	0.017769

Tableau 4-1 : Comparaisons de corrélation des séquences de sortie des NCM et de leurs cartes sources [37].

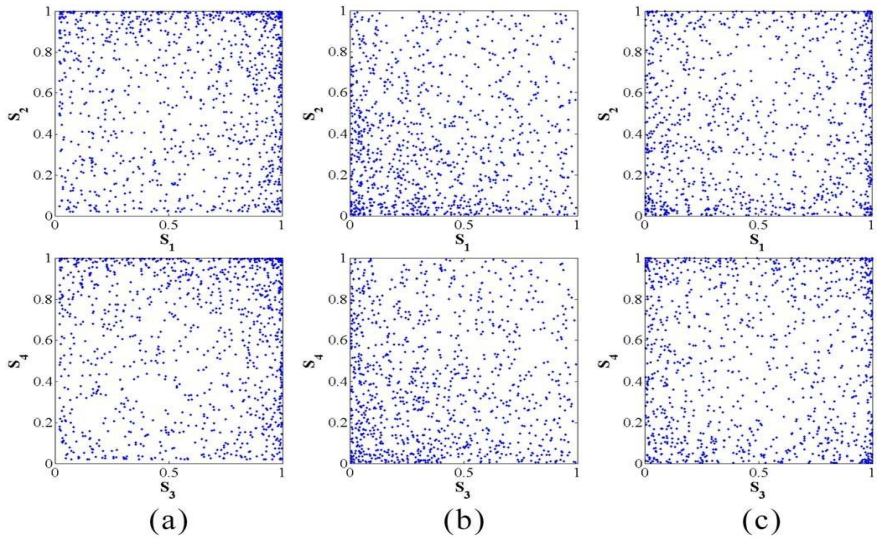


Figure 4-5 : Graphiques de corrélation des séquences de sortie générées par les (a) cartes tent-logistic, (b) logistic-tent et (c) double-sine avec une légère modification des valeurs initiales (rangée supérieure) et des paramètres (rangée inférieure) [37].

Ici, nous utilisons la corrélation pour évaluer la sensibilité d'une carte chaotique à ses valeurs initiales et à ses paramètres. Les résultats du test des différentes cartes chaotiques sont présentés dans la figure 4-5 et le tableau 4-1. Les paires de séquences de sortie S1 et S2, S3 et S4 sont générées en appliquant une légère modification aux valeurs initiales et aux paramètres, respectivement. Comme on peut le voir dans la figure 4-5 , de petites variations dans les valeurs initiales ou les paramètres des NCMs entraînent une répartition dynamique des séquences de sortie dans l'ensemble de l'intervalle de données. Cela signifie que les séquences de sortie n'ont aucune relation entre elles. Ainsi, ces NCMs sont extrêmement sensibles à leurs valeurs initiales et à leurs paramètres [37].

Les comparaisons quantitatives dans le tableau 4-1 montrent que les séquences de sortie des NCMs ont des valeurs de corrélation absolue plus faibles que celles de leurs cartes sources. Cela montre que les NCMs sont plus sensibles aux valeurs initiales et aux paramètres que leurs cartes sources [37].

4.4 PRNG PROPOSÉ :

En raison de leurs propriétés d'ergodicité, d'imprévisibilité et de sensibilité aux valeurs/paramètres initiaux, les cartes chaotiques sont des candidats idéaux pour la conception d'un générateur de nombres aléatoires (PRNG). Récemment, de nombreux PRNG basés sur des cartes chaotiques ont été proposés [5], [24]. Les performances chaotiques des cartes chaotiques déterminent la qualité aléatoire des PRNG. Comme discuté dans les sections précédentes, les cartes chaotiques générées par CCS présentent de meilleures performances chaotiques que les cartes de départ existantes, ce qui les rend plus adaptées aux PRNG [37].

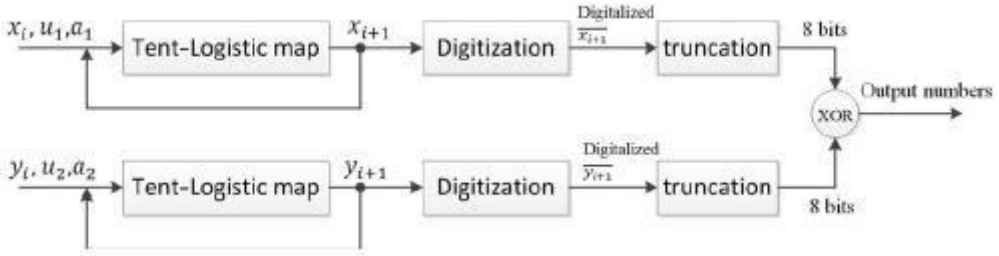


Figure 4-6 : Structure de TLPRNG [37].

Cette section utilise la carte Tent-Logistic comme exemple de NCM générée par CCS pour concevoir un nouveau PRNG, puis analyse sa propriété aléatoire [37].

Le PRNG proposé est appelé PRNG basé sur la carte du Tent-Logistic (TLPRNG). Son schéma bloc est présenté dans la Figure 4-6 . Supposons que $\{x_i, i = 1,2,\dots,N\}$ et $\{y_i, i = 1,2,\dots,N\}$ sont deux séquences chaotiques générées par la carte du Tent-Logistic avec des valeurs initiales et des paramètres différents [37]. TLPRNG est défini comme suit :

$$\mathbf{TLPRNG}\ (\boldsymbol{i}) = \boldsymbol{X}(\boldsymbol{i}) \oplus \boldsymbol{Y}(\boldsymbol{i}) \tag{17}$$

où $\oplus$ est l'opération XOR, $\boldsymbol{X}(\boldsymbol{i})$ et $\boldsymbol{Y}(\boldsymbol{i})$sont des nombres binaires sur 8 bits définis par :

$$\begin{aligned} \boldsymbol{X}(\boldsymbol{i}) &= \boldsymbol{T}\lceil\overline{\boldsymbol{x}}_{\boldsymbol{i}}\rfloor_{\boldsymbol{k_1}:(\boldsymbol{k_1}+7)} \\ \boldsymbol{Y}(\boldsymbol{i}) &= \boldsymbol{T}\lceil\overline{\boldsymbol{y}}_{\boldsymbol{i}}\rfloor_{\boldsymbol{k_2}:(\boldsymbol{k_2}+7)} \end{aligned} \tag{18}$$

où $T_m[\boldsymbol{k_1}:(\boldsymbol{k_1}+\boldsymbol{7})]$ est une fonction permettant de tronquer le flux de bits binaire m de la position $\boldsymbol{k_1}$ à la position $(\boldsymbol{k_1}+\boldsymbol{7})$. x_i et y_i sont des flux binaires de 52 bits convertis à partir des sorties x_i et y_i selon la norme IEEE 754 [25]. $\boldsymbol{k_1}$ et $\boldsymbol{k_2}$ sont deux entiers définis par :

$$k_1 = (x_i \times 10^{10} mod 6) + 39 \quad (19)$$
$$k_2 = (y_i \times 10^{10} mod 6) + 39.$$

À chaque itération, la séquence binaire de 8 bits est générée par TLPRNG.

Dans TLPRNG, nous utilisons deux sorties de la map Tent-Logistic avec des valeurs initiales et des paramètres différents pour générer des nombres pseudo-aléatoires. Comme on peut le voir dans la figure 4-6 , l'utilisation de deux sorties provenant d'orbites chaotiques différentes permet à TLPRNG de générer des nombres pseudo-aléatoires avec des tailles suffisamment grandes et une excellente aléatorité [37].

4.5 Système proposé pour le cryptage des données :

En tant que technologie de sécurité des données directe, le chiffrement des données suscite de plus en plus d'attention. Il transforme les données en un format de données dépourvu de sens. Au cours des dernières décennies, de nombreuses technologies de chiffrement des données ont été développées. Parmi les exemples figurent le standard de chiffrement numérique (DES), le standard de chiffrement avancé (AES), le chiffrement des données en réseau [30] et de nombreux autres algorithmes de chiffrement [7], [31]. En raison des propriétés de sensibilité aux paramètres et aux valeurs initiales, d'ergodicité et d'imprévisibilité, les cartes chaotiques sont de bons outils pour le chiffrement des données. Les cartes chaotiques présentant d'excellents comportements chaotiques offrent des avantages en termes de sécurité pour le chiffrement des données. Étant donné que le CCS proposé présente de bonnes performances chaotiques, il est adapté au chiffrement des données.

Dans ce chapitre, en utilisant l'exemple du CCS basé sur la carte Tent-Logistic, nous introduisons un nouvel algorithme de chiffrement des données basé sur la carte Tent-Logistic (TL-DEA). De nombreux DEA existants sont conçus pour chiffrer des données au format binaire, tels que le DES et l'AES. Les données avec d'autres formats doivent être transformées en format binaire avant le chiffrement. Cela peut être inefficace pour certaines données de grande taille, telles que des images/vidéos haute résolution. Mais TL-DEA peut chiffrer directement différents types de données. Des simulations et une analyse de sécurité sont fournies pour démontrer ses performances en matière de chiffrement [37].

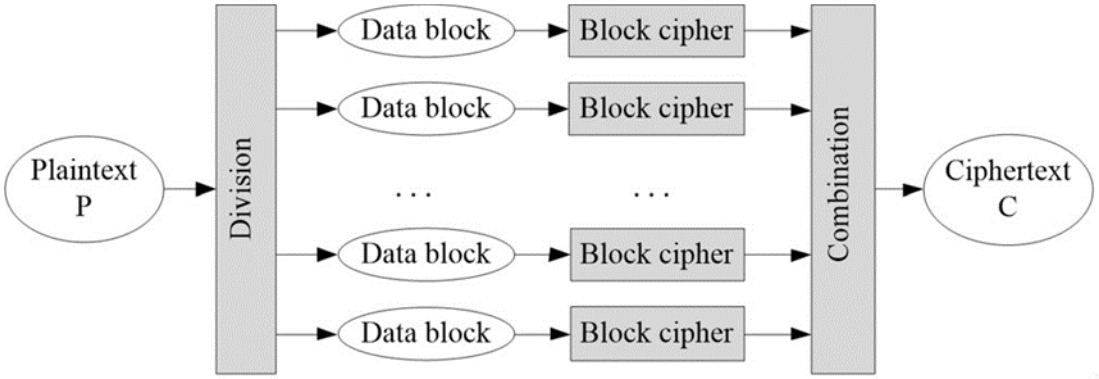


Figure 4-7 : Proposition de TL-DEA.

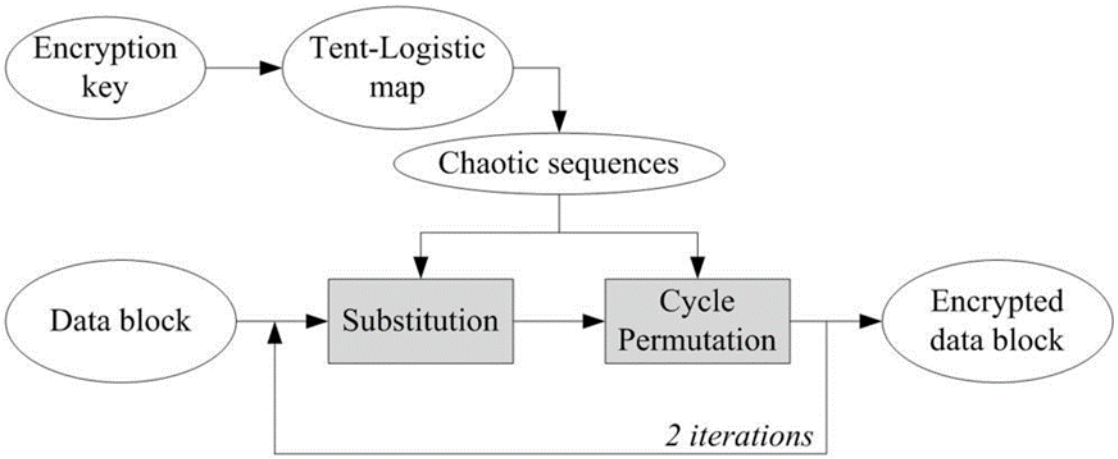


Figure 4-8 : Schéma fonctionnel du chiffrement par bloc.

Algorithme 1 Génération des valeurs initiales et des paramètres :

Input : Security key $\boldsymbol{K}$ with length of 256 bits

1 : Initial value $\boldsymbol{x_0} \leftarrow \left(\sum_{i=1}^{52} \boldsymbol{K_i}\, \boldsymbol{2^{52-i}} \right) / \boldsymbol{2^{52}}$

2 : parameter $\boldsymbol{u} \leftarrow \left(\sum_{i=53}^{104} \boldsymbol{K_i}\, \boldsymbol{2^{104-i}} \right) / \boldsymbol{2^{52}}$

3 : parameter $\boldsymbol{a} \leftarrow \left(\sum_{i=105}^{156} \boldsymbol{K_i}\, \boldsymbol{2^{156-i}} \right) / \boldsymbol{2^{52}}$

4 : $\boldsymbol{T} \leftarrow \left(\sum_{i=157}^{208} \boldsymbol{K_i}\, \boldsymbol{2^{208-i}} \right) / \boldsymbol{2^{52}}$

5 : $\boldsymbol{R_1} \leftarrow \sum_{i=209}^{232} \boldsymbol{K_i}\, \boldsymbol{2^{232-i}}$

6 : $\boldsymbol{R_2} \leftarrow \sum_{i=233}^{256} \boldsymbol{K_i}\, \boldsymbol{2^{256-i}}$

7 : **for** $\boldsymbol{i = 1}$ to 2 **do**

8 : $\boldsymbol{x_{0i}} \leftarrow (\boldsymbol{x_0} + \boldsymbol{R_i T})$ *mod* 1

9 : $\boldsymbol{u_i} \leftarrow \boldsymbol{1.8} + (\boldsymbol{u} + \boldsymbol{R_i T})$ *mod* 0.2

10 : $\boldsymbol{a_i} \leftarrow \boldsymbol{3.8} + (\boldsymbol{a} + \boldsymbol{R_i T})$ *mod* 0.2

11 : **end for**

Output : Initial conditions $(\boldsymbol{x_{01}}, \boldsymbol{u_1}, \boldsymbol{a_1})$ and $(\boldsymbol{x_{02}}, \boldsymbol{u_2}, \boldsymbol{a_2})$.

4.5.1 TL-DEA :

Le diagramme en blocs du TL-DEA proposé est présenté dans la Figure 4-7. Le texte en clair **P** représente les données originales, tandis que le **Ciphertext C** désigne les données chiffrées. L'opération de division permet de diviser le texte en clair en plusieurs blocs de données de longueur fixe. Le chiffrement par bloc est ensuite utilisé pour chiffrer chaque bloc de données individuellement. L'opération de combinaison permet de regrouper tous les blocs de données chiffrées en une séquence de données chiffrées afin d'obtenir le texte chiffré [37].

Le chiffrement par bloc est présenté dans la Figure 4-8. La clé de chiffrement est utilisée pour fournir des conditions initiales à la map Tent Logistic. Les deux étapes de substitution et de permutation dans le TL-DEA garantissent de bonnes propriétés de confusion et de diffusion [37].

1) **Analyse de clé :** La clé de sécurité dans TL-DEA est avec longueur de 256 bits. Il est utilisé pour produire deux groupes de valeurs et paramètres tels que décrits dans l'algorithme 1. La carte Tente-Logistique les utilise ensuite pour générer deux séquences chaotiques.

Algorithme 2 Cycle de permutation

Input : Data block $\boldsymbol{H}$ and chaotic sequence $\boldsymbol{S}$. Both are with length of $\boldsymbol{L}$

1 : Rearrange $\boldsymbol{H}$, $\boldsymbol{S}$ with size of $\boldsymbol{M} \times \boldsymbol{N}$, where $\boldsymbol{L} = \boldsymbol{M} \times \boldsymbol{N}$

2 : Sort each row of $\boldsymbol{S}$ and get the row index matrix $\boldsymbol{I}$. Then

Sorted_$\boldsymbol{S_{m,n}} = \boldsymbol{S_m}, \boldsymbol{I_{m,n}}$, where $\boldsymbol{m,n} \in [\boldsymbol{1,M}] \times [\boldsymbol{1,N}]$

3 : **for** $\boldsymbol{j} = \boldsymbol{1}$ to $\boldsymbol{N}$ **do**

4 : **for** $\boldsymbol{i} = \boldsymbol{1}$ to $\boldsymbol{M}$ **do**

5 : Find value $\boldsymbol{j}$ in $\boldsymbol{i}$th row of $\boldsymbol{I}$, get its position $(\boldsymbol{i}, \boldsymbol{j_i})$.

6 : **end for**

7 : Connect values of $\boldsymbol{H}$ in positions $(\boldsymbol{1,j_1})$, $(\boldsymbol{2,j_2})$, ... , $(\boldsymbol{M,j_M})$

into a circle, and shift them by $\boldsymbol{j}$ positions to upper direction.

8 : **end for**

9 : Rearrange the permutation result into length of $\boldsymbol{L}$

Output : The permuted result $\boldsymbol{C}$.

2) **Substitution :** Le processus de substitution est conçu pour modifier les valeurs de données dans le texte en clair en utilisant ses deux valeurs de données voisines précédentes et une valeur aléatoire de la séquence chaotique. Supposons qu'un bloc de données P est avec une longueur de L, une séquence chaotique S avec la longueur de L est générée par la Tente-Logistique carte, $S = \{x1, x2, \ldots, xL\}$. Relier chaque donnée à son précédent un et reliant les premières données avec le dernier sont à faire le bloc de données sous la forme d'un cercle. Ensuite, le processus de substitution pour chaque bloc de données est défini comme :

$$H_i = \begin{cases} (P_i + P_L + P_{L-1} + \lfloor S \times 2^{20} \rfloor_i) \ mod \ F & \text{if } i = 1 \\ (P_i + C_{i-1} + P_L + \lfloor S \times 2^{20} \rfloor_i) \ mod \ F & \text{if } i = 2 \\ (P_i + C_{i-1} + C_{i-2} + \lfloor S \times 2^{20} \rfloor_i) \ mod \ F & \text{if } i \in [3, L] \end{cases} \quad (20)$$

Là où F représente le nombre d'échelles d'intensité autorisées dans le texte en clair. Par exemple, $F = 2$ si le texte en clair ne contient que des données binaires, et $F = 256$ si

le texte en clair est représenté en décimales sur 8 bits. La notation $\lfloor . \rfloor$ correspond à l'opération de valeur entière inférieure.

3) Cycle de permutation : Le cycle de permutation consiste à mélanger toutes les positions de données, comme indiqué dans l'Algorithme 2.

Par exemple, supposons que la matrice d'index de ligne I soit la suivante :

$$I = \begin{bmatrix} 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 4 \\ 3 & 2 & 4 & 1 \\ 1 & 4 & 3 & 2 \end{bmatrix}$$

Figure 4-8 montre les opérations détaillées utilisant la matrice d'index I. Tout d'abord, nous recherchons la valeur d'index 1 dans toutes les lignes de I et obtenons les positions (1, 2), (2, 1), (3, 4) et (4, 1), puis nous connectons les données dans ces positions dans le bloc de données H en un cercle et les décalons d'une position vers le haut. Ensuite, nous recherchons la valeur d'index 2 dans I, et obtenons les positions (1, 1), (2, 3), (3, 2) et (4, 4), nous connectons les données dans ces positions dans H en un cercle, puis nous les décalons de 2 positions vers le haut. Nous répétons les mêmes procédures jusqu'à la valeur d'index maximale dans I. Après une permutation cyclique, les données peuvent être séparées de toutes leurs données voisines [37].

En répétant une fois de plus la substitution et la permutation circulaire avec une autre séquence chaotique, le bloc de données chiffrées est obtenu.

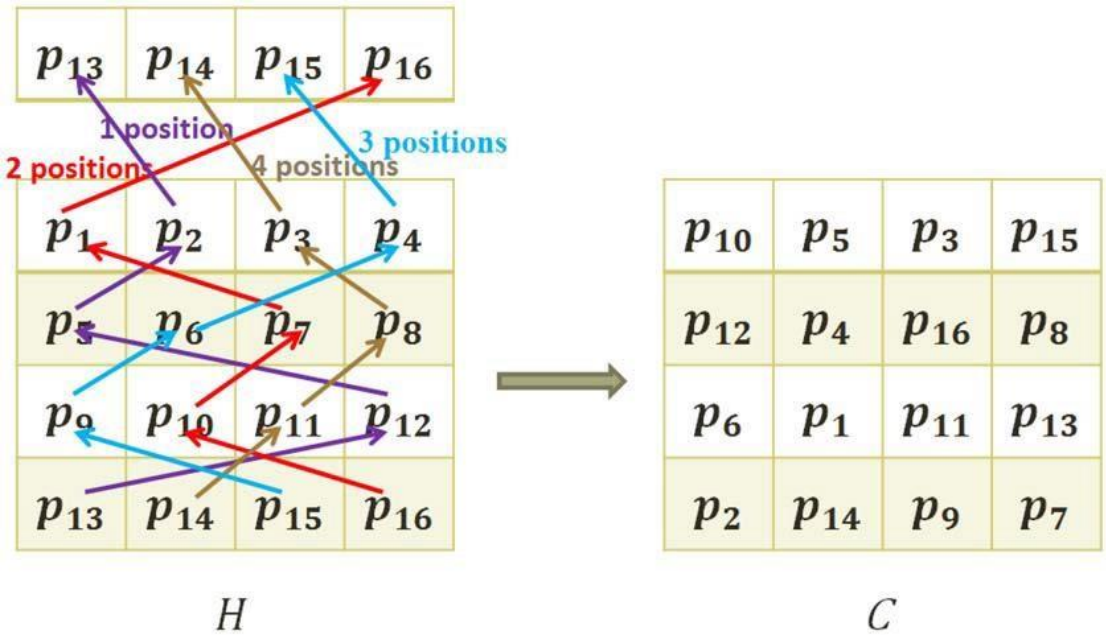
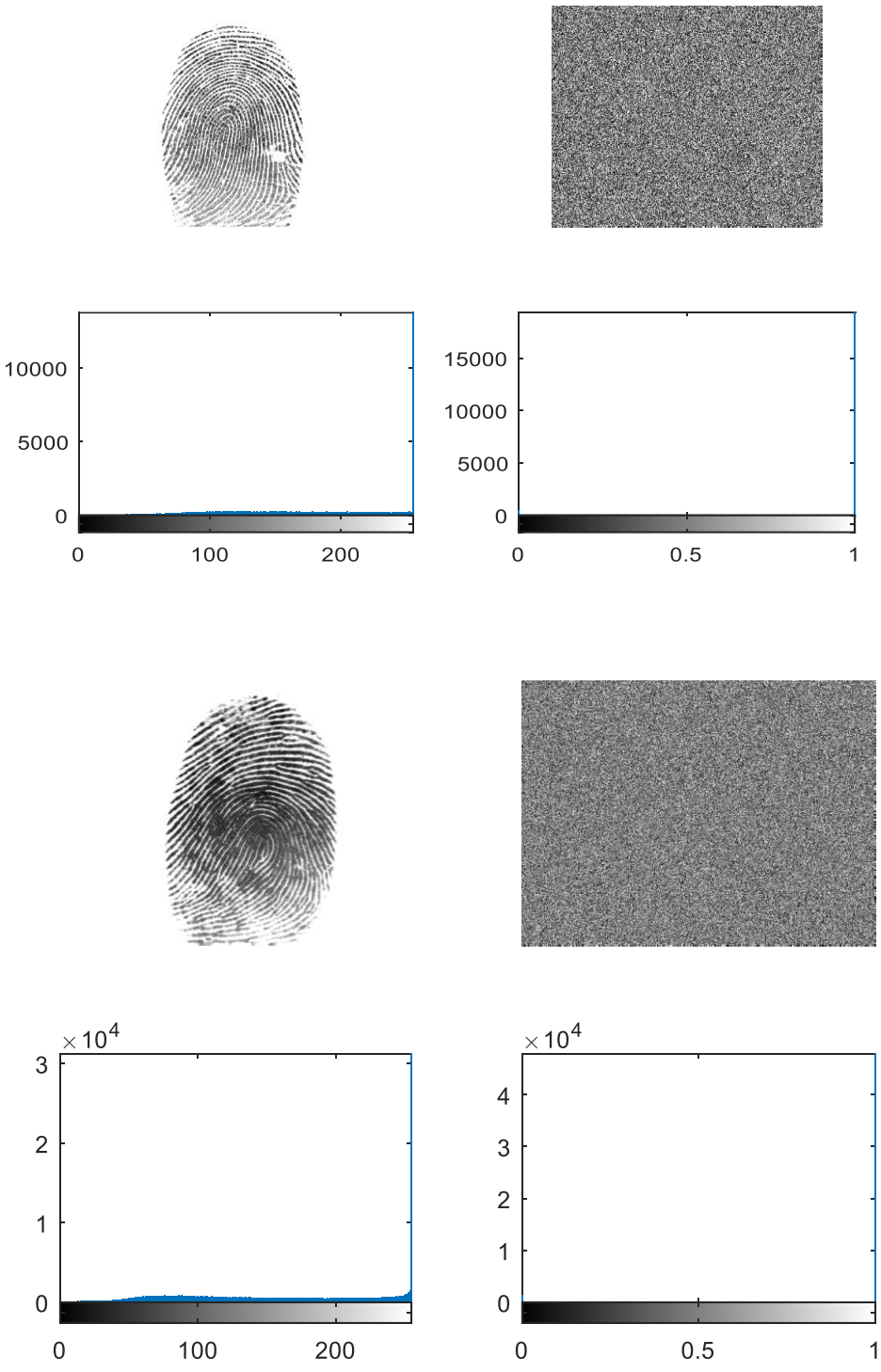


Figure 4-9 : Exemple de permutation de cycle [37].


10000
5000
0
0
100
200
15000
10000
5000
0
0
0.5
1
×10^4
3
2
1
0
0
100
200
×10^4
4
3
2
1
0
0
0.5
1

(a)

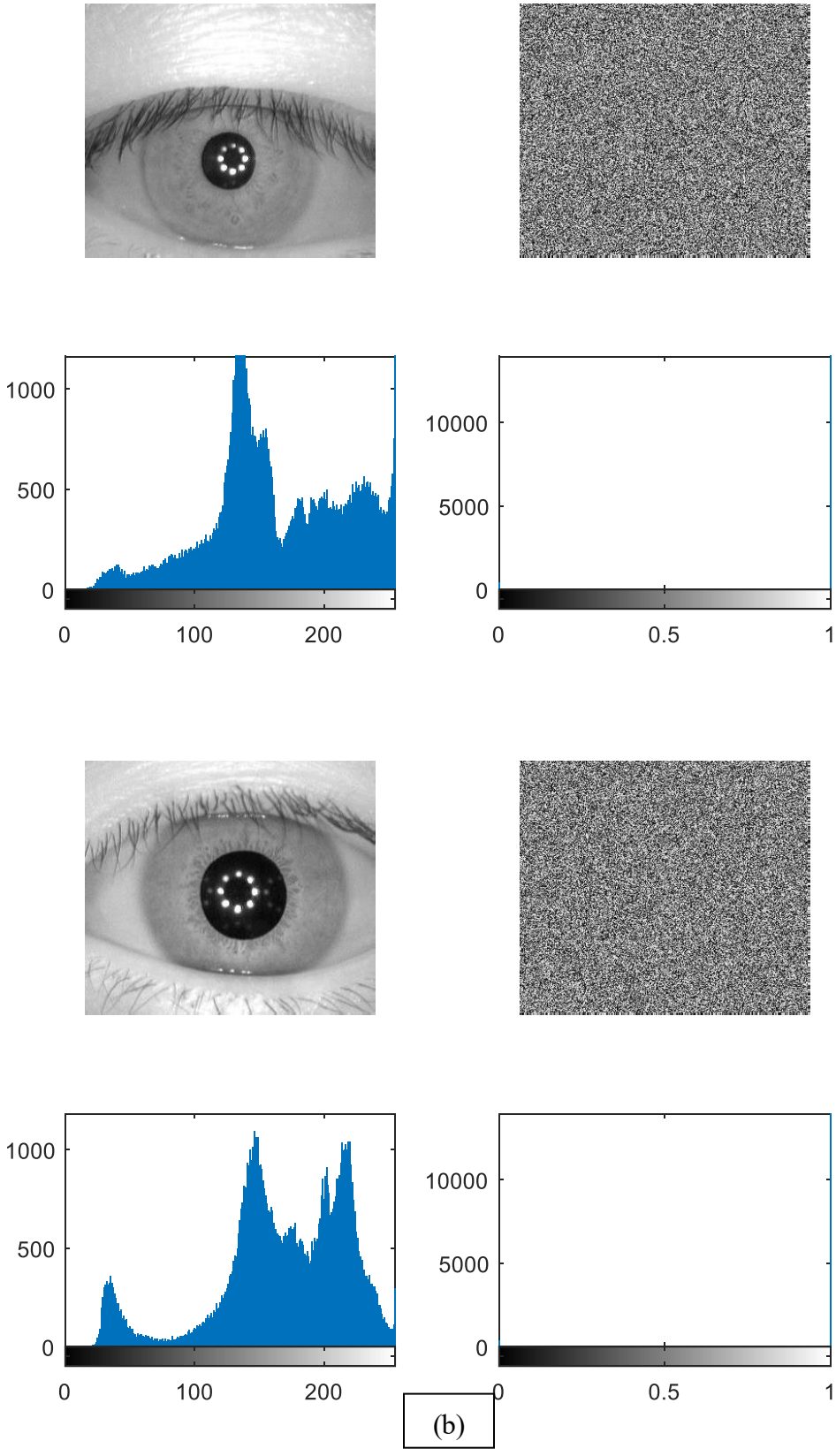


Figure 4-10 : Résultats de chiffrement des empreintes (a) et L'iris (b).

4.5.2 Résultats de la simulation :

Un bon algorithme de cryptographie devrait être capable de chiffrer différents types de textes en un texte chiffré semblable à du bruit. Dans nos expériences, les données binaires et les données décimales sur 8 bits (par exemple, les images) sont utilisées comme texte en clair pour tester les performances de chiffrement du TL-DEA proposé [37]. La simulation a été réalisée avec MATLAB R2015a sur le système d'exploitation Windows 10 Pro.

Pour chiffrer des données binaires, nous utilisons une image binaire à titre d'exemple. Étant donné qu'une image binaire est représentée par une matrice 2-D, elle peut être traitée comme un bloc de données et être soumise directement au chiffrement par bloc. Nous pouvons constater que les données binaires 0 et 1 dans l'information chiffré sont réparties de manière aléatoire dans toutes les positions. Aucune information sur les données d'origine n'est présente [37].

TL-DEA peut également chiffrer des données avec d'autres formats tels que des images numériques et des vidéos. Leurs pixels sont généralement représentés par 8 bits ou plus. TL-DEA peut les chiffrer directement au niveau des pixels, ce qui est plus efficace et pratique que ceux au niveau des bits. La figure 4-10 montre les résultats de chiffrement des empreinte digitale et L'iris. Comme on peut le voir, les empreintes digitales et L'iris chiffrées ont une apparence de bruit visuel avec une répartition uniforme des données. Les données d'origine sont protégées avec un haut niveau de sécurité [37].

4.5.3 Analyse de sécurité :

La sécurité est la propriété la plus importante d'un système de cryptographie. Un bon système de cryptographie devrait avoir la capacité de résister à différentes attaques bien connues.

Pour démontrer la performance en matière de sécurité de TL-DEA proposé, nous utilisons des images numériques représentées sur 8 bits comme exemples pour effectuer une analyse de sécurité, y compris le test de sensibilité des clés, l'analyse des attaques différentielles, ainsi que des attaques de bruit et de perte de données [37].

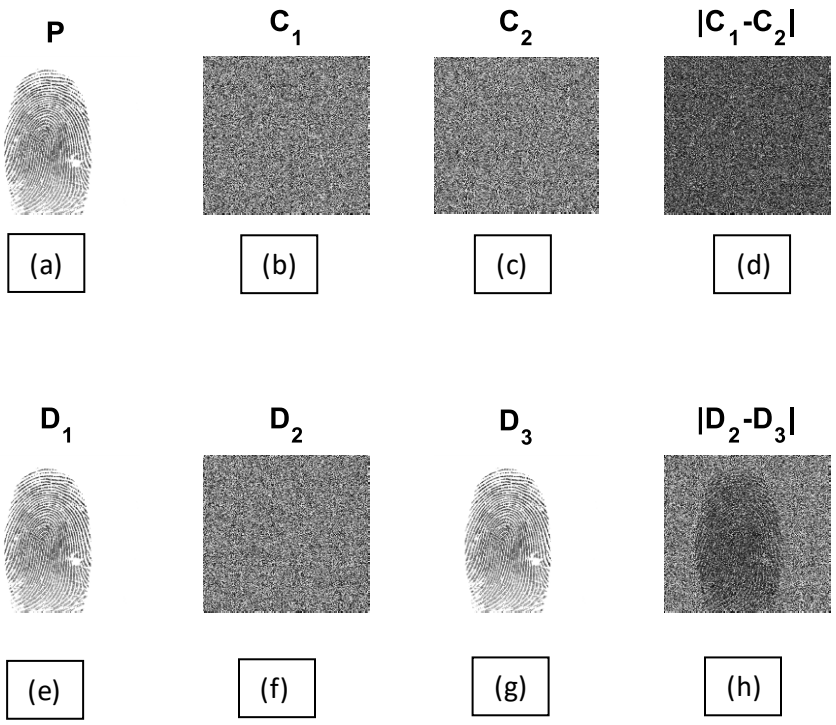
4.5.3.1 Test de sensibilité des clés :

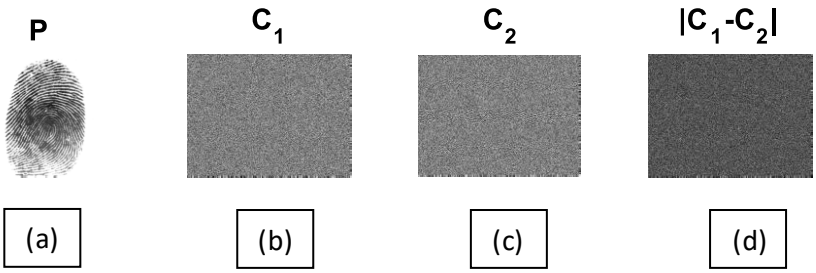
Un algorithme de chiffrement doit être sensible à ses clés de sécurité. La sensibilité des clés peut être testée dans les processus de chiffrement et de déchiffrement :

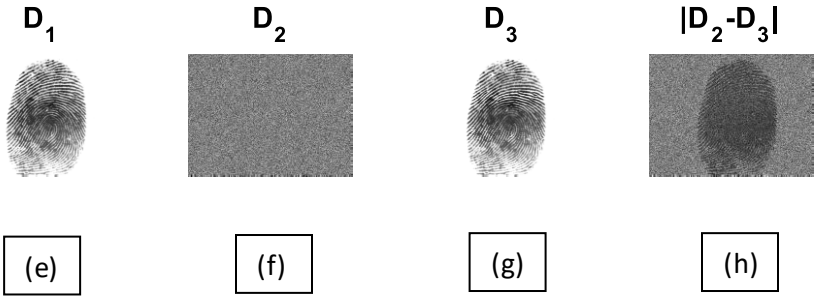
- sensibilité de la clé de chiffrement, ce qui signifie qu'un léger changement dans les clés de chiffrement produira un texte chiffré complètement différent.
- sensibilité de la clé de déchiffrement, ce qui signifie que le texte en clair d'origine ne peut être récupéré que lorsque les bonnes clés de sécurité sont utilisées,

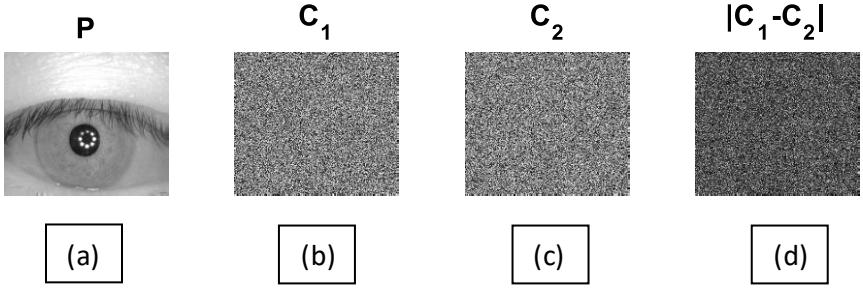
et qu'un léger changement des clés de sécurité entraînera un résultat de déchiffrement non reconnu.

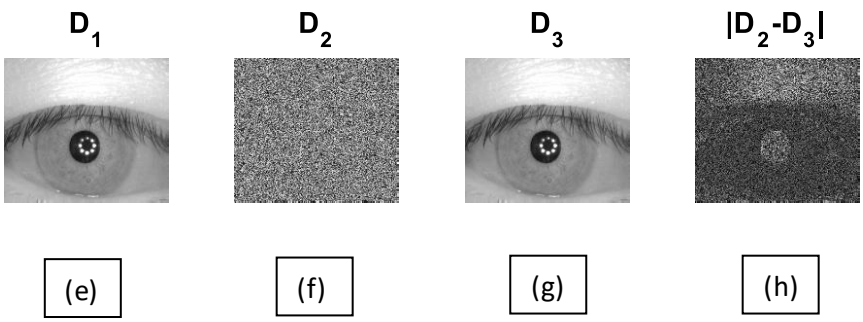
Les résultats de l'analyse de sensibilité des clés sont présentés dans la Figure 4-11 . K2 et K3 sont deux clés de sécurité différentes générées à partir de la clé de sécurité K1 avec un changement d'un seul bit. Comme on peut le voir,




P
C1
C2
|C1-C2|
(a)
(b)
(c)
(d)


D1
D2
D3
|D2-D3|
(e)
(f)
(g)
(h)


P
C1
C2
|C1-C2|
(a)
(b)
(c)
(d)


D1
D2
D3
|D2-D3|
(e)
(f)
(g)
(h)

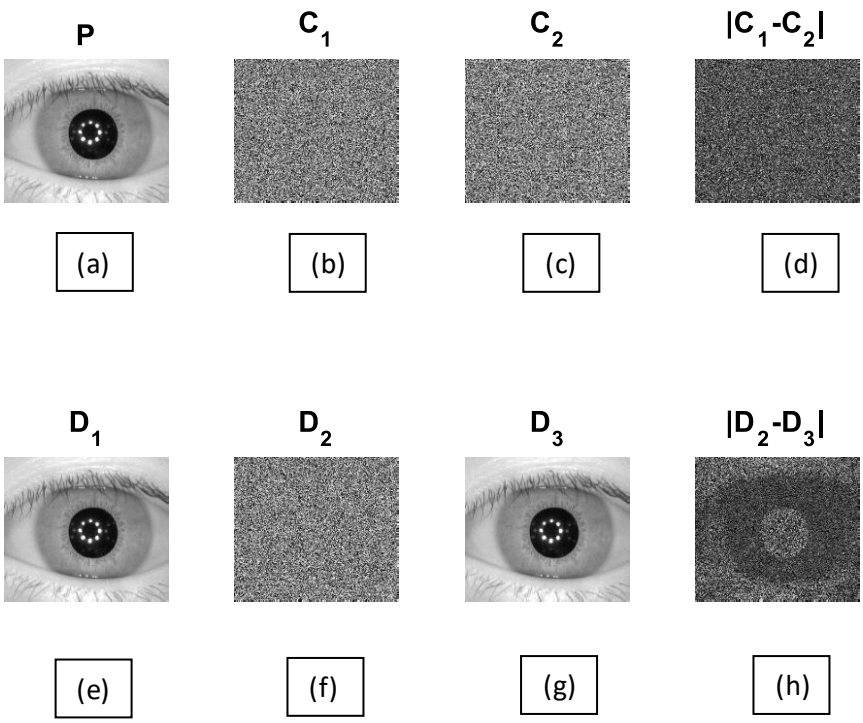


Figure 4-11 : Analyse de la sensibilité des clés. (a) Image en texte clair P. (b) Image en texte chiffré C1 avec K1. (c) Image en texte chiffré C2 avec K2. (d) Différence entre les images chiffrées, |C1 - C2|. (e) Image déchiffrée D1 à partir de C1 avec K1. (f) Image déchiffrée D2 à partir de C1 avec K2. (g) Image déchiffrée D3 à partir de C1 avec K3. (h) Différence entre les images déchiffrées, |D2 - D3|.

Lorsqu'une image en texte clair P [Figure 4-11 (a)] est chiffrée en utilisant K2 et K3 avec une différence d'un seul bit, on obtient deux résultats chiffrés totalement différents, comme le montrent les Figures 4-11 (b) et (c). La Figure 4-11 (d) montre leurs différences. D'autre part, lorsqu'une image en texte chiffré [Figure 4-11 (b)] est déchiffrée par deux clés de sécurité avec une différence d'un seul bit, on obtient également deux résultats déchiffrés totalement différents, comme le montrent les Figures 4-11 (f) et (g). Seule la clé de sécurité correcte peut reconstruire le texte clair d'origine, comme le montre la Figure 4-11 (e). Par conséquent, le TL-DEA proposé est sensible à ses clés de sécurité dans les processus de chiffrement et de déchiffrement.

4.5.3.2 Analyse de l'attaque différentielle :

Un système de cryptographie doté d'une excellente propriété de diffusion peut résister aux attaques différentielles. Pour évaluer quantitativement la propriété de diffusion de TL-DEA, nous utilisons le taux de changement du nombre de pixels (NPCR) et l'intensité moyenne modifiée unifiée (UACI) [37]. Mathématiquement, le NPCR et l'UACI de deux images $\boldsymbol{C_1}$ et $\boldsymbol{C_2}$ sont définis comme suit :

$$\mathbf{NPCR}\ (\boldsymbol{C_1}, \boldsymbol{C_2}) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\boldsymbol{D(i,j)}}{\boldsymbol{L}} \times \mathbf{100\%} \tag{21}$$

$$\mathbf{UACI}(\boldsymbol{C_1}, \boldsymbol{C_2}) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|\boldsymbol{C_1(i,j)} - \boldsymbol{C_2(i,j)}|}{\boldsymbol{T} \times \boldsymbol{L}} \times \mathbf{100\%} \tag{22}$$

$$\boldsymbol{D(i,j)} = \begin{cases} \mathbf{0}, & \mathbf{if} \boldsymbol{C_1(i,j)} = \boldsymbol{C_2(i,j)} \\ \mathbf{1}, & \mathbf{if} \boldsymbol{C_1(i,j)} \neq \boldsymbol{C_2(i,j)} \end{cases} \tag{23}$$

où $\boldsymbol{C_1}$ et $\boldsymbol{C_2}$ sont deux images chiffrées qui sont générées à partir de deux images en clair avec une différence d'un pixel, $\boldsymbol{T}$ désigne l'intensité de pixel maximale autorisée et $\boldsymbol{L}$ représente le nombre total de pixels dans l'image. NPCR mesure le pourcentage de pixels différents entre les deux images chiffrées, tandis que l'UACI teste les intensités modifiées.

Les images en clair proviennent de l'ensemble de données d'images diverses USC-SIPI. Pour chaque image de test, un pixel est mis à zéro pour générer une nouvelle image de test, puis TL-DEA avec la même clé de sécurité est appliqué aux deux images [37]. Les deux résultats chiffrés sont ensuite mesurés par NPCR et UACI.

Nom de fichier (L'empreinte)	NPCR %	UACI %
empriente1.tif	99.5925	33.5221
empriente2.tif	99.5732	33.4574
empriente3.tif	99.6536	33.3889
empriente4.tif	99.5983	33.4354
empriente5.tif	99.6116	33.4733
Moyenne	**99.6058**	**33.4554**

Tableau 4-2 : Résultats NPCR et UACI de TL-DEA avec les images de texte clair de l'ensemble de données d'images des emprientes.

Nom de fichier (L'iris)	NPCR %	UACI %
iris1.jpg	99.6104	33.3876
iris2.jpg	99.6216	33.5481
iris3.jpg	99.6004	33.3258
iris4.jpg	99.6093	33.3781
iris5.jpg	99.5970	33.4016
Moyenne	**99.6077**	**33.4082**

Tableau 4-3 : Résultats NPCR et UACI de TL-DEA avec les images de texte clair de l'ensemble de données d'images des iris.

Les Tableaux (4-2 et 4-3) montrant les résultats des mesures. Comme on peut le voir, les valeurs moyennes de NPCR et UACI sont respectivement de [**99.6058**% et **33.4554**%] pour les empreintes et [**99.6077**% et **33.4082**%] pour les iris. Elles sont extrêmement proches des valeurs théoriques idéales de NPCR et UACI (99,609% et 33,464%) prouvées dans [32]. Cela démontre que TL-DEA possède d'excellentes propriétés de diffusion et est capable de résister à une attaque différentielle.

4.5.3.3 Attaques de bruit et de perte de données :

Presque tous les canaux de transmission de données sont des canaux bruités [33]. Lorsque des données sont transmises sur des canaux bruités, elles sont facilement contaminées par le bruit. Il y a également des pertes de données pendant la transmission et le stockage des données. Par conséquent, il est important qu'un algorithme de chiffrement soit capable de résister aux attaques de bruit et de perte de données.

Pour tester les performances de résistance aux attaques de bruit et de perte de données, nous comparons TL-DEA avec trois algorithmes de chiffrement existants : l'AES [34], l'algorithme de Liao et al. [35] et l'algorithme de Wu et al. [36].

4.6 Conclusion :

Dans ce chapitre, nous avons simulé un nouveau système chaotique en cascade (CCS). Ce système est capable de générer un grand nombre de cartes chaotiques 1-D différentes en combinant deux cartes chaotiques 1-D existantes. Nous avons présenté trois exemples de cartes chaotiques générées par le CCS et les avons analysés. Les résultats de l'évaluation et de la comparaison ont démontré que les nouvelles cartes chaotiques générées sont plus imprévisibles, présentent une meilleure performance chaotique, ainsi que des paramètres et des propriétés chaotiques plus complexes que les cartes chaotiques existantes.

Nous avons ensuite montré comment le CCS proposé peut bénéficier des applications basées sur le chaos. En utilisant la carte Tent-Logistic comme exemple de carte chaotique du CCS, nous avons introduit TLPRNG (Tent-Logistic map-based Pseudo Random Number Generator) et TL-DEA (Tent-Logistic map-based Data Encryption Algorithm). Nous avons également évalué les performances de TL-DEA en termes de chiffrement de données et d'analyse de sécurité. Les résultats ont démontré que TL-DEA est capable de protéger différents types de données avec un haut niveau de sécurité, en résistant aux attaques différentielles ainsi qu'aux attaques de bruit et de perte de données.

Ce chapitre met en évidence l'importance et l'efficacité du CCS dans l'amélioration de la sécurité de la transmission des images biométriques. Les résultats obtenus soutiennent l'utilisation des techniques de cryptage chaotiques basées sur le CCS pour renforcer la confidentialité et la protection des données biométriques lors de leur transmission.

Bibliographie

[1] :E. Ott, Chaos dans les systèmes dynamiques. New York, NY, États-Unis: Cambridge Univ. Presse, 2002.

[2] :Q. Tao, Z. Sun et K. Kong, "Développer des algorithmes d'apprentissage via optimisé «IEEE Trans. Syst., Homme, Cybern. B, Cybern., Vol. 42, non. 1, pp. 140-149, février 2012.

[3] :K.-Y. Lian, T.-S. Chiang, C.-S. Chiu, et P. Liu, "Synthèse de floue conceptions à base de modèles pour la synchronisation et la sécurisation des communications pour Systèmes chaotiques, "IEEE Trans System, Homme, Cybern B, Cybern., Vol. non. 1, pp. 66-83, février 2001.

[4] :S.-L. Chen, T. Hwang et W.-W. Lin, "amélioration Randomness en utilisant "IEEE Trans Circuits System II, Exp. Mémoires, vol. 57, non. 12, pages 996-1000, déc. 2010.

[5] :T. Addabbo et al., «Une classe de congruence non linéaire à période maximale générateurs dérivés de la carte chaotique de Rényi, "IEEE Trans. Syst. I, Reg. Papiers, vol. 54, no. 4, pages 816-828, avril 2007.

[6] :R. Bose et S. Pathak, «Un nouveau système de compression et de cryptage utilisant un codage arithmétique à modèle variable et un système chaotique couplé, " IEEE Trans. Circuits Syst. I, Reg. Papiers, vol. 53, no. 4, pp. 848-857, Avril 2006.

[7] :K.-W. Wong, Q. Lin et J. Chen, "Codage arithmétique simultané et le cryptage en utilisant des cartes chaotiques, "IEEE Trans Circuits System II, Exp. Mémoires, vol. 57, non. 2, pp. 146-150, février 2010.

[8] :Y. Zhou, L. Bao, et C. L. P. Chen, "Un nouveau système chaotique 1D pour cryptage d'image, "Signal Process., volume 97, pages 172-182, avril 2014.

[9] :R. C. Hilborn, le chaos et la dynamique non linéaire: une introduction pour Scientifiques et ingénieurs, 2e éd. New York, NY, États-Unis: Oxford Univ. Presse, 2001.

[10] :Y. Wu, Y. Zhou et L. Bao, "Système chaotique à commutation de roues discrètes et applications, "Circuits IEEE Trans. I, Reg. Papiers, à être publié

[11] :D. Arroyo, R. Rhouma, G. Alvarez, S. Li et V. Fernandez, «Sur la sécurité d'un nouveau schéma de chiffrage d'image sur une carte chaotique treillis, "Chaos, volume 18, numéro 3, septembre 2008, article ID 033112.

[12] :H. C. Papadopoulos et G.W. Wornell, «Estimation du maximum de vraisemblance d'une classe de signaux chaotiques, "IEEE Trans. Inf. Théorie, volume 41, non. 1, pp. 312-317, janv. 1995.

[13] :X. Wu, H. Hu et B. Zhang, "estimation de des séquences symboliques générées par le système de chaos ", Chaos Soliton. vol. 22, non. 2, pages 359-366, oct. 2004.

[14] :G. Chen et X. Yu, Contrôle du chaos: théorie et applications, vol. 292. Berlin, Allemagne: Springer, 2003.

[15] :H.-K. Chen et C.-I. Lee, "Anti-contrôle du chaos dans le mouvement du corps rigide" Chaos Soliton. Fract., Vol. 21, non. 4, pages 957 à 965, 2004.

[16] :C. Shen, S. Yu, J. Lu et G. Chen, «Une méthodologie systématique pour la construction de systèmes hyperchaotiques avec plusieurs positifs Lyapunov Exposants et la mise en œuvre du circuit », IEEE Trans. Circuits Syst. I, Reg. Papiers, vol. 61, no. 3, pp. 854-864, mars 2014.

[17] :T. Gao et Z. Chen, «Un nouvel algorithme de cryptage d'image sur hyper-chaos », Phys., Lettonie A, volume 372, n ° 4, pp. 394-400, janvier 2008.

[18] :Y. Zhou, L. Bao et C. L. P. Chen, «Cryptage d'image en utilisant un nouveau système de commutation paramétrique, "Signal Process., volume 93, numéro 11, pp. 3039-3052, 2013.

[19] :G. Jakimoski et K. P. Subbalakshmi, «exposant discret de Lyapunov et cryptanalyse différentielle, "IEEE Circuits Circuits II, Exp. vol. 54, no. 6, pages 499-501, juin 2007.

[20] :J. Amigo, L. Kocarev et J. Szczepanski, "exposant discret de Lyapunov". et la résistance à la cryptanalyse différentielle, "IEEE Trans. Circuits Syst. II, Exp. Mémoires, vol. 54, no. 10, pages882 à 886, oct. 2007

[21] :A. Muchnik et S. Y. Positselsky, «l'entropie de Kolmogorov dans le contexte de la théorie dela calculabilité, "Theor, Comput, Sci., volume 271, numéro 12, pp. 15-35, 2002.

[22] :R. Frigg, "En quoi l'entropie de Kolmogorov-Sinaï est-elle une mesure pour un comportement chaotique? Combler le fossé entre les systèmes dynamiques théorie et théorie de la communication, "Brit. J. Philos. Sci., Vol. 55, non. 3, pp. 411-434, 2004.

[23] :J. Gao, J. Hu et W.-W. Tung, "Mesures d'entropie pour le signal biologique analyses, "Dyn. non linéaire, vol. 68, non. 3, pp. 431-444, 2012.

[24] :C.-Y. Li, J.-S. Chen, et T.-Y. Chang, "Un pseudo-aléatoire basé sur le chaos générateur de nombres utilisant la méthode de réensemencement basée sur la synchronisation, "dans Proc. IEEE Int. Symp. Circuits Syst., Pp. 3277-3280, île de Kos, Grèce, 2006.

[25] :Norme IEEE pour l'arithmétique en virgule flottante, norme IEEE 754-2008, 2008, pp. 1-70.

[26] :I. Lawrence et al., "SP 800-22 Rév. 1a. Une suite de tests statistiques aléatoires et des générateurs de nombres pseudo-aléatoires pour les applications cryptographiques " Nat. Inst. Supporter. Technol., Gaithersburg, MD, États-Unis, Tech. NIST Rep. SP 800-22, 2010.

[27] :P. L'Ecuyer et R. Simard, "TestU01: Une bibliothèque C pour les tests empiriques des générateurs de nombres aléatoires, "ACM Trans. Math. Softw., Vol. 33, non. 4, p. 22, 2007.

[28] :J. M. Bahi, X. Fang, C. Guyeux, et Q. Wang, "Qualité aléatoire" des générateurs chaotiques CI: Applications à la sécurité internet, "in Proc. 2ème Int. Conf. Evol. Internet(INTERNET), 2010, pp. 125-130.

[29] :Q. Wang, C. Guyeux et J. M. Bahi, «Un nouveau nombre pseudo-aléatoire générateur basé sur des itérations chaotiques discrètes », dans Proc. 1er Int. Conf. Evol. Internet (INTERNET), 2009, pp. 71-76.

[30] :J. Lu et G. Chen, «Un modèle de réseau dynamique complexe variant dans le temps. et ses

critères de synchronisation contrôlés, "IEEE Trans. Autom. Contrôle, vol. 50, non. 6, pages 841 à 846, juin 2005.

[31] :Y. Zhou, K. Panetta, S. Agaian, et C. L. P. Chen, "(n, k, p) -Gray code pour les systèmes d'image, "IEEE Trans. Cybern., Vol. 43, non. 2, pp. 515-529, Avril 2013.

[32] :C. Fu et al., «Un système de chiffrement d'image numérique basé sur le chaos avec une stratégie de diffusion améliorée, "Opt. Express, vol. 20, non. 3, pp. 2363-2378, 2012.

[33] :R. C. Gonzalez et R. E. Woods, Traitement d'images numériques, 3e éd. Harlow, Royaume-Uni: Prentice-Hall Inc., 2007.

[34] Advanced Encryption Standard (AES), FIPS PUB 197, 2001.

[35] :X. Liao, S. Lai, et Q. Zhou, "Un algorithme de cryptage d'image roman basé sur la transmission d'onde auto-adaptative, "Signal Process., vol. 90, non. 9, pp. 2714-2722, 2010.

[36] :Y. Wu, G. Yang, H. Jin, et J. P. Noonan, "cryptage d'image en utilisant la carte chaotique logistique bidimensionnelle, "J. Electron. Imagerie, vol. 21, non. 1, 2012, Art. ID 013014.

[37] :Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, “Cascade chaotic system with applications,” IEEE Transactions on Cybernetics, vol. 45, no. 9, pp. 2001–2012, 2015.

Conclusion generale :

En conclusion, cette recherche a exploré les concepts fondamentaux de la sécurité de transmission des images biométriques et l'importance du cryptage dans ce domaine. Nous avons examiné les différentes techniques biométriques utilisées pour l'identification et l'authentification des individus, en mettant l'accent sur la nécessité de protéger ces données sensibles contre les attaques potentielles.

Dans le cadre de cette étude, nous avons approfondi notre compréhension du cryptage et de la cryptographie, en particulier en ce qui concerne l'utilisation de systèmes chaotiques en cascade pour renforcer la sécurité. Le cryptage chaotique en cascade offre une approche prometteuse pour améliorer la sécurité de la transmission des images biométriques, en rendant les données illisibles pour les personnes non autorisées.

À travers nos résultats et discussions, nous avons constaté que l'utilisation du cryptage chaotique en cascade présente plusieurs avantages en termes de sécurité. Ce processus garantit la confidentialité des données en transformant les images biométriques en un format crypté complexe et en perturbant les corrélations potentielles. De plus, la sensibilité aux conditions initiales et aux paramètres des systèmes chaotiques utilisés renforce la sécurité du cryptage.

Cependant, il est important de noter que le cryptage chaotique en cascade n'est pas exempt de limitations et de défis. Des recherches supplémentaires sont nécessaires pour étudier en détail les performances de ce type de cryptage dans des scénarios réels, en tenant compte de facteurs tels que la vitesse de traitement, la résistance aux attaques avancées et la compatibilité avec les systèmes existants.

En fin de compte, cette recherche ouvre des perspectives intéressantes pour l'amélioration de la sécurité de transmission des images biométriques. Le cryptage chaotique en cascade offre une approche innovante pour protéger les données sensibles, en garantissant leur confidentialité et leur intégrité. Cependant, il reste encore beaucoup à faire pour optimiser cette technique et l'adapter aux exigences spécifiques des applications biométriques. Des efforts continus de recherche et de

développement sont nécessaires pour renforcer la sécurité des systèmes de transmission des images biométriques et garantir la protection des informations personnelles.