REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Seddik BEN YAHIA de Jijel
Faculté: Sciences et Technologie
Département: Electronique

Mémoire présenté en vue de l'obtention du diplôme de Master en Télécommunication

Option : Systèmes des Télécommunications

Thème

Compression et Cryptage des vidéos : application en IoT.

Encadré par :
Pr. Karim Kemih

Réalisé par :
Badis Amarouche

2020-2021

Remerciements

Au terme de ce travail je tiens à remercier au premier lieu le bon dieu miséricordieux qui m'a éclairé le bon chemin, pour m'avoir donné le courage et la volonté à amener ce travail à bon terme.

Mes vifs remerciements à mes parents et à ma famille d'avoir donné jour après jour autant d'amour, de soutien et d'encouragement,

Mes vifs remerciements sont aussi adressés à mon encadreur Mr. Karim KEMIH qui m'a proposé le thème de ce mémoire pour ses orientations, ses conseils, ses remarques judicieuses et sa disponibilité, je tiens à lui exprimer ma profonde gratitude en vue du bon déroulement du travail durant l'élaboration de ce mémoire.

Je tiens à exprimer ma parfaite considération aux membres de jury pour avoir accepté de me consacrer une partie de leurs temps, afin d'examiner et de juger ce modeste travail.

Je voudrais remercier tous les enseignants qui ont contribué énormément à ma formation de près ou de loin en particulier les enseignants du département d'électronique.

Enfin je remercie toute personne ayant participé de près ou de loin à l'élaboration de ce travail.

Compression et Cryptage des vidéos : application en IoT

Résumé

Le développement des systèmes de télécommunications a permis le déploiement de certains services sur internet comme la vidéo conférence, et a aussi permis l'émergence de l'internet des objets. Ce développement a mené à une grande Augmentation du nombre des flux vidéos échangés dans le réseau mondial.

Cette augmentation pose deux problèmes majeurs ; Le 1er problème étant la taille de ces flux vidéo qui pose elle-même deux problèmes ; concernant le stockage et la saturation du réseau.

Le 2eme problème concerne la sécurité de ces flux vidéos, vu leur importance, leur valeur ou leur confidentialité.

Notre objectif dans ce travail est donc de résoudre ces deux problèmes en réalisant un algorithme de compression et de cryptage vidéo pour réduire la taille des vidéos et pour les sécuriser.

Notre approche de compression est basée sur la transformation en ondelette, tandis que l'approche de cryptage se base sur le cryptage chaotique.

Les résultats des simulations des évaluations de la qualité de compression et du cryptage montrent l'efficacité de l'approche proposée.

ضغط وتشفير الفيديو: تطبيق في إنترنت الأشياء

ملخص

لقد مكّن تطوير أنظمة الاتصالات السلكية واللاسلكية من نشر بعض خدمات الإنترنت مثل مؤتمرات الفيديو ، كما أتاح ظهور إنترنت الأشياء. أدى هذا التطور إلى زيادة كبيرة في عدد تدفقات الفيديو المتبادلة في الشبكة العالمية.

هذه الزيادة تطرح مشكلتين رئيسيتين ؛ المشكلة الأولى هي حجم تدفقات الفيديو هذه والتي تطرح في حد ذاتها مشكلتين ؛ فيما يتعلق بالتخزين وتشبع الشبكة.

المشكلة الثانية تتعلق بأمن تدفقات الفيديو هذه ، بالنظر إلى أهميتها أو قيمتها أو سريتها.

لذلك فإن هدفنا في هذا العمل هو حل هاتين المشكلتين من خلال تصميم خوارزمية ضغط وتشفير الفيديو لتقليل حجم مقاطع الفيديو وتأمينها.

يعتمد نهج الضغط لدينا على تحويل المويجات ، بينما يعتمد نهج التشفير على الخرائط الفوضوية.

تظهر نتائج عمليات محاكاة جودة الضغط وتقييمات التشفير فعالية النهج المقترح.

Compression and Encryption of videos: application in IoT

Abstract

The development of telecommunications systems has enabled the deployment of certain Internet services such as video conferencing, and has enabled the emergence of the Internet of Things. This development has led to a great increase in the number of video streams exchanged in the global network.

This increase poses two major problems; the first problem being the size of these video streams which itself poses two problems; concerning storage and network saturation.

The second problem concerns the security of these video streams, given their importance, their value or their confidentiality.

Our objective in this work is therefore to solve these two problems by realizing a video compression and encryption algorithm to reduce the size of the videos and to secure them.

Our compression approach is based on wavelet transformation, while the encryption approach is based on chaotic encryption.

The results of the simulations of the compression quality and encryption evaluations show the effectiveness of the proposed approach**.**

Liste des abréviations

AES: Advance Encryption Standard

AVC: Advanced Video Coding

CIF: Common Intermediate Format

CSK: chaos shift keying

DCT**:** discrete cosine transform

DES: Data Encryption Standard

DPCM: Differential pulse-code modulation

DWT**:** discrete wavelet transform

ECC: Elliptic curve cryptography

EXI: Efficient XML Interchange

FPGA: field programmable gate array

GSM: Global System for Mobile Communications

HEVC: High Efficiency Video Coding

IEEE: Institute of Electrical and Electronics Engineers

IoT: Internet of things

IoV: internet of vehicles

IP: internet protocol

ISO: International Organization for Standardization

JPEG: Joint Photographic Experts Group

LTE: long term-evolution

MIMO: multi-in multi-out

MPEG: Moving Picture Experts Group

MSE: Mean square error

NFC: Near-field communication

NIST: National Institute of Standards and Technology

OWL: Web Ontology Language

PIN personal identification number

PSNR: Peak signal to noise ratio

RDF: Resource Description Framework

RFID: Radio-frequency identification

RGB : Red green blue

RNIS : Réseau numérique à intégration de services

RTOS: Real-time operating system

SBC: single-board computer

SSIM : Structural SIMilarity

SVH : système visuel humain

TCP : Transmission Control Protocol

TIC : Technologie de l'information et de la communication

UID : Unique identifier (identifiant unique)

UMTS: Universal Mobile Telecommunications System

UWB: ultra-wide bandwidth

VEA: video encrypting algorithm

WSN: wireless sensor network

XML: Extensible Markup Language

Sommaire

Liste des figures

Liste des tableaux

Introduction générale

Le développement exponentiel des systèmes de télécommunications a permis le déploiement de certains services sur internet comme la visioconférence ou les plateformes de vidéo en ligne, de plus avec l'arrivée de l'internet des objets, le nombre des flux vidéos devient de plus en plus énorme.

L'internet des objets est un nouveau concept dans lequel des objets sont reliés par un réseau, n'importe quel objet pouvant envoyer ou recevoir des informations ou pouvant être contrôlé, peut être un objet IoT, par exemple : les capteurs ; thermostat, capteur de mouvement ou une caméra. Des objets qu'on peut contrôler tel qu'une porte, une ampoule ou un climatiseur…etc. font aussi partie des objets IoT. Les informations collectées par les capteurs sont transmises vers le cloud ou bien traité localement (par des microcontrôleurs ou des microprocesseurs) pour la prise de décision concernant les objets connectés, un simple exemple est le contrôle de température à l'aide d'un thermostat et un climatiseur.

Un système IoT comprend plusieurs éléments nécessaires à sa fonctionnalité, on site parmi ces éléments :

- L'identification ; chaque objet doit être identifié et avoir une adresse dans le réseau.
- La détection ; collection des données par les objets connectés.
- La communication ; technologies utilisées pour la transmission des données collectées
- Traitement ; élément constitué d'une partie matérielle et une autre logicielle qui traitent les données pour décider des actions à prendre.
- Les services ; élément lié au traitement de données et dépend de l'application de l'IoT.
- La sémantique ; traitement et modélisation des métadonnées pour fournir de meilleurs services.

L'internet des objets a de nombreuses applications ayant le potentiel de changer la vie quotidienne et de développer plusieurs secteurs comme la santé, la sécurité ou l'industrie.

Les maisons intelligentes par exemple peuvent améliorer la vie quotidienne grâce à des applications comme la surveillance, le contrôle de température, l'éclairage intelligent…etc. un autre exemple est la ville intelligente qui améliore les transports publics et la sécurité et permet d'économiser l'énergie grâce à l'éclairage intelligent. Une autre application importante est la santé intelligente qui permet l'analyse et la surveillance à distance grâce à des capteurs et à un système de surveillance. Il existe d'autres applications comme les voitures intelligentes ou l'industrie intelligente…etc.

La caméra joue un rôle important dans la majorité des applications de l'IoT, surtout avec le développement de l'intelligence artificielle qui permet d'extraire plusieurs informations des vidéos enregistrées.

Le nombre et la diversité des flux vidéos circulant dans le réseau mondial pose deux problèmes majeurs. Le premier est la taille de ces flux vidéo qui doit être réduite considérablement pour éviter les problèmes de stockage et de saturation des réseaux. Le deuxième problème concerne la sécurité de certains de ces flux vidéos, vu leur importance, leur valeur ou leur confidentialité, les vidéos stockés devrait être cryptées et donc sécurisées contre tout essai de piratage.

Une vidéo est une succession d'images caractérisée par le nombre de pixels dans chaque image, le type de codage de chaque pixel (chaque pixel est codé sur 24 bits dans le cas d'une image RGB) et le nombre d'images affichées par seconde.

Chaque vidéo contient différents types de redondances, le but de la compression est de réduire la taille d'une vidéo, ce qui revient à éliminer ces redondances. En gros il existe deux types de compression ; la compression sans perte où la vidéo reste identique à l'original, ce type consiste à éliminer les redondances de codage, le codage de Huffman et le codage arithmétique font partie des méthodes de compression sans perte. Le deuxième type est la compression avec perte où la qualité se dégrade, plus le taux de compression est élevé ; plus une vidéo est compressée moins il y a de détails. Cette compression consiste à éliminer les redondances de façon permanente, les standards JPEG, JPEG2000 et H264 font partie des méthodes de compression avec perte.

Pour la compression vidéo nous avons deux approches ; la première consiste à éliminer les redondances existantes dans une seule image (redondances spatiales) et la deuxième consiste à éliminer les redondances existantes entre les images successives (redondances temporelles).
L'une des compressions les plus utilisées est la compression par transformé en ondelettes, utilisée dans les standard JPEG2000 et Motion JPEG 2000, on obtient des taux de compression assez

élevé tout en gardant une bonne qualité d'image, ces standards ne prennent pas en compte les redondances temporelles contrairement aux standards MPEG, et H.264…etc. qui éliminent les redondances entre les images successives.

La nécessité du cryptage vidéo a augmenté avec la croissance du nombre des flux vidéos, sécuriser une vidéo consiste à la rendre illisible ; même si un pirate arrive à s'emparer de la vidéo ses données resteront inintelligibles. En général il existe deux type de cryptographie ; La cryptographie à clé symétrique utilisée dans les normes DES, AES…etc. dans ce type le chiffrement et le déchiffrement se font par la même clé. Et la cryptographie à clé asymétrique utilisée dans les normes RSA, ECC…etc. dans ce type on utilise deux clé, une publique qui peut être partagée et une autre secrète.

L'une des approches de cryptographie qui prend du terrain est la cryptographie chaotique qui se base sur les systèmes chaotiques qui ont des caractéristiques idéales pour le cryptage :

- Sensible aux condition initiales ; un changement fractionnel cause de grands changements dans le système.
- Système déterministe ; comportement irrégulier mais pas aléatoire.
- Apériodique à long terme ; la trajectoire a une prévisibilité très limitée

Il existe plusieurs techniques de cryptage chaotique comme le cryptage par addition, par inclusion ou par décalage…etc.

La cryptographie et la compression des vidéos sont souvent associés, l'algorithme de cryptage est soit appliqué avant, pendant ou après l'algorithme de compression.

Dans le cadre de notre travail de fin d'études, on s'intéresse au cryptage et à la compression des vidéos pour le stockage dans le cadre des applications IoT.

La vidéo sera décomposée en images, et chaque image décomposée en trois matrices de couleurs, chaque matrice est ensuite compressée par un algorithme basé sur la transformation en ondelette.

Ensuite chaque matrice sera cryptée avec un algorithme de confusion (permutations de pixels) puis un algorithme de diffusion (modification des valeurs des pixels) le cryptage sera fait par une clé symétrique générée par un système chaotique. En fin les matrices de couleurs puis les images seront rassemblées pour former la vidéo cryptée.

Nous allons finalement étudier l'efficacité de notre approche avec des évaluations objectives comme le PSNR, le MSE et le SSIM pour la compression, et l'histogramme, l'entropie les coefficients de corrélation pour le cryptage.

Organisation du mémoire

Ce mémoire est structuré en quatre chapitres encadrés par une introduction générale et une conclusion générale.

Dans le premier chapitre nous allons présenter les différents aspects de l'internet des objets en définissant ce que c'est un objet IoT, comment marche un système IoT et de quoi il se compose, en suite on va donner un bref historique et un aperçu sur le marché de l'IoT. Puis on va détailler l'architecture et les éléments constitutifs de l'IoT. En fin nous allons parler de quelques applications de cette technologie ainsi que des défis que posent ces applications.

Le deuxième chapitre se focalise sur les techniques de compression, nous allons en premier donner des notions sur la vidéo, ensuite on va parler des différentes redondances dans la vidéo et puis des différents types de compression, en particulier la compression par transformé en ondelette. Enfin nous allons présenter quelques standards utilisés pour la compression d'image et de vidéos.

Le troisième chapitre concerne les techniques de cryptage, nous allons expliquer le besoin de cryptage vidéo, ensuite on va présenter la cryptographie, sa relation avec la compression et les type d'algorithme de cryptage existants. Puis on va parler de la cryptanalyse et des différentes attaques qui existent. Enfin on va présenter la cryptographie chaotique en définissant les systèmes chaotiques et leurs caractéristiques et puis en parlant de quelques techniques de cryptage chaotiques.

Le dernier chapitre sera réservé pour la présentation et l'étude de l'approche proposée où nous allons expliquer l'algorithme principale proposé ensuite le principe de compression par ondelette, et puis le principe de cryptage chaotique. On va ensuite discuter des critères d'évaluations des algorithmes de compression et de cryptage. Enfin nous allons présenter les résultats des simulations, des évaluations de qualité de compression ; PSNR, MSE et SSIM. Et des évaluations de qualité de cryptage ; histogramme, corrélations, et entropie.

Chapitre 1

Etat de l'art sur l'internet des objets

1.1. Introduction :

L'Internet évolue rapidement vers le futur « Internet des objets » (IoT), qui mettra potentiellement en réseau des milliards voire des billions d'appareils. Plus de 50 milliards appareils se connecteront à Internet d'ici 2025. La plupart de ces appareils seront situés à la périphérie d'Internet et pourraient fournir de nouvelles applications, modifiant de nombreux aspects des productions industrielles traditionnelles et de notre vie quotidienne. Certains appareils qui sont déjà apparus incluent les montres Apple, les casques Oculus Rift, Google Nest et les lunettes Google. Les objets IoT peuvent en fait être n'importe quel type de capteurs et de puces avec diverses habilités créées par différents fabricants, et de nombreuses applications peuvent être créées pour permettre la mise en œuvre des maisons intelligentes, des soins intelligents, des transports intelligents, des villes intelligentes...etc. [1]

1.2. L'internet des objets

L'Internet des objets (IoT) est un concept reflétant un ensemble connecté de n'importe qui, n'importe quoi, n'importe quand, n'importe où, n'importe quel service, et tout réseau. C'est un système de dispositifs informatiques interdépendants, de machines mécaniques et numériques, d'objets, d'animaux ou de personnes qui sont dotés d'identifiants uniques (UID) et de la capacité de transférer des données sur un réseau sans nécessiter d'interaction entre humains ou entre l'homme et l'ordinateur. [2] [3]

1.2.1. Qu'est-ce qu'un objet ?

Presque n'importe quel objet physique peut être transformé en objet d'IoT s'il peut être connecté à Internet pour être contrôlé ou pour communiquer des informations. Une ampoule qui peut être allumée à l'aide d'une application pour smartphone est un appareil IoT, tout comme un capteur de mouvement ou un thermostat intelligent ou un lampadaire connecté. Un appareil IoT peut être aussi simple qu'un jouet d'enfant ou aussi sérieux qu'un camion sans conducteur. Certains objets plus grands peuvent eux-mêmes être remplis de nombreux composants IoT plus petits, comme un moteur à réaction qui est maintenant rempli de milliers

de capteurs collectant et transmettant des données pour s'assurer de l'efficacité du fonctionnement. À une échelle encore plus grande, les projets de villes intelligentes remplissent des régions entières de capteurs pour aider à comprendre et à contrôler l'environnement. [4]

1.2.2. Comment ça marche ?

Un écosystème IoT se compose d'appareils intelligents compatibles avec le Web qui utilisent des systèmes embarqués, tels que des processeurs, des capteurs et du matériel de communication, pour collecter, envoyer et agir sur les données qu'ils acquièrent de leurs environnements. Les appareils IoT partagent les données de capteurs qu'ils collectent en se connectant à une passerelle IoT ou à un autre appareil périphérique où les données sont soit envoyées au cloud pour être analysées ou bien analysées localement. Parfois, ces appareils communiquent avec d'autres appareils associés et agissent sur les informations qu'ils obtiennent les uns des autres. Les appareils font la plupart du travail sans intervention humaine, bien que les gens puissent interagir avec les appareils - par exemple, pour les configurer, leur donner des instructions ou accéder aux données. [3]

1.2.3. Historique

Le terme IoT a été entendu pour la toute première fois en 1999 mais l'idée de connecter des appareils intelligents existait avant, en 1990, le premier appareil connecté à l'internet a été créé par John Romkey, cet appareil était un grille-pain qui pouvait être allumé et éteint sur Internet. En 1994, Steve Mann a inventé 'Wear Cam ', une caméra portable ayant une performance en temps quasi réel utilisant un système de processeur 64 bits.

En 1997, la première description des capteurs identifié par Paul Saffo, mais le terme IoT a été inventé par Kevin Ashton en 1999 lors de son travail chez Procter & Gamble (P&G), Kevin travaillait sur l'optimisation de la chaîne logistique, il a essayé d'attirer l'attention de sa direction sur la nouvelle technologie passionnante appelée "RFID" en même temps l'Internet était le sujet le plus populaire en 1999, cette situation l'a incité à promouvoir sa présentation pour le concept de l'IoT. Bien que cette idée ait attiré l'attention de certains Dirigeants de P&G, le terme IoT n'a été utilisé publiquement qu'après une décennie.

En 1999, le livre "Quand les choses commencent à penser" était publié par Neil Girchenfeld, qui illustre les principes de l'IoT. De plus, en 2000, le plan concernant sa première génération de réfrigérateurs Internet annoncée par l'entreprise 'LG'.

En (2003-2004), la RFID a été déployée à grande échelle par le département américain de la Défense dans le programme Savi et par l'entreprise de vente au détail 'Walmart' dans le monde

commercial. En 2005 L'Union internationale des télécommunications a publié le premier rapport sur le thème de l'IoT. En 2008-2009, L'IoT est né selon le groupe de solutions commerciales de Cisco. [5]

1.2.4. Marché de l'IoT:

L'internet des objets joue un rôle essentiel dans les futurs projets des entreprises. Pour cela, les bénéfices attendus de l'IoT sont largement répandus. Les avantages offerts par l'IoT sont énormes et peuvent augmenter les bénéfices de toute organisation, en particulier ceux axés sur la transformation numérique comme indiqué dans le tableau 1.1 prévisionnel qui se concentre sur la plupart des secteurs concerné par l'IoT, indiquant en même temps le développement du Marché de l'IoT, les dépenses par secteur et la croissance attendue par Applications grand public et industrielles, en milliards de dollars de 2020 à 2030.

Il est évident que le marché de l'IoT devient de plus en plus grand. Par conséquent, les grandes entreprises commencent déjà à investir dans les différents secteurs de l'internet des objets.

Le tableau de prévision et les chiffres montrent que la taille du marché de l'IoT est variée, énorme, et en croissance constante. [5]

Marché de l'IoT en milliard de dollars							
	2020	2022	2024	2026	2028	2030	Taux de croissance
Prévisions du marché mondial de l'IoT	245	585	1,110	2178.13	4208.37	8,131	39%
Taille du marché	457.29	874.28	1671.47	3195.57	6109.38	11680.1	38%
Taille du marché mondial dans l'industrie	119	223	424.7	797.12	1496.13	2808.1	37%
par Secteur (en millions of dollars)							
Automobile	1325.2	1536.62	1,780	2066.06	2395.68	2777.9	7.70%
Construction & Infrastructure	103.31	303.23	890	1174.98	1551.2	2047.9	14.90%
Énergie et services publics	103.31	303.23	890	2335.72	6129.86	16087.2	62%
Industriel et Fabrication	690.57	783.97	890	1009.45	1144.93	1298.6	6.50%
Santé et style de vie	915.57	1105.57	1,335	1824.36	2493.11	3407	16.90%
Electronique grand public	1687.75	1937.84	2,225	3150.83	4461.89	6318.5	19%
Vente au détail	59.2	229.54	890	3013.18	10201.44	34538	84%
Croissance attendue de l'IoT par application grand public et industrielle (en milliards de dollars)							
base installée IoT par catégorie	3,010	4756.1	7515.13	11874.66	18763.17	29647.7	25,7%
Base installée IoT par consommateur	1,534	2100.86	2877.2	3940.41	5396.52	7390.7	14%
Base installée IoT par industrie	1,476	2979.46	6014.36	12140.62	24507.12	49470.2	42%

Tableau 1.1 : prévision sur la taille du marché de l'IoT par secteur 2020-2030 [5]

1.3. Architecture

De nos jours, l'internet utilise la pile de protocoles TCP / IP pour la communication entre les hôtes du réseau. Cependant, l'IoT connecte des milliards d'objets, ce qui va créer un trafic beaucoup plus grand et un stockage de données beaucoup plus important sera nécessaire. En outre, l'IoT sera confronté à de nombreux défis spécialement liés à la confidentialité et à la sécurité. Ainsi, la nouvelle architecture proposée pour l'IoT doit prendre en compte de nombreux facteurs comme l'évolutivité, l'interopérabilité, la fiabilité, la qualité de service, etc. Puisque l'IoT connecte tous et chacun pour échanger des informations entre eux, le trafic et les stockages dans le réseau augmenteront également de manière exponentielle. Ainsi, le développement de l'IoT dépend des progrès technologiques et de la conception de diverses nouvelles applications et modèles commerciaux. [6]. L'architecture de base de l'IoT est composée de 3 couches : la couche de perception, la Couche réseau et la couche Application, comme illustré dans la figure1.1.

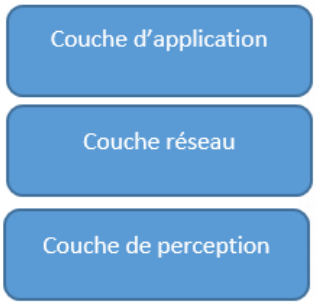

Figure 1.1 : L'architecture de base d'un système IoT [7]

Généralement, la structure moderne de l'IoT est divisée en 5 couches, comme le montre la figure 1.2.

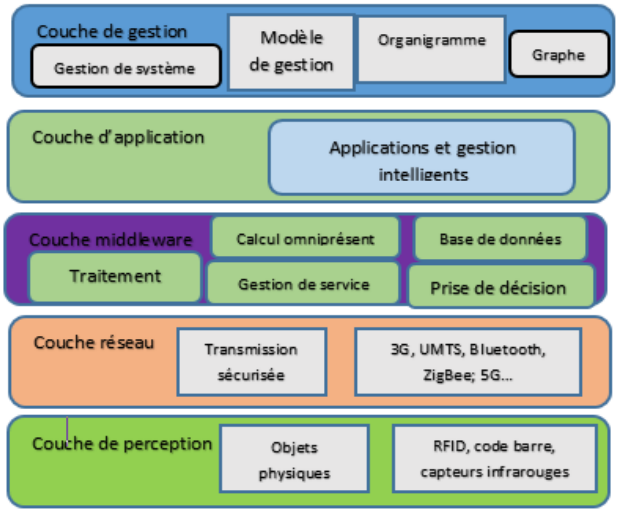

Figure 1.2: la structure moderne de l'IoT divisée en 5 couches

1.3.1 Couche de perception: également connue sous le nom de « couche de périphérique », elle se compose des objets physiques et des capteurs. Les capteurs peuvent être des capteurs RFID, à code barre 2D ou infrarouge selon la méthode d'identification des objets. Cette couche traite essentiellement de l'identification et de la collecte d'informations spécifiques aux objets par les dispositifs de détection. Selon le type de capteurs, les informations peuvent concerner l'emplacement, la température, l'orientation, le mouvement, les vibrations, l'accélération, l'humidité, les changements chimiques dans l'air, etc. Les informations collectées sont ensuite transmises à la couche réseau pour leur transmission sécurisée au système de traitement de l'information.

1.3.2 Couche réseau: également appelée « couche de transmission ». Cette couche transfère en toute sécurité les informations des capteurs au système de traitement de l'information. Le support de transmission peut être filaire ou sans fil et la technologie peut être la 5G, Wifi, Bluetooth, infrarouge, ZigBee, etc., en fonction des capteurs. Ainsi, la couche Réseau transfère les informations de la couche Perception vers la couche Middleware.

1.3.3 Couche middleware (intergiciel) : les appareils sur l'IoT implémentent différents types de services. Chaque appareil se connecte et ne communique qu'avec les autres appareils qui implémentent le même type de service. Cette couche est responsable de la gestion des services et a un lien vers la base de données. Elle reçoit les informations de la couche réseau et les stocke dans la base de données. Elle effectue le traitement de l'information et le calcul ubiquitaire et prend une décision automatique en fonction des résultats.

1.3.4 Couche Application: cette couche fournit une gestion globale de l'application basée sur les informations sur les objets traitées dans la couche Middleware. Les applications mises en œuvre par l'IoT peuvent être la santé intelligente, l'agriculture intelligente, la maison intelligente, la ville intelligente, le transport intelligent, etc.

1.3.5 Couche Gestion: cette couche est responsable de la gestion du système IoT global, y compris les applications et les services. Il construit des modèles commerciaux, des graphiques, des organigrammes, etc. en fonction des données reçues de la couche Application. Le vrai succès de la technologie IoT dépend également des bons modèles commerciaux. Sur la base de l'analyse des résultats, cette couche aidera à déterminer les futures actions et stratégies commerciales. [6]

1.4. Les Eléments de l'IoT

Comprendre les éléments constitutifs de l'IoT permet de mieux comprendre sa signification et ses fonctionnalités. L'IoT nécessite six éléments principaux comme illustré dans la figure 1.3

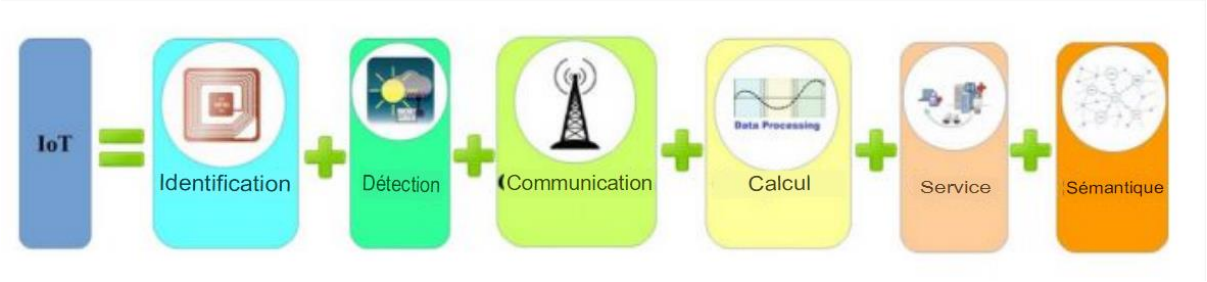

Figure 1.3 : les élements de l'IoT

Le tableau 1.2 montre les catégories de ces éléments et des exemples de chaque catégorie.

Les éléments de l'IoT		Exemples
Identification	Dénomination	EPC, uCode
	Adressage	IPv4, IPv6
Captage		Capteurs intelligents, dispositifs de détection portables, capteurs intégrés, actionneurs, RFID
communication		RFID, NFC, UWB, Bluetooth, IEEE 802.15.4, Z-Wave, Wi-Fi, LTE-A
Traitement	Materiel	Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, SmartPhones
	Logiciel	os (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop)
Service		lié à l'identité (expédition), agrégation d'informations (réseau électrique intelligent), collaboratif (maison intelligente), omniprésent (ville intelligente)
sémantique		RDF, OWL, EXI

Tableau 1.2 : les catégories des éléments de l'IoT et des exemples de chaque catégorie

1.4.1 L'identification

L'identification est cruciale pour que l'IoT nomme et associe les services à leurs demandes. De nombreuses méthodes d'identification sont disponibles pour l'IoT comme les codes de produits électroniques et les codes ubiquitaires (uCode). En outre, l'adressage des objets IoT est essentiel pour différencier l'identité de l'objet et son adresse. L'identité d'objet fait référence à son nom tel que « T1 » pour un capteur de température particulier et l'adresse de l'objet fait référence à son adresse dans un réseau de communication.

Les méthodes d'adressage des objets IoT incluent IPv6 et IPv4. 6LoWPAN fournit un mécanisme de compression sur les en-têtes IPv6 qui rend l'adressage IPv6 approprié pour les réseaux sans fil à faible puissance. Il est impératif de faire la distinction entre l'identification de l'objet et l'adressage, car les méthodes d'identification ne sont pas uniques au monde. L'adressage aide à identifier les objets de manière unique. De plus, les objets du réseau peuvent utiliser des adresses IP publiques et non privées. Des méthodes d'identification sont utilisées pour fournir une identité claire pour chaque objet du réseau.

1.4.2 La Détection

La détection consiste à collecter des données à partir des objets associés dans le réseau et de les renvoyer vers une base de données ou au cloud. Les données collectées sont analysées pour prendre des mesures spécifiques en fonction des services requis. Les capteurs IoT peuvent être des capteurs intelligents, des actionneurs ou des dispositifs de détection portables. Par exemple, des entreprises comme *Wemo*, *revolv* et *SmartThings* proposent des hubs intelligents et des applications mobiles qui permettent aux gens de surveiller et de contrôler des milliers d'appareils et d'appareils intelligents à l'intérieur des bâtiments à l'aide de leurs smartphones. Les ordinateurs à carte unique (SBC) avec des capteurs et des fonctionnalités TCP/IP et de sécurité intégrées, sont généralement utilisés pour réaliser des produits IoT (par exemple, Arduino Yun, Raspberry PI, BeagleBone Black, etc.). Ces appareils se connectent généralement à un portail de gestion central pour fournir les données requises par les clients.

1.4.3 La communication

Les technologies de communication de l'IoT connectent des objets hétérogènes entre eux pour fournir des services intelligents spécifiques. En générale, les nœuds IoT doivent fonctionner avec une faible puissance en présence de liaisons de communication avec des pertes et du bruit.

Les protocoles de communication utilisés pour l'IoT sont ; Wifi, Bluetooth, IEEE 802.15.4, Z-wave, LTE-Advanced, etc. Certaines technologies de communication spécifiques sont également utilisées comme la RFID, la communication en champ proche (NFC) et la bande passante ultra-large (UWB).

- La RFID est la première technologie utilisée pour réaliser le concept M2M (étiquette et lecteur RFID). L'étiquette RFID représente une simple puce ou une étiquette attachée pour fournir l'identité de l'objet. Le lecteur RFID transmet un signal d'interrogation à l'étiquette et reçoit un signal réfléchi de l'étiquette, qui à son tour est transmis à la base de données. La base de données se connecte à un centre de traitement pour identifier les objets sur la base des signaux réfléchis dans une plage (10 cm à 200 m). Les étiquettes RFID peuvent être actives, passives ou semi-passives/actives. Les tags actifs sont alimentés par batterie tandis que les passifs n'ont pas besoin de batterie. Les tags semi-passifs / actifs utilisent l'alimentation de la carte en cas de besoin.
- Le protocole NFC fonctionne sur la bande haute fréquence à 13,56 MHz et prend en charge un débit de données jusqu'à 424 kbps. La portée applicable est jusqu'à 10 cm où la communication entre les lecteurs actifs et les balises passives ou deux lecteurs actifs peut avoir lieu.

- La technologie UWB est conçue pour prendre en charge les communications dans une zone de couverture à faible portée utilisant une faible énergie et une bande passante élevée dont les applications pour connecter des capteurs ont été récemment augmentées
- Le Wifi utilise des ondes radio pour échanger des données entre les objets à moins de 100m. Le Wifi permet aux appareils intelligents de communiquer et d'échanger des informations sans utiliser de routeur dans certaines configurations ad hoc.
- Le Bluetooth représente une technologie de communication utilisée pour échanger des données entre appareils sur de courtes distances à l'aide d'une radio à courte longueur d'onde afin de minimiser la consommation d'énergie. Récemment, le groupe d'intérêt spécial a produit Bluetooth 4.1 qui fournit un Bluetooth à basse consommation ainsi qu'une connectivité haut débit et IP pour prendre en charge l'IoT.
- La norme IEEE 802.15.4 spécifie à la fois une couche physique et un contrôle d'accès pour les réseaux sans fil de faible puissance ciblant des communications fiables et évolutives.
- LTE (Long-Term Evolution) est à l'origine une communication sans fil standard pour le transfert de données à haut débit entre téléphones mobiles basée sur les technologies de réseau GSM / UMTS. Il peut couvrir les appareils à déplacement rapide et fournir des services de multidiffusion et de diffusion. LTE-A (LTE Advanced) est une version améliorée de LTE comprenant une extension de bande passante qui prend en charge jusqu'à 100 MHz, le multiplexage spatial en liaison descendante et montante, une couverture étendue, un débit plus élevé et des latences plus faibles. [8]
- 6LoWPAN : 6LowPAN est une technologie de réseau qui combine le protocole Internet (IPv6) avec les réseaux personnels sans fil à faible consommation (LoWPAN), qui est l'une des technologies les plus appropriées pour le déploiement de l'IoT. C'est un bon choix pour les petits appareils dont les capacités de traitement et de transmission sont limitées.
- 5G : La cinquième génération sans fil est la dernière itération de la technologie cellulaire basée sur la norme de réseau sans fil IEEE 802.11ac afin d'améliorer le débit de données et de réduire la latence. L'évolution à long terme (LTE) et la sortie multiple à entrées multiples (MIMO) sont utilisées comme base dans le réseau 5G, ainsi que le découpage du réseau. [9]

1.4.4 Traitement de données

Les unités de traitement (par exemple, les microcontrôleurs, les microprocesseurs, les FPGA) et les applications logicielles représentent le « cerveau » et la capacité de calcul de l'IoT. Diverses plateformes matérielles ont été développées pour exécuter des applications IoT telles que Arduino, UDOO, FriendlyARM, Intel Galileo, Raspberry PI, Gadgeteer, etc. En outre, de nombreuses plateformes logicielles sont utilisées pour fournir des fonctionnalités IoT. Parmi ces plateformes, les systèmes d'exploitation sont vitaux car ils fonctionnent pendant toute la durée d'activation d'un appareil. Il existe plusieurs systèmes d'exploitation en temps réel (RTOS) qui sont de bons candidats pour le développement d'applications IoT. Par exemple, le Contiki RTOS a été largement utilisé dans les scénarios IoT. Contiki a un simulateur appelé Cooja qui permet aux chercheurs et aux développeurs de simuler et d'émuler les applications IoT et de réseau de capteurs sans fil (WSN). TinyOS, LiteOS et Riot OS proposent également un système d'exploitation léger conçu pour les environnements IoT. De plus, certains leaders de l'industrie automobile avec Google ont établi l'Open Auto Alliance et prévoient d'apporter de nouvelles fonctionnalités à la plateforme Android pour accélérer l'adoption du paradigme de l'Internet des véhicules (IoV).

Les plateformes cloud constituent une partie de traitement de données importante de l'IoT. Ces plateformes permettent aux objets intelligents d'envoyer leurs données dans le cloud, de traiter les mégadonnées en temps réel et, éventuellement, aux utilisateurs de bénéficier des connaissances extraites des mégadonnées collectées. Il existe de nombreuses plateformes et infrastructures cloud gratuites et commerciales pour héberger des services IoT.

1.4.5 Les services

En général, les services IoT peuvent être classés en quatre classes : Services liés à l'identité, services d'agrégation d'informations, services collaboratifs et conscients et services omniprésents.

Les services liés à l'identité sont les services les plus élémentaires et les plus importants qui sont utilisés dans d'autres types de services. Chaque application qui a besoin d'amener des objets du monde réel dans le monde virtuel doit identifier ces objets.

Les services d'agrégation d'informations collectent et résument les mesures sensorielles brutes qui doivent être traitées et rapportées à l'application IoT.

Les services collaboratifs et conscients agissent en plus des services d'agrégation d'informations et utilisent les données obtenues pour prendre des décisions et réagir en conséquence.

Les services omniprésents, cependant, visent à fournir des services collaboratifs à chaque fois qu'ils sont nécessaires à quiconque en a besoin n'importe où.

Le but ultime de toutes les applications IoT est d'atteindre le niveau des services omniprésents. Cependant, cette fin n'est pas facilement réalisable car il y a beaucoup de difficultés et de défis à relever. La plupart des applications existantes fournissent des services liés à l'identité, à l'agrégation d'informations et à la collaboration. Les soins de santé et les Réseau électrique intelligent entrent dans la catégorie de l'agrégation d'informations et la maison intelligente, les bâtiments intelligents, les systèmes de transport intelligents et l'automatisation industrielle sont plus proches de la catégorie de la collaboration.

1.4.6 La Sémantique

La sémantique dans l'IoT fait référence à la capacité d'extraire intelligemment des connaissances par différentes machines pour fournir les services requis. L'extraction des connaissances comprend la découverte et l'utilisation des ressources et la modélisation des informations. En outre, cela comprend la reconnaissance et l'analyse des données pour donner un sens à la bonne décision de fournir le service exact. Ainsi, la sémantique représente le cerveau de l'IoT en envoyant des demandes à la bonne ressource. Cette exigence est prise en charge par les technologies du Web sémantique telles que le Resource Description Framework (RDF) et le Web Ontology Language (OWL). En 2011, le consortium World Wide Web (W3C) a adopté le format Efficient XML Interchange (EXI) comme recommandation. EXI est important dans le contexte de l'IoT car il est conçu pour optimiser les applications XML pour les environnements aux ressources limitées. En outre, il réduit les besoins en bande passante sans affecter les ressources associées telles que la durée de vie de la batterie, la taille du code, l'énergie consommée pour le traitement et la taille de la mémoire. EXI convertit les messages XML en binaire pour réduire la bande passante nécessaire et minimiser la taille de stockage requise. [8]

1.5. Applications

Les Applications IoT gagnent largement du terrain dans des domaines tels que les villes intelligentes, les bâtiments intelligents, les transports et les infrastructures, l'industrie, la santé, la sécurité, etc. L'application de l'IoT dans des domaines pertinents pourrait considérablement améliorer la vie quotidienne. Des gains économiques importants s'accompagnent également dans les domaines de l'industrie, les transports, la santé et de l'agriculture.

1.5.1 Villes intelligentes

De nombreuses grandes villes ont été soutenues par des projets intelligents, comme Séoul, New York, Tokyo, Amsterdam et Dubaï. Les villes intelligentes peuvent encore être considérées comme les villes du futur. La demande des villes intelligentes nécessite une planification

minutieuse à chaque étape, avec le soutien des gouvernements et des citoyens pour mettre en œuvre la technologie de l'Internet des objets dans tous ses aspects. Grâce à l'IoT, les villes peuvent être améliorées à plusieurs niveaux, en améliorant les infrastructures et les transports publics, en réduisant la congestion routière et en gardant les citoyens en sécurité, en bonne santé et plus engagés dans la communauté. En connectant tous les systèmes dans les villes comme le système de transport, le système de santé, les systèmes de surveillance météorologique, etc., en plus d'aider les gens par Internet en tout lieu à accéder à la base de données des aéroports, des chemins de fer, du suivi des transports, les villes deviendront plus intelligentes grâce à l'internet des objets. [10]

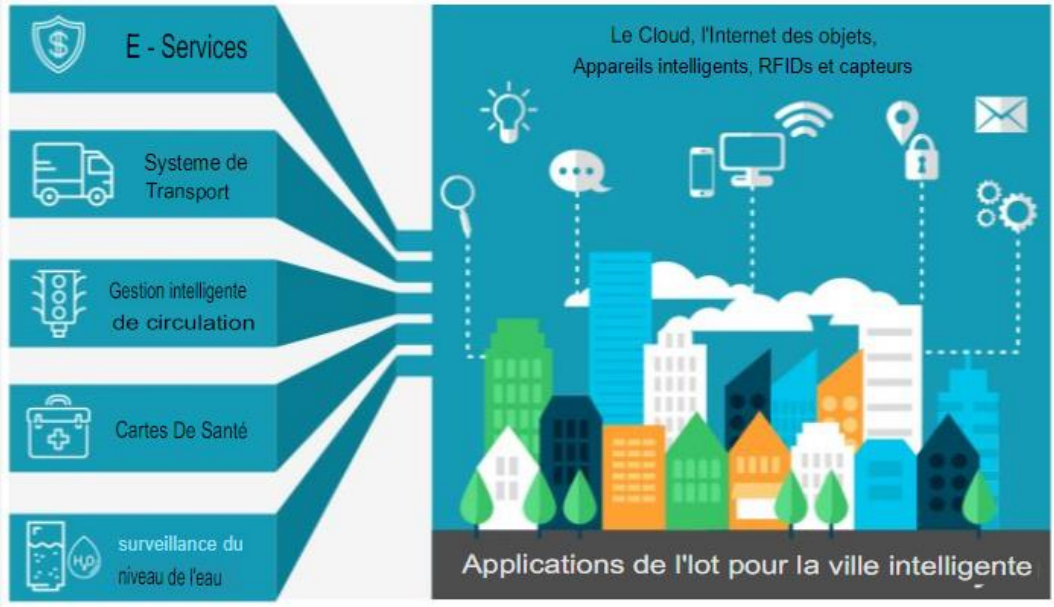

Figure 1.4 : application de l'IoT pour les villes intelligentes [11]

1.5.2 Maison et bâtiments intelligents

Les technologies Wi-Fi dans la domotique ont été utilisées principalement en raison de la nature en réseau des appareils électroniques tels que les téléviseurs, les appareils mobiles, qui sont généralement pris en charge par le Wi-Fi. Le Wi-Fi fait partie du réseau IP domestique et en raison du taux croissant d'adoption d'appareils informatiques mobiles tels que les smartphones, les tablettes, etc. les appareils mobiles garantissent que les consommateurs ont accès à un « contrôleur » portable pour les appareils électroniques connectée au réseau.

De nombreuses entreprises envisagent de développer des plateformes qui intègrent l'automatisation des bâtiments avec le divertissement, la surveillance, les soins de santé, l'économie de l'énergie et la surveillance de capteurs sans fil dans la maison. Grace à l'Internet des objets, les maisons et les bâtiments peuvent faire fonctionner de nombreux appareils et objets intelligemment, tel que l'éclairage intelligent, l'environnement et les médias intelligents,

le contrôle de l'air et du chauffage central, la gestion de l'énergie et la sécurité, comme montré dans la figure 1.5.

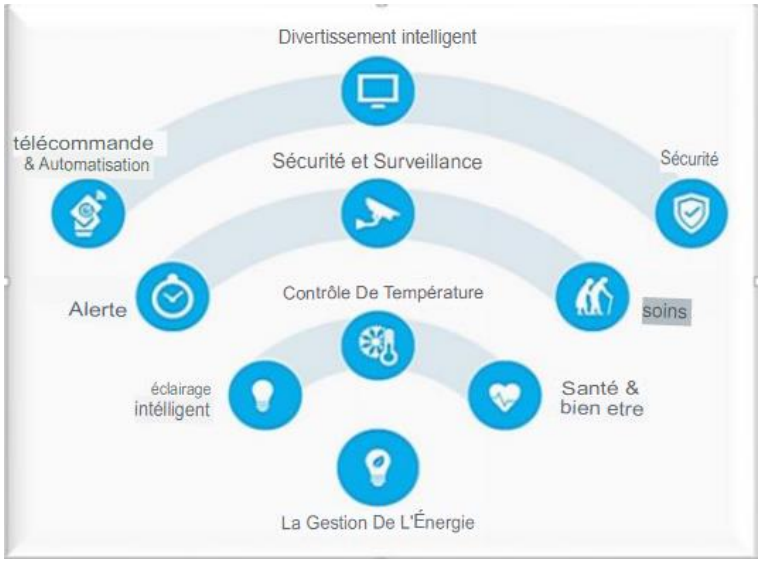

Figure 1.5 : application de l'IoT pour les maisons intelligentes

1.5.3 Les Réseau électrique intelligent

Un réseau électrique intelligent est lié à l'information et au contrôle et développé pour avoir une gestion intelligente de l'énergie. L'intégration des technologies de l'information et de la communication (TIC) au réseau électrique permettra une communication bidirectionnelle en temps réel entre les fournisseurs et les consommateurs, créant une interaction plus dynamique sur les flux d'énergie, ce qui contribuera à fournir de l'électricité de manière plus efficace et durable. Les principaux éléments des TIC comprendront les technologies de détection et de surveillance des flux d'énergie, les compteurs intelligents avec affichage à domicile pour informer sur la consommation d'énergie; des systèmes de coordination, de contrôle et d'automatisation pour agréger et traiter diverses données et pour créer une électricité hautement interactive et réactive. De nombreuses applications peuvent être manipulées en raison de l'Internet des objets pour les réseaux électriques intelligents, telles que le contrôle de l'énergie industriel, solaire, nucléaire, des véhicules, des hôpitaux et des villes.

La figure 1.6 montre les applications les plus importantes réalisable grâce à l'Internet des objets dans l'aspect du réseau électrique intelligent.

Figure 1.6 : application de l'IoT pour les réseaux électriques intelligents

1.5.4 Santé intelligente

Certains patients hospitalisés dont l'état physiologique doit être surveillé en permanence nécessitent une attention particulière qui peut être constamment réalisée en utilisant les technologies de surveillance IoT. Pour la santé intelligente, les capteurs sont utilisés pour collecter des informations physiologiques complètes et utilisent des passerelles et le cloud pour analyser et stocker les informations, puis envoyer les données analysées sans fil aux soignants pour une analyse et un examen plus approfondis. Ceci remplace le processus consistant à faire venir un professionnel de la santé à intervalles réguliers pour vérifier les signes vitaux du patient, offrant au lieu de cela un flux d'informations automatisé continu. De cette manière, il améliore simultanément la qualité des soins grâce à une attention constante et réduit le coût des soins en réduisant le coût des modes de soins traditionnels en plus de la collecte et de l'analyse des données.

De nombreuses personnes dans le monde souffrent de problèmes de santé parce qu'elles n'ont pas facilement accès à une surveillance sanitaire efficace. Mais avec de petits et puissants objets sans fil connectées via l'IoT, il est désormais possible de surveiller ces patients. Ces objets peuvent être utilisées pour capturer en toute sécurité les données de santé des patients à partir d'une variété de capteurs, appliquer des algorithmes complexes pour analyser les données, puis les partager via une connectivité sans fil avec des professionnels de la santé qui peuvent faire des recommandations de santé appropriées.

1.5.5 Transport et mobilité intelligents

La surveillance et l'alerte de l'état des routes est l'une des applications IoT de transport et de mobilité les plus importantes. L'idée principale du concept de transport et de mobilité intelligents est d'appliquer les principes de la Production et de la détection participative. Le processus commence avec l'utilisateur qui identifie son itinéraire et marque certains points comme nids-de-poule ; une cavité dans la chaussée ; sur une application. Le transport intelligent est traité avec trois concepts principaux, à savoir l'analyse des transports, le contrôle des transports et la connectivité des véhicules. L'analyse du transport représente l'analyse de la prévision, de la demande et de la détection des anomalies. L'acheminement des véhicules et le contrôle de la vitesse en plus de la gestion du trafic sont tous connus sous le nom de contrôle des transports qu'ils sont en fait étroitement liés au mode de connectivité des véhicules (communication V2X).

L'IoT peut également être utilisé dans les véhicules électriques, qui sont un moyen important de réduire à la fois le coût du carburant et l'impact du réchauffement climatique.

1.5.6 Usine intelligente et fabrication intelligente (industrie 4.0)

L'usine intelligente a ajouté de nouvelles valeurs dans la révolution de la fabrication en intégrant l'intelligence artificielle, l'apprentissage automatique et l'automatisation du travail de connaissance et de la communication M2M avec le processus de fabrication. L'usine intelligente changera fondamentalement la façon dont les produits sont inventés, fabriqués et expédiés. En même temps, améliorera la sécurité des travailleurs et protégera l'environnement en permettant de faibles émissions et une fabrication à faible incident. Ces progrès dans la manière dont les machines et autres objets communiquent et la manière dont la prise de décision passe des humains aux systèmes techniques signifient que la fabrication devient de nouvelles technologies «plus intelligentes» telles que; L'automatisation, la robotique et la mobilité autonome qui fournissent tous un moyen de fabrication intelligente, mais les communications M2M appliquée par l'internet des objets «industriel» fourniront un sens complet de l'usine intelligente et de fabrication intelligente par le biais du concept des mégadonnées qui, dans ce contexte, fait référence aux possibilités analytiques offertes par le volume et la variété des données générées, par une économie en réseau pour optimiser les processus industriels pour impliquer moins de temps d'arrêt de maintenance, moins de pannes et une consommation d'énergie très réduite. L'industrie intelligente en tant que quatrième génération connue sous le nom d'industrie 4.0 est basée sur des systèmes physiques chiffrés capables de se connecter à Internet. Le concept de l'industrie 4.0 avec l'Internet des objets peut répondre à de grandes attentes pour les industries.

1.6. Les défis de l'IoT

L'application du concept de l'Internet des objets pose certains défis en termes de coût de mise en œuvre, d'évolutivité, de sécurité, etc. L'IoT est également confronté à de nombreux autres défis.

- **Évolutivité**: l'Internet des objets a un concept plus complexe que celui de l'Internet conventionnel, car les objets sont installés dans un environnement ouvert. Les fonctionnalités de base telles que la communication et la découverte de services doivent donc fonctionner de manière tout aussi efficace dans les environnements à petite et à grande échelle. L'IoT nécessite de nouvelles fonctions et méthodes afin d'obtenir un fonctionnement efficace pour l'évolutivité.
- **Auto-organisation**: les objets intelligents ne doivent pas être gérés comme des ordinateurs qui obligent leurs utilisateurs à les configurer et à les adapter à des situations particulières. Les objets mobiles, qui ne sont souvent utilisés que sporadiquement, doivent établir des connexions spontanément et pouvoir s'organiser et se configurer en fonction de leur environnement particulier.
- **Volumes de données**: certaines applications de l'Internet des objets impliqueront une communication peu fréquente, et la collecte d'informations sous forme de réseaux de capteurs, ou sous forme de réseaux logistiques et à grande échelle, collectera d'énormes volumes de données sur des nœuds ou des serveurs de réseau central. Le terme représentant ce phénomène est le big data qui nécessite de nombreux mécanismes opérationnels en plus des nouvelles technologies de stockage, de traitement et de gestion.
- **Interprétation des données**: pour accompagner les utilisateurs d'objets intelligents, il est nécessaire d'interpréter le plus précisément possible le contexte local déterminé par les capteurs. Pour que les fournisseurs de services profitent de diverses données qui seront générées, il faut pouvoir tirer des conclusions généralisables à partir des données de capteurs interprétées.
- **Interopérabilité**: chaque type d'objets intelligents dans l'Internet des objets a des capacités d'information, de traitement et de communications différentes. Différents objets intelligents seraient également soumis à différentes conditions telles que la disponibilité d'énergie et les besoins en bande passante de communication. Pour

faciliter la communication et la coopération de ces objets, des normes communes sont nécessaires.

- **Découverte automatique**: dans les environnements dynamiques, les services adaptés aux objets doivent être automatiquement identifiés, ce qui nécessite des moyens sémantiques appropriés pour décrire leurs fonctionnalités.
- **Complexité logicielle**: une infrastructure logicielle plus étendue sera nécessaire sur le réseau et sur les serveurs d'arrière-plan afin de gérer les objets intelligents et de fournir des services pour les prendre en charge. Cela parce que les systèmes logiciels dans les objets intelligents devront fonctionner avec des ressources minimales, comme dans les systèmes embarqués conventionnels.
- **Sécurité et confidentialité**: Outre les aspects de sécurité et de protection d'Internet tels que la confidentialité des communications, l'authenticité et la fiabilité des partenaires de communication et l'intégrité des messages, d'autres exigences seraient également importantes dans l'Internet des objets. Il est nécessaire d'accéder à certains services ou d'empêcher de communiquer avec d'autres éléments de l'IoT, et les transactions commerciales impliquant des objets intelligents devraient également être protégées des regards indiscrets des concurrents.
- **Alimentation électrique**: les objets se déplacent généralement et ne sont pas connectés à une alimentation électrique, de sorte que leur intelligence doit être alimentée par une source d'énergie autonome. Bien que les transpondeurs RFID passifs n'aient pas besoin de leur propre source d'énergie, leurs fonctionnalités et leur portée de communication sont très limitées. Les espoirs sont tournés vers les futurs processeurs et unités de communication basse consommation pour les systèmes embarqués capables de fonctionner avec beaucoup moins d'énergie.
- **Communications sans fil**: du point de vue énergétique, les technologies sans fil établies telles que le GSM, l'UMTS, le Wi-Fi et le Bluetooth sont beaucoup moins adaptées; les normes WPAN plus récentes telles que ZigBee et d'autres encore en cours de développement peuvent avoir une bande passante plus étroite, et elles utilisent beaucoup moins d'énergie [10].

1.7. Conclusion

Le nouveau concept de l'Internet des objets (IoT) est rapidement en train de gagner du terrain dans notre vie quotidienne ainsi que dans plusieurs domaines, visant à améliorer la

qualité de vie, l'économie et l'industrie, en connectant de nombreux objets intelligents. Cette nouvelle technologie attire de plus en plus d'investisseur grâce à la diversité et à l'impact de ses applications, d'où les grandes estimations de croissance dans le marché mondial. Cependant la récence de cette technologie fait qu'il y a de nombreux défis à surmonter notamment techniques mais aussi économiques et managériaux, pour fournir des services durables sécurisé et surtout efficace.

Références

[1] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, 2018, doi: 10.1109/JIOT.2017.2767608.

[2] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[3] "https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT." .

[4] "https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now." .

[5] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020-2030," *Proc. World Conf. Smart Trends Syst. Secur. Sustain. WS4 2020*, pp. 449–453, 2020, doi: 10.1109/WorldS450073.2020.9210375.

[6] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," *Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012*, pp. 257–260, 2012, doi: 10.1109/FIT.2012.53.

[7] W. D. Fang, W. He, W. Chen, L. H. Shan, and F. Y. Ma, "Research on the application-driven architecture in internet of things," *Front. Artif. Intell. Appl.*, vol. 293, pp. 458–465, 2016, doi: 10.3233/978-1-61499-722-1-458.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[9] B. Nour *et al.*, "A survey of Internet of Things communication using ICN: A use case perspective," *Comput. Commun.*, vol. 142–143, no. October 2018, pp. 95–123, 2019, doi: 10.1016/j.comcom.2019.05.010.

[10] Z. K. A. Mohammed and E. S. A. Ahmed, “Internet of Things Applications, Challenges and Related Future Technologies,” *World Sci. News*, vol. 67, no. 2, pp. 126–148, 2017, [Online]. Available: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.psjd-b638cb4d-d68f-4f4c-afa5-ad309a7c4838%0Ahttps://www.infona.pl/resource/bwmeta1.element.psjd-8c8e8b68-9180-4879-85d8-a7870d5644e9.

[11] https://www.kreyonsystems.com/Blog/iot-applications-for-smart-cities.

Chapitre 2

Etude des différentes techniques de compression

2.1. Introduction

L'une des applications des IoT dans les maisons intelligentes, les usines, la santé intelligente…etc., sont les Systèmes de surveillance, les nouvelles cameras sont désormais équipées de certains capteurs, en plus avec le développement de l'intelligence artificielle les cameras auront un rôle plus important dans l'IoT et par conséquence la taille des vidéos enregistrée, stockée et transmise vers le Cloud deviendra de plus en plus énorme, ce qui rend la compression de ces vidéos indispensables. La compression réduit le temps de transmission, la taille de stockage tout en gardant une qualité d'image acceptable.

2.2. Notions sur la vidéo

Une vidéo est une succession d'images fixes ayant 3 caractéristiques :

- Le nombre de bits réservé pour l'espace couleur (8 bits pour les images en noir et blanc et 24 bits pour les images en couleurs)
- Le nombre de colonnes et de ligne ou le nombre de pixels que comporte chaque image
- Le nombre d'image par seconde

2.3. Les espaces couleurs

Ce sont des représentations des couleurs d'une image on site parmi ces espaces **:**

2.3.1. L'espace RGB

Dans l'espace couleur RGB, chaque pixel est représenté par trois nombres indiquant les proportions relatives du rouge, du vert et du bleu. Ce sont les trois couleurs primaires additives de la lumière.

Chaque couleur est codée sur 8 bits ce qui donne la possibilité d'avoir plus de 16 millions couleurs différentes.

2.3.2. L'espace YCrCb

L'espace couleur Y: Cr: Cb représente les couleurs d'une image plus efficacement en séparant la luminance de la chrominance, ou Y représentant la luminance est obtenue par une moyenne pondérée du R, G et B.

$$Y = Kr\ R + Kb\ B + Kg\ G$$

Où ki sont des facteurs de pondération.

Seules deux des trois composantes de chrominance doivent être transmises : la troisième composante peut toujours être trouvée parmi les deux autres. Dans l'espace Y : Cr : Cb, seules la luminance (Y) et la chrominance rouge et bleue (Cr, Cb) sont transmises. [1]

2.4. Définition de la compression.

La compression consiste à éliminer les redondances dans un signal (audio, image ou vidéo), afin de réduire considérablement la taille de stockage et la bande passante occupé pour la transmission (ou le temps de transmission). Dans le cas de la vidéo il existe deux type de redondance, les redondances statistiques et les redondances psychovisuelles. La compression peut aussi être classée en 2 classes ; la compression sans perte et la compression avec perte.

2.5. Les redondances statistiques

La redondance statistique peut être classée en deux types : la redondance interpixels et la redondance de codage. La redondance interpixels, est le fait que les pixels d'une trame d'image, et les pixels d'une séquence d'images successives (une vidéo), sont corrélés à des degrés divers. Ce type de corrélation peut en outre être divisée en deux catégories : la redondance spatiale et la redondance temporelle. La redondance de codage est la redondance statistique associée à des techniques de codage**.**

2.5.1 La redondance spatiale

La redondance spatiale représente la corrélation statistique entre les pixels dans une trame d'image. Elle est aussi appelée redondance intra-trame.

2.5.2 La redondance temporelle

La redondance temporelle concerne la corrélation statistique entre les pixels de trames successives dans une séquence vidéo. On l'appelle également redondance intertrame.

2.5.3 La redondance de codage

Cela n'a rien à voir avec la redondance de l'information mais avec la représentation de l'information, Eviter la redondance de codage revient à créer des techniques de codage plus efficaces pour compresser les données image et vidéo. Parmi les techniques utilisées on site deux techniques de codage à longueur variable, le Codage de Huffman et le codage arithmétique.

2.6. Les redondances psychovisuelles

La redondance psychovisuelle provient des caractéristiques du système visuel humain. La perception de l'œil humaine est différente de celle de la caméra. Dans le SVH, les informations visuelles ne sont pas perçues de manière égale ; certaines informations peuvent être plus importantes que d'autres. Cela implique que si nous appliquons moins de données pour représenter des informations visuelles moins importantes, la perception ne sera pas affectée.

On site parmi les redondances psychovisuelles les plus importantes :

Le masquage de la luminance : concerne la perception de la luminosité du SVH.

Le masquage de la chrominance : concerne la perception des couleurs.

Le masquage de texture : concerne la perception des détails ; plus la texture est forte, plus le SVH ignore de détails.

Le masquage temporel : le SVH prend un certain temps pour s'adapter à la scène lorsqu'elle change brusquement. Pendant cette transition, le SVH n'est pas sensible aux détails. [2]

2.7. Compression sans pertes

La compression sans pertes consiste à réduire la taille de la vidéo tout en ayant la possibilité de reconstituer une vidéo identique à l'originale. Le codage arithmétique et le codage de Huffman ainsi que les codages à base de dictionnaire sont des codages utilisés pour la compression sans pertes. [3]

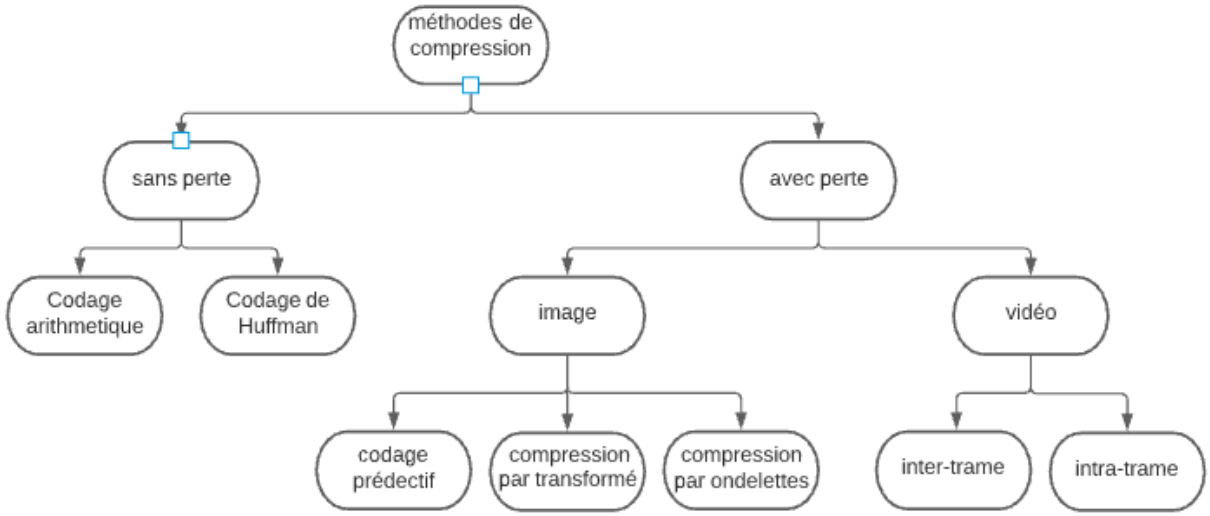

Figure 2.1 : taxonomie des méthodes de compression d'images et de vidéos

2.7.1. Codage de Huffman

Le codage de Huffman est effectué pour réaliser une compression sans perte, les données d'entrée sont divisées en une séquence de symboles afin de faciliter le processus de modélisation. Dans la plupart des applications de compression d'images et de vidéos, la taille de l'alphabet composant ces symboles est limitée à 64 000 symboles au maximum. La procédure de construction du code de Huffman se fait selon les étapes suivantes :

1. Ordonner les symboles selon leurs probabilités. Pour la construction du code de Huffman, la fréquence d'occurrence de chaque symbole doit être connue à priori. En pratique, la fréquence d'occurrence peut être estimée à partir d'un ensemble de données d'apprentissage représentatif des données à compresser sans perte.
2. Appliquer un processus de contraction aux deux symboles avec les probabilités les plus petites. Supposons que les deux symboles sont SN-1 et SN. Nous remplaçons ces deux symboles par un symbole hypothétique, nommé, HN- I, qui a une probabilité d'occurrence de (PN-1) + PN. Ainsi, le nouvel ensemble a N-1 symboles:
   S1. S2... SN-2, HN-1·
3. On répète l'étape précédente jusqu'au dernier ensemble n'ayant qu'un seul membre. La procédure récursive de l'étape 2 peut être considérée comme la construction d'un arbre binaire, car à chaque étape nous fusionnons deux symboles. À la fin du processus de récursivité, tous les symboles seront des feuilles de cet arbre et le mot de code pour

chaque symbole est obtenu en parcourant l'arbre binaire de sa racine jusqu'au nœud correspondant au symbole.

2.7.2. Codage arithmétique

Le codage arithmétique est une technique de compression sans perte qui traite plusieurs symboles comme une seule unité de données, tout en conservant l'approche de codage incrémentiel; symbole par symbole du codage de Huffman. Le codage arithmétique sépare le codage de la modélisation. Ce processus permet l'adaptation dynamique du modèle probabiliste sans affecter la conception du code.

Dans la théorie du codage arithmétique. Un seul mot de code est attribué à chaque ensemble de données possible. Chaque mot de code peut être considéré comme un sous-intervalle semi-ouvert dans l'intervalle [0,1). En attribuant suffisamment de bits de précision à chacun des mots de code, on peut distinguer un sous-intervalle de tout autre sous-intervalle, et ainsi décoder de manière unique l'ensemble de données correspondant. Comme les mots de code de Huffman, les ensembles de données les plus probables correspondent à des sous-intervalles plus grands et nécessitent donc moins de bits de précision. [4]

2.8. Compression avec pertes

C’est une compression irréversible consistant à éliminer les redondances de façon permanente.

Les compression JPEG, JPEG2000, H264 font partie des compressions avec pertes. [3]

2.8.1. Codage par transformation

Le codage par transformation est principalement utilisé pour supprimer les redondances spatiales dans les images en projetant les pixels dans un domaine de transformation avant la compression des données. L’avantage du codage par transformée dans la réalisation de la compression des données est que l'énergie d'image de la plupart des scènes naturelles est principalement concentrée dans la région des basses fréquences, et donc dans quelques coefficients de transformation. Ces coefficients peuvent ensuite être quantifiés dans le but d'écarter les coefficients non significatifs, sans affecter significativement la qualité de l'image reconstruite. Ce processus de quantification est cependant avec perte car les valeurs originales ne peuvent pas être conservées. [5]

2.8.2. Transformée en cosinus discrète (DCT)

Le codage d'image basé sur la Transformée en cosinus discrète est la base de toutes les normes de compression d'images et de vidéos. Le calcul de base dans un système basé sur cette transformée

est la transformation d'un bloc d'image N x N du domaine spatial au domaine DCT. Pour les normes de compression d'image, N = 8. Une taille de bloc de 8 x 8 est choisie pour plusieurs raisons. Du point de vue de l'implémentation matérielle ou logicielle, une taille de bloc de 8 x 8 n'impose pas d'exigences de mémoire importantes ; en outre, la complexité de calcul d'un DCT 8 x 8 est gérable sur la plupart des plates-formes informatiques. Du point de vue de l'efficacité de la compression, une taille de bloc supérieure à 8 x 8 n'offre pas une compression significativement meilleure ; la corrélation spatiale est réduite lorsqu'un voisinage de pixels est supérieur à huit pixels. [4]

2.8.3. Transformée en ondelette discrète (DWT)

Une ondelette est définie comme une "petite onde" dont l'énergie est concentrée dans le temps pour fournir un outil pour l'analyse des phénomènes transitoires, non stationnaires ou variables dans le temps et elle a les propriétés ondulatoires oscillantes mais a également la capacité de permettre l'analyse de temps et de fréquence simultanément.

La transformation en ondelettes discrètes (DWT) consiste à choisir des échelles et des positions basées sur des puissances de deux et sont appelées échelles et positions dyadiques (ensemble de deux éléments). L'ondelette mère est redimensionnée ou « dilatée » par des puissances de deux et traduite par des nombres entiers. Plus précisément, une fonction f(t)∈L² (R) peut être représentée par :

$$\mathrm{f(t)} = \sum_{j=1}^{L} . \sum_{k=-\infty}^{\infty} d(j,k)\Psi(2 - \mathrm{jt} - \mathrm{k}) + \sum_{k=-\infty}^{+\infty} a(L,K)\Phi(2^{-\mathrm{L}}\mathrm{t} - \mathrm{k}) \quad 2.1$$

où, Ψ (t) est connu comme l'ondelette mère, ϕ(t) est connu comme la fonction d'échelle. Les nombres a (L, k) sont appelés coefficients d'approximation à l'échelle L et d (j, k) sont appelés coefficients de détail à l'échelle j. Les coefficients d'approximation et de détail peuvent être exprimés comme suit :

$$a(L,k) = \frac{1}{\sqrt{2^L}} \int_{-\infty}^{\infty} f(t)\Phi(2^{-L}t - k)d(t) \quad 2.2$$

$$d(j,k) = \frac{1}{\sqrt{2^j}} \int_{-\infty}^{\infty} f(t)\Phi(2^{-j}t - k)d(t) \quad 2.3$$

Les deux équations ci-dessus donnent une relation mathématique pour calculer les coefficients d'approximation et de détail.

2.8.3.1. La transformée en ondelette discrète bidimensionnelle

La DWT bidimensionnelle est obtenue grâce à la mise en œuvre de filtres passe-bas et passe-haut sur les lignes et les colonnes de l'image respectivement. Cette paire de filtres est appelée paire de

filtres d'analyse. Initialement, le filtre passe-bas est appliqué pour chaque ligne de données, obtenant ainsi les composants basse fréquence de la ligne et les données de sortie ne contiennent des fréquences que dans la première moitié de la plage de fréquences d'origine car le filtre passe-bas est un filtre demi-bande. Ensuite, le filtre passe-haut est appliqué pour la même rangée de données, et les composantes passe-haut sont séparées, et ces composantes passe-haut sont placées à côté des composantes passe-bas. Cette procédure est effectuée pour toutes les lignes. Comme indiqué ci-dessus, la bande LL au niveau le plus élevé peut être classée comme la plus importante, et les autres bandes (de détail) peuvent être classées comme moins importantes. DWT est une technique multispectrale utilisée pour convertir le signal ou l'image en quatre bandes différentes 1) bas-bas (LL), 2) bas-haut (LH), 3) haut-bas (HL), 4) haut-haut (HH) comme le montre la figure 2.2.

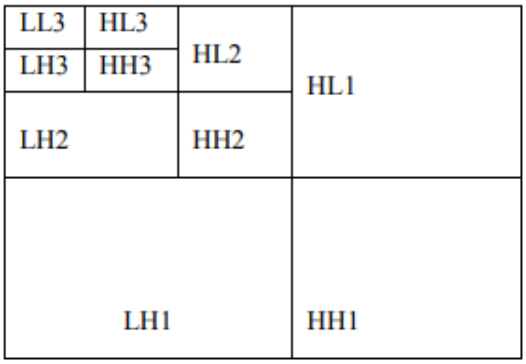

Figure 2.2 : Décomposition de l'image en appliquant DWT

Le processus d'analyse d'ondelettes implique un filtrage et un échantillonnage descendant et le processus de reconstruction d'ondelettes implique un échantillonnage ascendant et un filtrage. Le processus d'allongement d'une composante de signal en insérant des zéros entre les échantillons est connu sous le nom de suréchantillonnage.

2.8.3.2. Les types de transformation en ondelette

On site ci-dessous trois des familles d'ondelettes les plus utilisées dans la transformée en ondelette discrète.

- **Les ondelettes de Haar**

Haar est une fonction en ondelettes qui s'applique facilement, en utilisant le moins de temps et elle a une propriété orthogonale. L'ondelette mère de Haar ψ (x) peut être décrite par l'équation suivante :

$$\psi(x) = \begin{cases} 1 & 0 < t < 1/2 \\ -1 & \frac{1}{2} < t < 1 \\ 0 & ailleur \end{cases} \quad 2.4$$

La transformée de Haar a des applications telles que la compression de signal et d'image, et elle a l'avantage d'être conceptuellement simple, rapide et efficace en mémoire car elle peut être calculée sur place sans tableau temporaire.

- **Les ondelettes de Daubechies**

Les ondelettes de Daubechies sont une famille d'ondelettes orthogonales définissant une transformée en ondelettes discrète et caractérisée par un nombre maximal de moments nuls. Pour chaque type d'ondelettes de cette classe, une analyse multi-résolution orthogonale est générée par une fonction d'échelle. Les noms des ondelettes de la famille Daubechies s'écrivent dbN, où N est l'ordre de l'ondelette. Ce type d'ondelettes a des réponses en fréquence équilibrées mais des réponses en phase non linéaires. Ces ondelettes utilisent des fenêtres qui se chevauchent de telle sorte que le spectre de coefficients haute fréquence reflète tous les changements haute fréquence. Par conséquent, ces ondelettes sont utiles pour la compression et la suppression du bruit dans le traitement du signal audio.

- **Les ondelettes biorthogonales**

L'ondelette biorthogonale ou semi-orthogonale est uniquement orthogonale à la fonction de base décalée sous un facteur d'échelle différent, mais n'a pas d'orthogonalité dans le même facteur d'échelle. La famille d'ondelettes biorthogonales a la propriété de phase linéaire, qui est nécessaire pour la reconstruction du signal et de l'image. [6]

2.9. Motion JPEG

Une séquence vidéo numérique peut être représentée comme une série d'images JPEG. Les avantages sont les mêmes qu'avec les images fixes JPEG – flexibilité à la fois en termes de qualité et de taux de compression. Le principal inconvénient de Motion JPEG (MJPEG) est que, puisqu'il n'utilise qu'une série d'images fixes, il n'utilise pas de techniques de compression vidéo (n'élimine pas les redondances temporelles). Le résultat est un taux de compression légèrement inférieur pour les séquences vidéo par rapport aux techniques de compression vidéo.

2.10. Motion JPEG 2000

Comme pour la compression JPEG et Motion JPEG, Motion JPEG 2000 peut également être utilisé pour représenter une séquence vidéo. JPEG 2000 est une norme de compression basée sur la transformation en ondelettes discrète (DWT).

Les avantages sont égaux au JPEG 2000, c'est-à-dire un taux de compression légèrement meilleur par rapport au JPEG mais au prix d'une complexité de la compression. L'inconvénient remonte à celui du Motion JPEG. Comme il s'agit d'une technique de compression d'images fixes, elle ne profite pas de la compression de séquence vidéo. Cela se traduit par un taux de compression inférieur par rapport aux techniques de compression vidéo réelles.

2.11. MPEG-1

La première norme publique du comité MPEG était MPEG-1, dont les premières parties ont été publiées en 1993. La compression vidéo MPEG-1 est basée sur la même technique que celle utilisée dans JPEG. En plus de cela, il comprend également des techniques pour un codage efficace d'une séquence vidéo. Considérez la séquence vidéo affichée sur la figure 2.3.

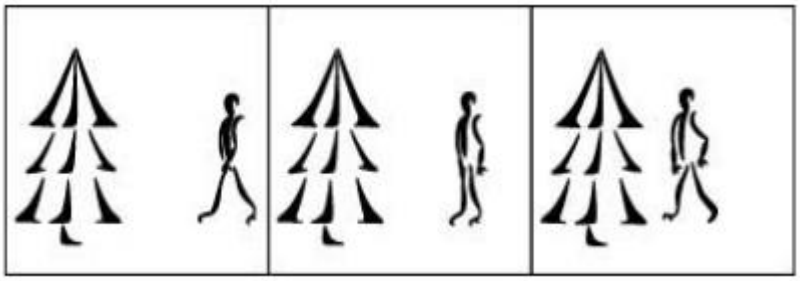

Figure 2.3 : Une séquence vidéo JPEG de trois images

L'image de gauche est la première image de la séquence, suivie de l'image du milieu, puis de l'image de droite. Lorsqu'elle est affichée, la séquence vidéo montre un homme marchant de droite à gauche avec un arbre immobile. Dans Motion JPEG/Motion JPEG 2000, chaque image de la séquence est codée comme une image unique distincte résultant en la même séquence que l'originale. Dans la vidéo MPEG, seules les nouvelles parties de la séquence vidéo sont incluses avec les informations des parties mobiles. La séquence vidéo de la figure 2.3 apparaîtra alors comme sur la figure 2.4. Mais ceci n'est vrai que lors de la transmission de la séquence vidéo pour limiter la consommation de bande passante. Lorsqu'il est affiché, il apparaît à nouveau comme la séquence vidéo d'origine.

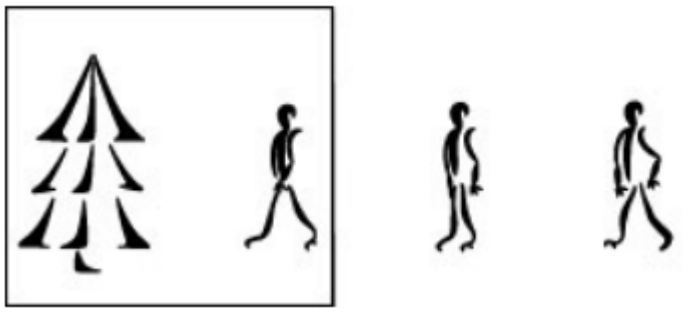

Figure 2.4 : Une séquence vidéo MPEG de trois images

MPEG-1 se concentre sur des flux binaires d'environ 1,5 Mbps, développé à l'origine pour le stockage de vidéo numérique sur CD. L'accent est mis sur le taux de compression plutôt que sur la qualité de l'image.

2.12. MPEG-2

La norme MPEG-2 est destinée à la transmission TV et à d'autres applications capables de débits de données de 4 Mbps et plus. Elle offre une qualité d'image très élevée. MPEG-2 prend en charge les formats vidéo entrelacés, une qualité d'image améliorée et d'autres fonctionnalités destinées à la TVHD. C'est une extension compatible avec MPEG-1, ce qui signifie qu'un décodeur MPEG-2 peut également décoder les flux MPEG-1. L'audio MPEG-2 fournira jusqu'à cinq canaux à bande passante complète (gauche, droite, centre et deux canaux arrières), plus un canal d'amélioration des basses fréquences supplémentaire, ou jusqu'à sept canaux de commentaires. La norme des systèmes MPEG-2 spécifie comment combiner plusieurs flux audio, vidéo et de données privées en un seul flux multiplexé et prend en charge un large éventail d'applications de diffusion, de télécommunications, d'informatique et de stockage. MPEG-2, fournit également des techniques plus avancées pour améliorer la qualité vidéo au même débit binaire. La contrainte pour cette norme est le besoin d'équipements beaucoup plus complexes. Par conséquent, ces fonctionnalités ne sont pas adaptées à une utilisation dans des applications de surveillance en temps réel.

2.13. MPEG-4

Les nouvelles fonctionnalités les plus importantes de MPEG-4, concernant la compression vidéo sont le support d'applications consommant encore moins de bande passante, par ex. unités mobiles, et d'autre part des applications avec une qualité extrêmement élevée et une bande passante presque illimitée. La réalisation de films en studio en est un exemple. La plupart des différences entre MPEG-2 et MPEG-4 sont des fonctionnalités non liées au codage vidéo et donc non liées aux applications de surveillance. MPEG implique le codage complet uniquement des images clés via

l'algorithme JPEG et l'estimation des changements de mouvement entre ces images clés. Étant donné que des informations minimales sont envoyées toutes les quatre ou cinq images, une réduction significative du nombre de bits requis pour décrire l'image en résulte. Par conséquent, des taux de compression supérieurs à 100:1 sont atteints.

Le schéma est asymétrique ; l'encodeur MPEG est très complexe et impose une charge de calcul très lourde pour l'estimation de mouvement. Le décodage est beaucoup plus simple et peut être effectué par les processeurs de bureau d'aujourd'hui ou avec des puces de décodeur à faible coût. Le schéma de base est de prédire le mouvement d'une image à l'autre dans la direction temporelle, puis d'utiliser des DCT (transformées en cosinus discrètes) pour organiser la redondance dans les directions spatiales. Les DCT sont effectués sur des blocs de 8x8 et la prédiction de mouvement est effectuée dans le canal de luminance (Y) sur des blocs de 16x16. Pour un bloc 16x16 dans la trame actuelle en cours de compression, l'encodeur recherche une correspondance étroite avec ce bloc dans une trame précédente ou future (il existe des modes de prédiction vers l'arrière où les trames ultérieures sont envoyées en premier pour permettre l'interpolation entre les trames). Les coefficients DCT (soit des données réelles, soit de la différence entre ce bloc et la correspondance étroite) sont quantifiés. La plupart des coefficients finissent par être nuls. La quantification peut changer pour chaque bloc, qui est de 16x16 de Y et les 8x8 correspondants dans U et V. Les résultats de tout cela, y compris les coefficients DCT, les vecteurs de mouvement et les paramètres de quantification sont codés par Huffman à l'aide de tableaux fixes. Les coefficients DCT ont un tableau de Huffman spéciale qui est bidimensionnelle dont un code spécifie une longueur d'exécution de zéros et la valeur non nulle qui a terminé l'exécution. De plus, les vecteurs de mouvement et les composants DCT sont codés en DPCM.

2.14. H.261

H.261 est un algorithme de compression de mouvement développé spécifiquement pour la vidéoconférence, bien qu'il puisse être utilisé pour toute tâche de compression de vidéo. Cette norme permet une utilisation des canaux de communication multiples de 64 kbps (P=1, 2, 3...30.), la même structure de données que RNIS. Le codage H.261 est basé sur la transformée en cosinus discrète (DCT) et permet de ne coder entièrement que certaines trames (intra-trame) tout en codant les différences entre les autres trames (inter-trame). Les principaux éléments du codeur source H.261 sont la prédiction, la transformation de blocs (translation du domaine spatial vers le domaine fréquentiel), la quantification et le codage entropique.

Alors que le décodeur nécessite une prédiction, la compensation de mouvement est optionnelle. Une autre option dans la recommandation est le filtrage en boucle. Le filtre de boucle est appliqué aux données de prédiction pour réduire les erreurs importantes lors de l'utilisation du codage inter-trame. Le filtrage en boucle offre une amélioration notable de la qualité vidéo, mais nécessite une puissance de traitement supplémentaire. Le fonctionnement du décodeur permet à de nombreux CODEC compatibles avec la norme H.261 de fournir des niveaux de qualité très différents.

2.15. H.263

C'est le codec vidéo introduit avec H.324, qui est destiné à la visioconférence sur le réseau téléphonique analogique. Alors que la vidéo est une option sous H.324, tout terminal prenant en charge la vidéo doit prendre en charge à la fois H.263 et H.261. H.263 est un raffinement structurellement similaire à H.261 et est rétrocompatible avec H.261. À des bandes passantes inférieures à 1000 kbps, la qualité d'image de H.263 est supérieure à celle de H.261. Les images sont grandement améliorées en utilisant une nouvelle estimation de mouvement de 1/2 pixel plutôt que l'estimation d'entier facultative utilisée dans H.261. Les techniques demi-pixel donnent de meilleures correspondances et sont nettement supérieures avec des images à faible résolution (Sub Quarter Common Intermediate Format ou SQCIF). Avec H.263, comme avec H.261, chaque image est divisée en groupes de blocs. Un groupe de blocs comprend k*16 lignes, selon le format d'image (k = 1 pour les sous-QCIF, QCIF et CIF ; k = 2 pour 4CIF ; k = 4 pour 16CIF).

2.16. H.264

H.264 est le résultat d'un projet conjoint entre le groupe d'experts en codage vidéo de l'ITUT et le groupe MPEG. H.264 est le nom utilisé par l'UIT-T, tandis que ISO/IEC l'a nommé MPEG-4 Part 10/AVC puisqu'il est présenté comme une nouvelle partie dans sa suite MPEG-4. La suite MPEG-4 comprend, par exemple, MPEG-4 Part 2, une norme utilisée par les encodeurs vidéo IP et les caméras réseau. Conçu pour remédier à plusieurs faiblesses des normes de compression vidéo précédentes, H.264 atteint ses objectifs de prise en charge :

1) Des implémentations offrant une réduction moyenne du débit binaire de 50 %, avec une qualité vidéo fixe par rapport à toute autre norme vidéo.

2) Robustesse aux erreurs afin que les erreurs de transmission sur divers réseaux soient tolérées.

3) Capacités de faible latence et meilleure qualité pour une latence plus élevée.

4) Spécification de syntaxe simple qui simplifie les implémentations.

5) Décodage par correspondance exacte, qui définit exactement comment les calculs numériques doivent être effectués par un encodeur et un décodeur pour éviter l'accumulation d'erreurs. [7]

Standard	Applications	Bit rate
Motion-JPEG	Still image compression	Variable
MPEG-2000	Improved still image compression	Variable
MPEG-1	Video on digital storage media	1.5 mb/s
MPEG-4	Object based coding	Variable
H.261	Video conferencing Over ISDN	P × 64 kb/s
H.263	Video telephony over PSTN	33.6 kb/s
H.264	Improved video compression	10–100 kb/s

Tableau 2.1 : Comparaison des normes de compression vidéo [8]

2.17. HEVC (H.265)

La norme HEVC (H.265) a été développée dans le but d'améliorer l'efficacité du codage vidéo d'au moins un facteur de deux, la résilience aux pertes de données et d'implémenter des architectures de traitement parallèles. Semblable à ses prédécesseurs, la norme HEVC utilise des approches de codage vidéo hybrides qui utilisent les techniques de prédiction inter-image et intra-image et de codage par transformation. HEVC utilise un nouveau schéma de partitionnement d'image, qui partitionne l'image en unités de 64x64 appelées unités de codage. Un schéma de partitionnement hiérarchique en quatre arbres est utilisé pour les unités de codage, ce qui les divise en blocs de codage plus petits. Il utilise 33 modes angulaires pour les prédictions intra-image ainsi que deux modes supplémentaires, à savoir le mode intra et le mode LM Chroma (ce mode utilise un modèle linéaire pour prédire la chrominance à partir de la luminance en tant que mode de prédiction intra de la chrominance). [9]

L'unité de codage est en outre utilisée comme unité de prédiction, qui est sous-divisée en différentes tailles pour mettre en œuvre des techniques de prédiction de mouvement. Les unités résiduelles obtenues à partir des unités partitionnées ci-dessus sont ensuite codées en unités de transformation suivies d'un schéma de quantification. HEVC a conservé le schéma de codage arithmétique binaire adaptatif au contexte de H.264/AVC pour le codage des coefficients. Trois types de techniques de filtrage sont appliqués aux coefficients codés, à savoir le filtrage par décalage adaptatif d'échantillon, le filtrage de boucle adaptatif et le filtre de déblocage. Ces techniques de filtrage visent à réduire la distorsion et les artefacts dus aux blocs d'image. Les fonctionnalités décrites ci-dessus et le traitement parallèle de front d'onde mis en œuvre dans

HEVC lui permettent d'effectuer des opérations de codage et de décodage parallèles. Cela améliore encore son efficacité de codage et réduit également sa complexité de calcul. [10]

2.18. Conclusion

Dans ce chapitre nous avons présenté des notions sur la vidéo ; les espaces couleurs, le nombre de pixels et nombre de trames par seconde; on a ensuite défini la compression et les redondances à éliminer dans la vidéo, nous avons aussi discuté des différents types de compressions et détaillé la compression par ondelette, et enfin on a décrit les standards de compression d'images et de vidéos les plus utilisés actuellement.

Références

[1] I. E. G. Richardson, *Video codec design : developing image and video compression systems*. John Wiley and Sons, 2002.

[2] Y.-Q. Shi and H. Sun, *Image and Video Compression for Multimedia Engineering*. CRC press, 2008.

[3] K. S. Thyagarajan, *Still Image and Video Compression with MATLAB*. John Wiley and Sons, 2011.

[4] V. Bhaskaran and K. Konstantinides, *Image and Video Compression Standards: Algorithms and Architectures*. Kluwer Academic Publishers, 1997.

[5] M. Ghanbari, *Standard Codecs: Image Compression to Advanced Video Coding (Telecommunications)*. IEE, London, UK, 2003.

[6] L. E. Tresa and M. Sundararajan, "Comparative analysis of different wavelets in DWT for video compression," *2014 Int. Conf. Circuits, Power Comput. Technol. ICCPCT 2014*, pp. 1512–1517, 2014, doi: 10.1109/ICCPCT.2014.7054859.

[7] S. Ponlatha and R. S. Sabeenian, "Comparison of Video Compression Standards," *Int. J. Comput. Electr. Eng.*, no. December 2013, pp. 549–554, 2013, doi: 10.7763/ijcee.2013.v5.770.

[8] S. Pandit, P. K. Shukla, A. Tiwari, P. K. Shukla, M. Maheshwari, and R. Dubey, "Review of video compression techniques based on fractal transform function and swarm intelligence," *Int. J. Mod. Phys. B*, vol. 34, no. 8, pp. 1–21, 2020, doi: 10.1142/S0217979220500617.

[9] X. Zhang, O. C. Au, J. Dai, C. Pang, and F. Zou, "New chroma intra prediction modes based on linear model for HEVC," *Proc. - Int. Conf. Image Process. ICIP*, pp. 197–200, 2012, doi: 10.1109/ICIP.2012.6466829.

[10] M. M. Nasralla, M. Razaak, I. Rehman, and M. G. Martini, "A Comparative Performance Evaluation of the HEVC Standard with its Predecessor H.264/AVC for Medical videos over 4G and beyond Wireless Networks," *2018 8th Int. Conf. Comput. Sci. Inf. Technol. CSIT 2018*, pp. 50–54, 2018, doi: 10.1109/CSIT.2018.8486153.

[11] E. Doutsi, "Retina-inspired Image and Video coding,", PhD thesis, Université Côte d'Azur, 2017.

Chapitre 3

Etude des différentes techniques de cryptage

3.1. Introduction

Les progrès récents dans l'intelligence artificielle et le développement du cloud computing ont permis le déploiement des systèmes IoT contemporains constitués de réseaux de capteurs multimédias pour la surveillance de vastes zones géographiques pour la sécurité publique, les transports intelligents et les villes intelligentes ainsi que pour l'industrie intelligente. [1] Selon [2] Il est probable que le nombre de caméras dans le monde se situerait entre 10 et 100 milliards en 2030, la taille des flux vidéos sera donc de plus en plus importante, et cette augmentation est accompagné par une diversité de contenus de ces vidéos, ce qui mène à la nécessité de développer des systèmes de cryptographie plus fort pour sécuriser ces flux vidéos.

3.2. Définition de la cryptographie.

La cryptographie est l'art de protéger les informations contre les individus indésirables en les convertissant sous une forme non reconnaissable par ces individus lorsqu'elles sont stockées et transmises. La cryptographie des données consiste à brouiller le contenu des données, telles que le texte, l'image, l'audio, la vidéo, etc. pour rendre les données illisibles, invisibles ou inintelligibles lors de la transmission ou du stockage, appelé aussi chiffrement. L'objectif principal de la cryptographie est de protéger les données des attaquants non autorisés. [3]

3.3. Le besoin du cryptage vidéo

Le cryptage des vidéos est important pour les raisons suivantes :

- Pour empêcher la visualisation indésirable de la vidéo transmise, par exemple à partir de la surveillance vidéo des forces de l'ordre qui est relayée vers un centre de visualisation central.

- Pour protéger les messages multimédias privés échangés sur les réseaux sans fil ou filaires.
- Le cryptage vidéo est utile pour sécuriser les vidéos utilisées dans des services tels que l'apprentissage par vidéoconférence.
- Pour protéger les vidéos médicales pouvant contenir des informations privées d'un patient contre tout accès non autorisé par des utilisateurs malveillants. [4]
- Pour sécuriser les vidéos provenant des diverses applications de l'internet des objets (systèmes de surveillance dans les maisons, les usines, etc.)

3.4. Classification des algorithmes de cryptage vidéo

Pour identifier de manière unique les caractéristiques des algorithmes de cryptage vidéo, nous suivons ici une classification liée à leur association avec des algorithmes de compression vidéo ce qui donne des algorithmes de crypto-compression (cryptage et compression conjoints), et des algorithmes de cryptage indépendants de la compression.

3.4.1. Algorithmes de crypto-compression

L'idée principale des algorithmes de crypto-compression est que le cryptage est appliqué à une certaine étape de l'algorithme de compression de sorte que la sortie est considérablement différente d'un flux vidéo utilisant un algorithme de compression standardisé. La procédure de cryptage peut être appliquée à l'une des trois phases de codage. Il en résulte trois types d'algorithmes :

- Cryptage après transformation.
- Cryptage après quantification.
- Cryptage dans le codage entropique.

3.4.2. Algorithmes de cryptage indépendants de la compression.

Dans ce type d'algorithme de cryptage, la compression et le cryptage sont effectués séparément. Le cryptage peut être effectué avant ou après la compression.

3.4.3. Algorithmes de cryptage avant compression

Les algorithmes de compression visent à réduire au maximum les redondances du texte en clair. Les algorithmes de chiffrement masquent les redondances du texte en clair à l'aide d'opérations cryptographiques. En conséquence, il y a beaucoup moins de redondance à compresser si les

algorithmes de chiffrement sont placés avant la compression. Par conséquent, les algorithmes de cryptage indépendants de la compression sont rarement réalisés avant la compression.

3.4.4. Algorithmes de cryptage après compression

Les algorithmes de cryptage après compression prennent en compte les propriétés spécifiques du flux vidéo compressé, telles que la distribution uniforme des valeurs d'octets dans le flux vidéo compressé. Ils peuvent réduire la surcharge de calcul du cryptage car ils sélectionnent généralement un flux vidéo partiel pour le cryptage ou ils cryptent l'intégralité du flux vidéo à l'aide d'un algorithme léger spécifique.[5]

3.5. Types de cryptage :

Les algorithmes de cryptographie sont divisés en deux catégories, des algorithmes qui utilisent des clés symétriques (ou clés privées), et des algorithmes qui utilisent des clés asymétriques (clés publiques et privées).

3.5.1. Algorithmes à clé symétrique

Dans le chiffrement à clé symétrique, l'expéditeur et le destinataire utilisent la même clé pour le chiffrement et le déchiffrement. Le cryptage à clé symétrique est également appelé clé secrète, car l'expéditeur et le destinataire doivent garder la clé secrète et correctement protégée Fondamentalement, le niveau de sécurité de la méthode de cryptage à clés symétriques dépend totalement de l'aptitude des utilisateurs à garder les clés protégées. Si la clé est connue d'un intrus, toutes les données chiffrées avec cette clé peuvent être déchiffrées. C'est ce qui rend plus compliquée la façon dont les clés symétriques sont pratiquement partagées et mises à jour si nécessaire. Les clés symétriques peuvent assurer la confidentialité mais elles ne peuvent pas fournir l'authentification, car il n'y a aucun moyen de prouver par cryptographie qui a réellement envoyé un massage si deux personnes utilisent la même clé. Ces algorithmes sont encore utilisés dans de nombreuses applications, car ils sont très rapides et peuvent être difficiles à casser si vous utilisez une grande taille de clé. Les clés symétriques peuvent gérer une grande quantité de données qui prendraient un temps inacceptable avec des clés asymétriques pour chiffrer et déchiffrer. Les algorithmes à clé symétrique les plus populaires sont Data Encryption Standard (DES), Triple DES et Advance Encryption Standard (AES).

- **Data Encryption Standard (DES)**

DES est l'un des exemples les plus importants d'un chiffrement par bloc. Le DES est largement utilisé pour le cryptage des numéros PIN, des transactions bancaires, etc. Le DES est un exemple de chiffrement par bloc, qui fonctionne sur des blocs de 64 bits à la fois, avec une clé d'entrée de 64 bits. Chaque 8ème bit dans la clé d'entrée est un bit de contrôle de parité, ce qui signifie qu'en fait la taille de la clé est effectivement réduite à 56 bits.

- **Advance Encryption Standard (AES)**

En 1997, le NIST a demandé des soumissions pour une nouvelle norme pour remplacer le DES. Le concours s'est terminé en novembre 2001 avec la sélection du cryptosystème Rijndael nommé Advanced Encryption Standard (AES). Le cryptosystème Rijndael fonctionne sur des blocs de 128 bits, organisés en matrices 4 × 4 avec des entrées de 8 bits. L'algorithme peut utiliser une longueur de bloc et une longueur de clé variables ; la dernière spécification autorise n'importe quelle combinaison de longueurs de clés de 128, 192 ou 256 bits et de blocs de longueur 128, 192 ou 256 bits.

3.5.2. Algorithmes à clé asymétrique

Le système de cryptage à clé publique est un système de chiffrement à deux clés dans lequel deux parties peuvent communiquer en toute sécurité sur un canal de communication non sécurisé sans avoir à partager une clé secrète et résoudre le problème de la distribution des clés secrètes en utilisant deux clés au lieu d'une seule. Dans l'algorithme à clé publique, deux clés sont utilisées. Une clé publique, qui peut être connue de tous, et une clé privée, qui doit être gardée secrète et connue uniquement du propriétaire.

Si le massage est chiffré par une clé, l'autre clé est requise pour déchiffrer le message. La clé publique et la clé privée sont mathématiquement liées. Cependant, cela ne signifie pas que, si quelqu'un a la clé publique, il sera capable de découvrir la clé privée, mais la clé privée ne doit être accessible que par le propriétaire. À condition que l'authentification soit requise, les données seraient cryptées avec la clé privée de l'expéditeur puis chaque personne disposant de la clé publique correspondante pourra décrypter les données. Cela donne au destinataire l'assurance que les données ont été cryptées par une personne en possession de cette clé privée. Le cryptage des données avec une clé privée est appelé format de message ouvert, car la confidentialité n'est pas assurée. Toute personne disposant d'une copie de la clé publique

correspondante peut déchiffrer les données. Les algorithmes à clé asymétrique les plus populaires sont (RSA) et ECC. [3]

- **RSA**

L'algorithme RSA, est le premier algorithme qui peut être utilisé à la fois pour le chiffrement des données et les signatures numériques. La sécurité de l'algorithme RSA dépend de la difficulté de décomposition de grands nombres. Deux grands nombres premiers sont utilisés pour construire la clé publique et la clé privée. On estime que la difficulté de deviner le texte en clair à partir de la clé et du texte chiffré équivaut à celle de la décomposition du produit de deux grands nombres premiers. [6]

- **La cryptographie à courbe elliptique (ECC)**

La cryptographie à courbe elliptique couvre toutes les primitives cryptographiques asymétriques pertinentes telles que les signatures numériques et les algorithmes d'accord de clé. L'opération de base de l'algorithme ECC est la multiplication scalaire k.P. Où k est un entier et P est un point sur une courbe elliptique. [7]

3.6. Approches utilisés pour le cryptage

3.6.1. Chiffrement complet : Un algorithme de chiffrement vidéo qui effectue le cryptage sur l'intégralité du flux de bits vidéo appartient à cette classe d'algorithmes. Il nécessite des capacités de calculs assez lourds et à une vitesse lente.

3.6.2. Chiffrement sélectif : également connu sous le nom de chiffrement partiel, il s'agit d'une sous-catégorie du chiffrement variable. Les algorithmes de cette classe chiffrent de manière sélective les octets dans les images vidéo. Comme ces algorithmes ne chiffrent pas chaque octet de données vidéo, cela réduit la complexité de cryptage. [4]

3.7. La cryptanalyse

La cryptanalyse est l'art de déchiffrer un message chiffré, en tout ou en partie, lorsque la clé de déchiffrement n'est pas connue. Selon la quantité d'informations connues et le degré de contrôle du système par l'adversaire (cryptanalyste), il existe plusieurs types d'attaque cryptanalytique :

- **Attaque par texte chiffré uniquement** : Le cryptanalyste n'a accès qu'à un ou plusieurs messages cryptés. L'objectif le plus important d'un cryptosystème proposé est de résister à ce type d'attaque.
- **Attaque par force brute** : Il s'agit d'un type d'attaque par texte chiffré uniquement. Il est basé sur une recherche exhaustive par clé ; et pour les cryptosystèmes bien conçus, cela

devrait être infaisable du point de vue informatique. Selon les normes actuelles, les clés 128 bits sont considérées comme sécurisées contre les attaques par force brute.

- **Attaque à texte clair connue**: Dans ce type d'attaque, un cryptanalyste a une certaine connaissance du texte en clair correspondant au texte chiffré donné. Cela peut aider à déterminer la clé ou une partie de la clé.
- **Attaque à texte clair choisi :** En général, un cryptanalyste peut introduire le texte en clair choisi dans la boîte noire qui contient l'algorithme de cryptage et la clé de cryptage. La boîte noire produit le texte chiffré correspondant et le cryptanalyste peut utiliser les connaissances accumulées sur les paires (texte clair-texte chiffré) pour obtenir la clé secrète ou au moins une partie de celle-ci.
- **Attaque par texte chiffré choisi :** Ici, un cryptanalyste peut alimenter le texte chiffré choisi dans la boîte noire qui contient l'algorithme de déchiffrement et la clé de déchiffrement. La boîte noire produit le texte en clair correspondant et le cryptanalyste essaie d'obtenir la clé secrète ou une partie de la clé en analysant les paires texte chiffré-texte en clair accumulées. [8]

3.8. Techniques de cryptage vidéos

Il existe plusieurs schémas de cryptage des images et des vidéos, ces schémas peuvent être des cryptages complets ou sélectifs :

3.8.1 Approche naïve : Il s'agit d'un type d'approche de cryptage complet dans laquelle un système de cryptage conventionnel est utilisé. C'est la méthode la plus simple pour crypter chaque octet de l'ensemble du flux vidéo à l'aide de schémas de cryptage standard tels que DES ou AES. Cependant, cet algorithme n'est pas applicable pour la vidéo lourde, car il est très lent surtout lorsque nous utilisons le triple DES. En raison de l'opération de cryptage, le délai augmente, il ne convient donc pas au cryptage vidéo en temps réel.

3.8.2 Algorithme de permutation pure : il brouille simplement les octets dans une trame de flux vidéo par permutation.

3.8.3 Algorithme de permutation en zigzag : dans cette méthode, au lieu de projeter le bloc 8x8 au vecteur 1x64 dans l'ordre du Zigzag, il projette le bloc 8x8 individuel à un vecteur 1x64 en utilisant une liste de permutation aléatoire (clé secrète).

3.8.4 Algorithmes de cryptage basés sur le chaos : C'est l'un des algorithmes les plus populaires dans le domaine des réseaux de neurones pour effectuer le cryptage et le décryptage, car il s'agit d'un algorithme à faible coût adapté à une grande quantité de données.

3.8.5 Algorithme de cryptage vidéo (VEA) : dans ce concept, ce nouveau cryptage divisera les flux vidéo d'entrée en morceaux impairs (a1, a3, a5, …, a2n-1) et en morceaux pairs (a2, a4, …a2n) la clé de chiffrement sera appliquée à la liste paire E (a2, a4, a6, …, a2n), où E désigne une fonction de chiffrement. Enfin, le texte chiffré est une concaténation de la sortie de l'algorithme de chiffrement XOR avec les flux de liste impairs. [4]

3.9. Cryptographie chaotique

La théorie du chaos est basée sur le comportement des systèmes dynamiques qui sont très sensibles aux conditions initiales. Les phénomènes de chaos dans la vie réelle comprennent la météo, le marché boursier, les tremblements de terre, etc. La théorie du chaos a gagné sa popularité lorsqu'en 1960, le météorologue Lorenz a répété une simulation météorologique en utilisant des données précédemment obtenues et a obtenu des résultats très différents par rapport à la simulation précédente. La différence dans le résultat de la simulation était causée par une différence de 0,000127 dans la deuxième entrée d'exécution. Cela a indiqué que les systèmes chaotiques ont une sensibilité élevée aux conditions initiales ; le moindre changement dans l'entrée se traduira par un changement dramatique dans la sortie, rendant impossible la prévisibilité à long terme. Une autre caractéristique chaotique attrayante est l'ergodicité, dans laquelle la trajectoire dans l'espace des phases revient finalement arbitrairement proche (mais jamais la même) de ses états initiaux. La trajectoire forme un attracteur, où dans la simulation de Lorenz a la forme similaire à celle des ailes d'un papillon. D'où peut-être le surnom populaire de la théorie, l'effet papillon. L'ergodicité a également indiqué que les systèmes chaotiques ne sont pas entièrement aléatoires, comme le suggère le terme chaos. La sortie (pseudo) aléatoire résultant de la moindre variation d'entrée démontre en quelque sorte des régularités subtiles, comme le montre l'attracteur de trajectoire (figure 3.1) [9]

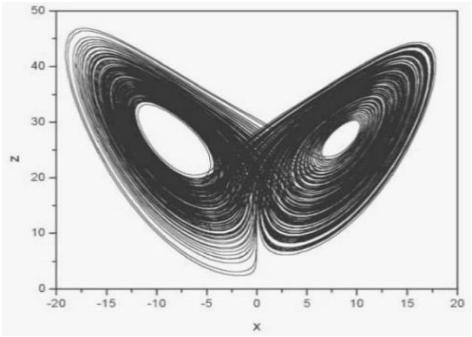

Figure 3.1 : Attracteur de Lorenz en 2D

3.10. Caractéristiques des systèmes chaotiques

- **Comportement apériodique à long terme**: Cela signifie que les trajectoires du système ne se stabilisent pas vers des points fixes, des orbites périodiques ou des orbites quasipériodiques lorsque $t \to \infty$. Ainsi, la trajectoire qui suit aura une prévisibilité limitée.
- **Système déterministe**: Cela signifie que le système n'est pas aléatoire ou n'a pas des paramètres d'entrée stochastiques. Le comportement irrégulier des systèmes chaotiques est dû à la non-linéarité intrinsèque du système plutôt qu'au bruit.
- **Sensibilité aux conditions initiales**: Cela signifie que les trajectoires, même si elles partent de conditions initiales très proches, se sépareront avec une vitesse exponentielle, c'est-à-dire que le système a un exposant positif de Lyapunov. Cela signifie qu'une prévisibilité à long terme devient impossible. [10]

3.11. Les systèmes chaotiques et la cryptographie

Il existe de fortes similitudes entre la théorie du chaos et les exigences des algorithmes cryptographiques, comme indiqué par le tableau 3.1 montrant une Comparaison entre les propriétés de la théorie du chaos et de la cryptographie

Système chaotique	Cryptographie
Sensibilité aux paramètres initiaux	Confusion et diffusion dans la clé et / ou le texte brut
Ergodicité	Confusion
Dynamique déterministe	Déterministe et pseudo aléatoire
Mélange	Diffusion

Tableau 3.1 comparaison entre les caractéristiques des systèmes chaotiques et la cryptographie

Ces similitudes ont fait du chaos une alternative attirante, comme base d'algorithmes cryptographiques.

De nombreuses recherches ont proposé la cryptographie basée sur le chaos ces dernières années. Les implémentations cryptographiques basées sur le chaos peuvent être généralement divisées en deux classes: à base analogique et à base numérique. Le chiffrement d'une information dans le chaos, s'effectue en mélangeant l'information à un signal chaotique, issue d'un émetteur décrit généralement par un vecteur d'état .la sortie de l'émetteur envoyé au récepteur, ce dernier a le rôle d'extraire l'information à partir du signal reçu. La restitution de l'information basée essentiellement sur la synchronisation entre l'émetteur et le récepteur.

Il existe plusieurs méthodes d'injection de l'information dans le système chaotique (émetteur), une seule configuration est utilisée dans ces différentes méthodes celle du Maitre-esclave d'où l'émetteur représente le maitre et le récepteur connu par l'esclave.

Dans la référence [11], on trouve les différentes techniques de cryptage bien détaillées. Parmi lesquelles on peut citer : cryptage par addition, cryptage par inclusion, cryptage par modulation-paramétrique, cryptage combiné, cryptage par décalage.

3.11.1 Cryptage par addition

Dans ce type de cryptage, l'information confidentiel $s(t)$ est additionné au signal chaotique $y(t)$ de l'émetteur, le signal résultant $m(t)$ sera transmis par un canal de transmission au récepteur, avec une synchronisation appliqué a l'ensemble du système (émetteur-récepteur), l'information $\widehat{m}(t)$peut être récupérée par une petite opération de soustraction [12].

La figure (3.2) illustre le principe de cette technique de cryptage.

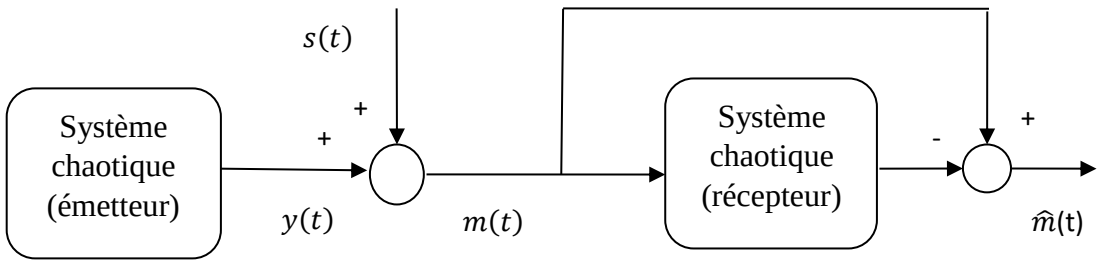

Figure 3.2 : Cryptage par addition

3.11.2 Cryptage par inclusion

Dans cette méthode l'information est injecté a la dynamique du système chaotique émetteur, après y aura une synchronisation avec le récepteur, deux méthodes en littérature sont appliqués pour la récupération de l'information, la première consiste à l'utilisation des observateurs comme par exemple, Dans [13] l'observateurs à entrés inconnu est utilisé, dans [14] l'observateur a mode glissant.

La deuxième méthode pour le décryptage est la technique par inversion du système, ici le modèle d'émetteur doit être inversé dans le récepteur pour restituer l'information.[15]

La figure (3.3) présente un schéma qui illustre cette méthode de cryptage.

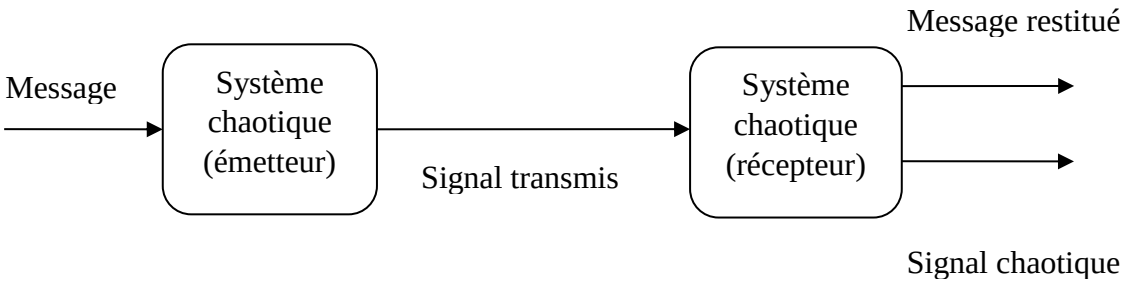

Figure 3.3 : Cryptage par inclusion

3.11.3 Cryptage par modulation-paramétrique

Dans cette technique l'information est utilisée pour moduler un ou plusieurs paramètres du système chaotique de l'émetteur [16] ,dans ce cas le signal transmis au récepteur est plus complexe qu'un signal chaotique normale par ce que la modulation réalisée dans l'émetteur provoque un changement d'attracteur ,pour obtenir une synchronisation avec le récepteur une loi d'adaptation est nécessaire .voici un schéma qui présente cette méthode.

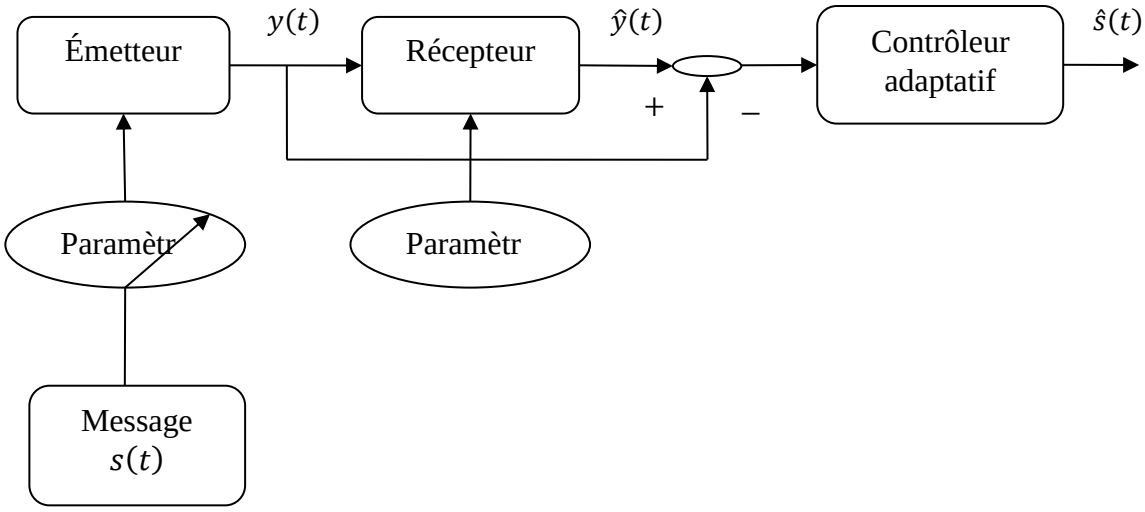

Figure 3.4 : Cryptage par modulation-paramétrique

3.11.4 Cryptage combiné

C'est une nouvelle technique qui repose sur la combinaison entre les systèmes cryptographiques classique et les systèmes qui se basent sur la synchronisation chaotique, le principe de cette méthode repose sur la réinjection du signal crypté dans la dynamique du système chaotique (émetteur), pour augmenter le degré de sa complexité, le signal est transmis de l'émetteur vers le récepteur pour assurer la synchronisation après la clé sera restauré et par conséquence le message sera décodé.

La figure (3.5) illustre cette méthode de cryptage.

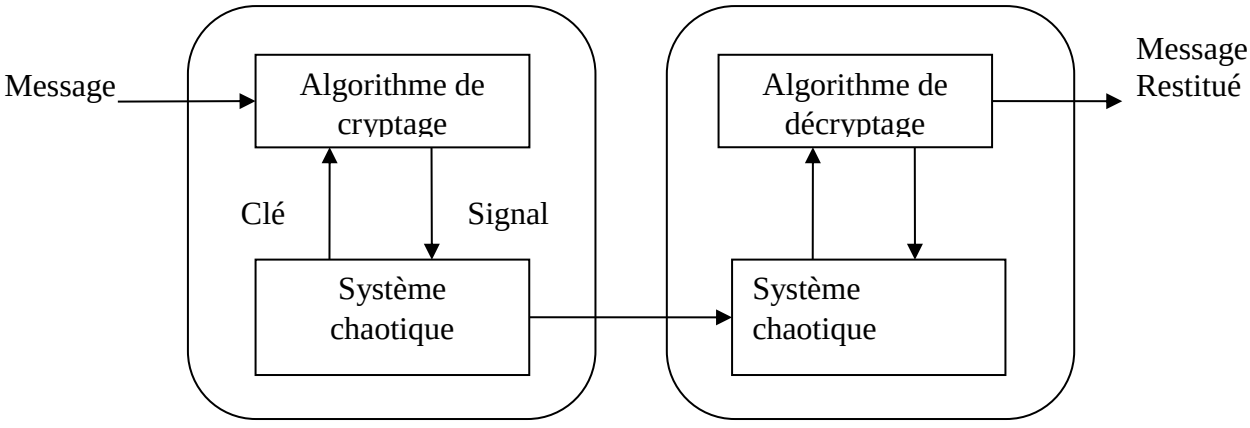

Figure 3.5: Cryptage combiné

3.11.5 Cryptage par décalage

Il est connu par CSK (chaos shift keying), cette méthode est réservée aux messages numériques, la partie émetteur est constitué de deux systèmes chaotiques, chaque système relié à un niveau binaire du message (0 et 1) respectivement, dans la partie du récepteur, en utilisant un filtre passe bas, et avec une application de seuillage à l'erreur de synchronisation, le signal peut être restitué facilement. Cette technique est appliquée sur les systèmes cryptographiques électroniques de faible dimension, on trouve de bon résultats de ce type de masquage dans [17]

La figure (3.6) illustre cette méthode de cryptage.

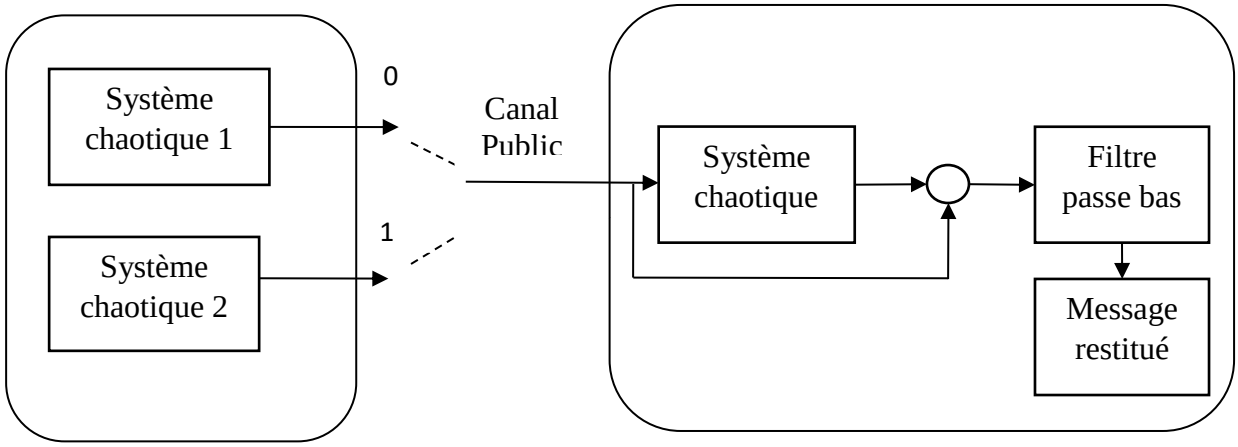

Figure 3.6 : Cryptage par décalage

3.12. Conclusion

Dans ce chapitre nous avons présenté la cryptographie et sa nécessité pour la vidéo, on a ensuite discuté des algorithmes de cryptage vidéo par rapport à la compression, ainsi que des types de cryptage ; à clé symétrique et à clé asymétrique. Nous avons également défini quelques types d'attaques cryptanalytiques, et quelques techniques de cryptage vidéos. Enfin nous avons donné quelques détails sur la cryptographie chaotique ; les systèmes chaotiques et leurs caractéristiques ainsi que quelques techniques de cryptage chaotique.

Références

[1] C. W. Chen, “Internet of Video Things: Next-Generation IoT with Visual Sensors,” IEEE Internet Things J., vol. 7, no. 8, pp. 6676–6685, 2020, doi: 10.1109/JIOT.2020.3005727.

[2] A. Mohan, K. Gauen, Y. H. Lu, W. W. Li, and X. Chen, “Internet of video things in 2030: A world with many cameras,” Proc. - IEEE Int. Symp. Circuits Syst., pp. 2–5, 2017, doi: 10.1109/ISCAS.2017.8050296.

[3] M. Abomhara, O. Zakaria, and O. O. Khalifa, “An Overview of Video Encryption Techniques,” Int. J. Comput. Theory Eng., pp. 103–110, 2009, doi: 10.7763/ijcte.2010.v2.123.

[4] Y. Negi Asstt Professor, “A Survey on Video Encryption Techniques,” Int. J. Emerg. Technol. Adv. Eng. A Surv. Video Encryption Tech., vol. 9001, no. 4, pp. 234–237, 2008, [Online]. Available: www.ijetae.com.

[5] F. Liu and H. Koenig, “A survey of video encryption algorithms,” Comput. Secur., vol. 29, no. 1, pp. 3–15, 2010, doi: 10.1016/j.cose.2009.06.004.

[6] X. Zhou and X. Tang, “Research and implementation of RSA algorithm for encryption and decryption,” Proc. 6th Int. Forum Strateg. Technol. IFOST 2011, vol. 2, pp. 1118–1121, 2011, doi: 10.1109/IFOST.2011.6021216.

[7] M. Amara and A. Siad, “Elliptic Curve Cryptography and its applications,” 7th Int. Work. Syst. Signal Process. their Appl. WoSSPA 2011, pp. 247–250, 2011, doi: 10.1109/WOSSPA.2011.5931464.

[8] B. Furht and D. Kirovski, Multimedia encryption and authentication techniques and applications. 2006.

[9] A. Sharif, N. Intan Raihana, and A. Samsudin, “Chaos-based Cryptography: A Brief Look into An Alternate Approach to Data Security,” J. Phys. Conf. Ser., vol. 1566, no. 1, 2020, doi: 10.1088/1742-6596/1566/1/012110.

[10] R. Kharel, “DESIGN AND IMPLEMENTATION OF SECURE CHAOTIC COMMUNICATION SYSTEMS,” Northumbria University, 2011.

[11] O. Megherbi, “Synchronisation des systèmes chaotiques discrets d’ordre fractionnaire pour la sûreté de communication à base d’observateurs impulsifs,” UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU, 2018.

[12] S. Li, G. Alvarez, Z. Li, and W. A. Halang, “Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey,” 2007, [Online]. Available: http://arxiv.org/abs/0710.5455.

[13] J. P. Barbot, M. Fliess, and T. Floquet, “An algebraic framework for the design of nonlinear observers with unknown inputs,” Proc. IEEE Conf. Decis. Control, pp. 384–389, 2007, doi: 10.1109/CDC.2007.4434695.

[14] K. Rabah, S. Ladaci, and M. Lashab, “A novel fractional sliding mode control

configuration for synchronizing disturbed fractional-order chaotic systems," Pramana - J. Phys., vol. 89, no. 3, 2017, doi: 10.1007/s12043-017-1443-7.

[15] H. Hamiche., "Inversion à gauche des systèmes dynamiques hybrides chaotiques : Application à la transmission sécurisée de données.," université Mouloud Mammeri de Tizi-Ouzou, 2011.

[16] T. Yang, "Secure communication via chaotic parameter modulation," IEEE Trans. Circuits Syst. I Fundam. Theory Appl., vol. 43, no. 9, pp. 817–819, 1996, doi: 10.1109/81.536758.

[17] S. H. Strogatz and A. V. Oppenheim, "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications," IEEE Trans. Circuits Syst. II Analog Digit. Signal Process., vol. 40, no. 10, pp. 626–633, 1993, doi: 10.1109/82.246163.

Chapitre 4

Simulation et interprétation des résultats

4.1. Introduction

La compression et le chiffrement des vidéos sont de plus en plus nécessaires à cause de l'augmentation de la taille des flux vidéos dans le réseau mondial et de la diversité des domaines nécessitant une confidentialité infaillible notamment avec l'arrivée des applications de l'internet des objets.

Dans ce chapitre nous allons proposer un nouvel algorithme de compression et de cryptage pour la vidéo, basé sur un cryptage chaotique par confusion et diffusion et sur une compression spatiale par ondelette. Nous allons enfin effectuer des analyses de performance de notre technique de cryptage et de compression.

4.2. Environnement de travail

4.2.1 Environnement logiciel

L'algorithme proposé ainsi que les évaluations des performances sont implémentés sous MATLAB (matrix Laboratory) qui est un langage de programmation multi-paradigmes et un environnement informatique numérique développé par MathWorks. MATLAB permet des manipulations matricielles, le tracé de fonctions et de données, la mise en œuvre d'algorithmes, la création d'interfaces utilisateur et l'interfaçage avec des programmes écrits dans d'autres langages. [1]

4.2.2 Environnement matériel

Les simulations ont été réalisés à partir d'un PC ASUS X53S :

- Mémoire RAM : 4 GB
- Processeur : Intel(R) Core (TM) i5-2450M CPU @ 2.50GHz. (2011)
- Système d'exploitation : Windows 10 Home 64 bits
- Carte Graphique : Nvidia GeForce 610m.

4.3. L'approche proposée

L'approche proposé est une combinaison de deux algorithmes que nous allons exposer, le premier pour la compression et le deuxième pour le chiffrement de la vidéo en couleur.

4.3.1 Principe général

L'algorithme principal consiste à décomposer la vidéo en trames (en images) ensuite chaque image est décomposée pour obtenir les trois matrices de couleurs (Rouge, vert et bleu), puis les trois représentations de couleurs de chaque image seront en premier compressées par transformation en ondelette et puis cryptées avec une clé générée par un système chaotique. Enfin les images sont reconstituées pour former la vidéo compressé et crypté.

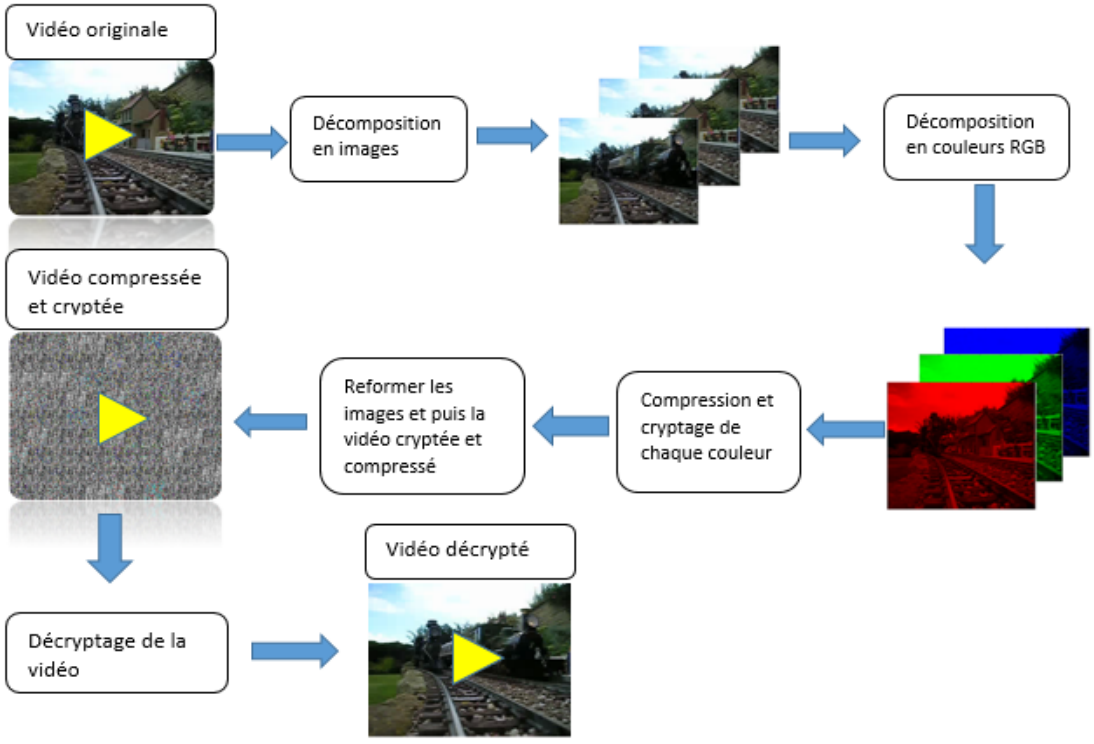

Figure 4.1 algorithme principal de compression et de cryptage

4.3.2 Principe de compression

La méthode de compression consiste à éliminer les redondances intra-trame en réalisant la compression de chaque trame indépendamment des autres. L'algorithme de compression est basé sur la transformé en ondelettes.

4.3.2.1 Le type d'Image

L'image compressé est de type RGB contenant 3 composantes (Rouge Vert et Bleu), chaque image est donc décomposée en 3 matrices de couleurs et puis on applique l'algorithme de compression sur chaque matrice.

4.3.2.2 Famille d'ondelette

Le choix de la famille d'ondelette détermine les filtres (passe haut et passe bas) dont dépend la décomposition de l'image. Le filtre passe bas donne l'approximation de l'image tandis que le filtre passe haut donne sépare les détails. Dans notre approche on a choisi l'ondelette de Haar ayant l'avantage d'être conceptuellement simple, rapide et efficace en mémoire.

$$\psi(x) = \begin{cases} 1 & 0 < t < 1/2 \\ -1 & \frac{1}{2} < t < 1 \\ 0 & ailleur \end{cases}$$

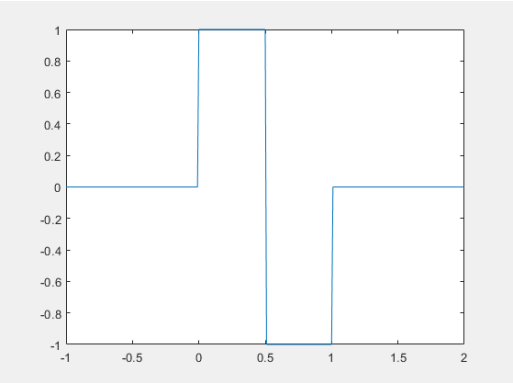

Figure 4.2: Ondelette de Haar

4.3.2.3 Niveau de décomposition

Le niveau de décomposition détermine le nombre d'application des filtres sur l'image comme montré dans la figure 4.3.

Pour mieux illustrer la méthode nous allons présenter une décomposition à 2 niveau, cependant pour notre approche nous allons étudier les résultats pour 4 niveau de décomposition.

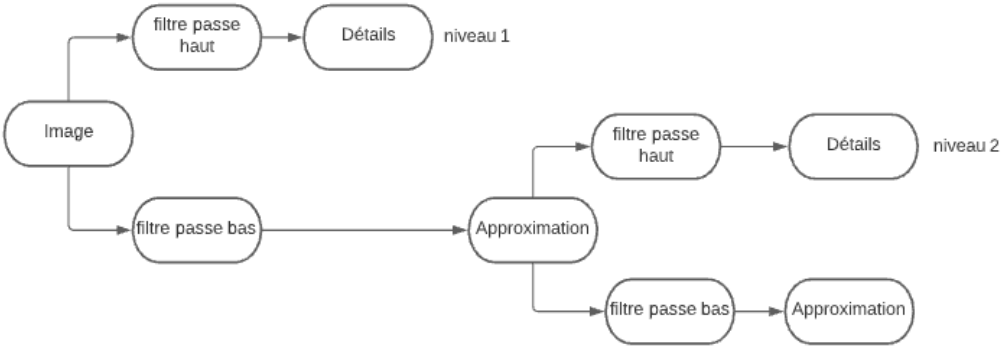

Figure 4.3: décomposition d'image en approximation et en détails à 2 niveau

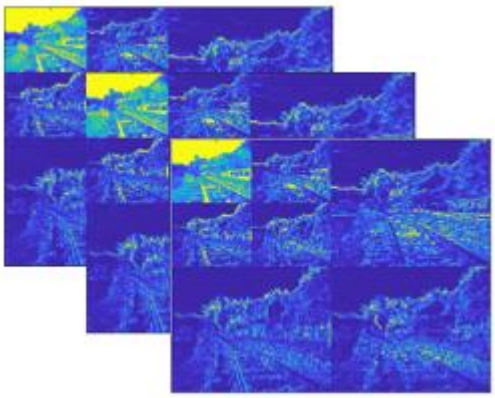

Figure 4.4 : décomposition de chaque trame de couleur

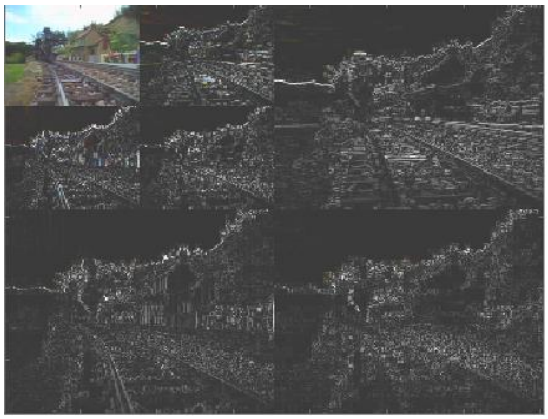

Figure 4.5 : image en couleur résultante de la décomposition

Après la décomposition on choisit le pourcentage de détail à garder pour l'image compressée, dans notre approche nous allons garder que 10% des coefficients d'ondelette les plus importants obtenus lors de la décomposition.

4.3.3 Principe de cryptage :

- La méthode de cryptage consiste à découper les trois représentations de couleur de l'image (RGB) en bloc de 32*32, en suite pour chaque bloc on réalise une confusion et puis une diffusion des pixels du bloc à l'aide d'une clé générée par un système chaotique.

En fin les blocs cryptés subissent une opération de confusion et sont ensuite reconstruits pour former l'image crypté.

- Le décryptage consiste à refaire les étapes de cryptage dans l'ordre inverse en utilisant la même clé chaotique.

Génération de la clé chaotique

La génération de la clé se fait par une fonction logistique qui donnes des valeurs chaotiques comprises entre 0 et 1 qui dépendent largement des conditions initiales et du coefficient r.

$$x(i) = 1 - abs(r * x(i-1) * x(i-2))$$

Un changement, aussi infime qu'il soit, de r, x (1) ou x (2) change radicalement les valeurs de la clé ce qui est souhaitable pour le cryptage.

Cryptage par confusion

La confusion consiste à désordonner les pixels d'une image, dans notre approche la diffusion se fait selon une clé chaotique, le nouvel emplacement des pixels est donc déterminé par cette clé.

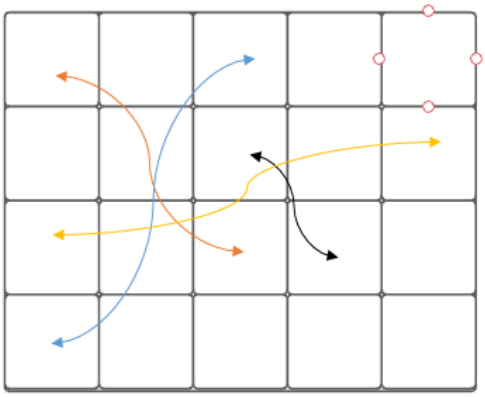

Figure 4.6 Principe de confusion des pixels

- Par ce même principe, on fait la permutation des blocs après la diffusion à l'aide d'une partie de cette même clé chaotique.

L'application du cryptage par confusion seul donne des images assez dégradées visuellement comme montré dans la figure 4.7, mais l'histogramme des images reste le même. Pour obtenir des images plus sécurisé nous allons réaliser un cryptage par diffusion après la permutation des pixels.

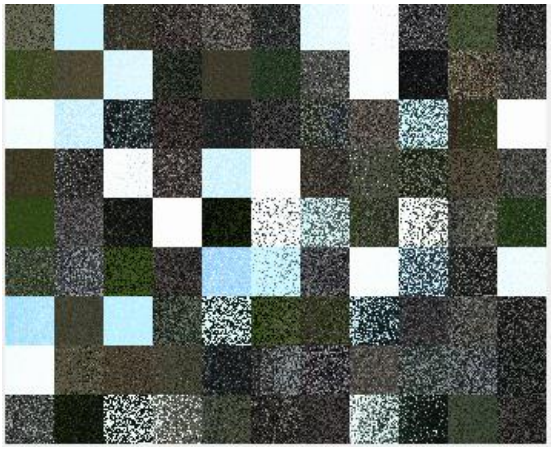

Figure 4.7 : image chiffrée par permutation seulement

Cryptage par diffusion :

La diffusion consiste à modifier les valeurs des pixels ce qui change les données statistiques de chaque image en clair, on obtient à la fin un histogramme bien répartie et totalement différent des images en clair.

Dans notre approche la diffusion est faite par la clé utilisé pour la confusion décalée (les mêmes valeurs de la clé mais avec un décalage), chaque pixel codé sur 8 bits subit une opération XOR avec une partie de la clé décalée.

4.3.4 Le décryptage : L'algorithme de décryptage consiste à refaire les étapes de cryptage en utilisant la même clé chaotique, en premier les blocs sont restitués en suite on réalise l'opération XOR entre la clé et l'image crypté et en fin on fait la permutation des pixels pour reconstruire l'image original**.**

Figure 4.8 cryptage et décryptage de la vidéo

4.4. Evaluation des performances des techniques de cryptage de vidéos

En raison de certaines caractéristiques des données multimédias, telles que la grande taille des données et la redondance élevée, un algorithme de cryptage idéal devrait satisfaire certains critères. Il doit assurer la sécurité des applications en temps réel et les limitations d'énergie comme le temps de traitement et la complexité de l'algorithme pour le cryptage et le décryptage.

- **Optimisation :** Il pourrait être très souhaitable de pouvoir définir dynamiquement la partie chiffrée et les paramètres de chiffrement en fonction des différentes applications et exigences. La définition statique de la partie chiffrée et des paramètres chiffrés limite l'utilisation du schéma à un ensemble restreint d'applications.
- **Vitesse:** dans de nombreuses applications en temps réel, il est important que les algorithmes de chiffrement et de déchiffrement soient suffisamment rapides pour répondre aux exigences en temps réel.
- **Taux de cryptage** : Ce critère mesure la quantité de données à crypter. Le taux de cryptage doit être minimisé pour réduire la complexité de calcul.
- **Sécurité cryptographique** : la sécurité cryptographique définit si le schéma de cryptage est sécurisé contre les attaque par force brute et les différentes attaques de texte en clair. Pour une application multimédia de grande valeur, le schéma de cryptage doit satisfaire à la sécurité cryptographique.
- **Conformité du format :** le flux de bits crypté doit être conforme au compresseur. Et le décodeur standard devrait être capable de décoder le flux de bits crypté sans décryptage.
- **Dégradation visuelle:** Ce critère mesure la distorsion perceptive des données d'image par rapport à l'image d'origine. Dans certaines applications, il peut être souhaitable d'obtenir une dégradation visuelle suffisante pour qu'un attaquant comprenne toujours le contenu mais préfère payer pour accéder au contenu non crypté. Cependant, pour les données sensibles, une dégradation visuelle élevée pourrait être souhaitable pour masquer complètement le contenu visuel.
- **Compatibilité avec la compression:** Un schéma de cryptage est considéré comme convivial pour la compression s'il n'a aucun ou très peu d'impact sur l'efficacité de la compression des données. Certains schémas de chiffrement ont un impact sur la compression des données ou introduisent des données supplémentaires nécessaires au déchiffrement. Il est souhaitable que la taille des données cryptées n'augmente pas. [2]

4.5. Critères d'évaluation de la qualité de compression

Il existe plusieurs Critères pour évaluer la qualité du signal reconstruit par rapport à celui d'entrée. Il est souhaitable d'obtenir la distorsion D la plus faible possible alors qu'une grande partie des informations a été rejetée.

Erreur quadratique moyenne (MSE)

L'évaluation de distorsion la plus couramment utilisée est la MSE (Mean Squared Error), définie par :

$$\mathrm{MSE}(f, f') = \frac{1}{n}\sum_{i=1}^{n}(f_i - {f'}_i)^2$$

Où n est la taille du signal d'entrée, f est le signal original et f' est le signal reconstitué.

La distorsion est minimisée lorsque le MSE s'approche de zéro.

PSNR (Peak Signal to Noise Ratio)

Pour la compression d'images et de vidéos, le MSE est le plus souvent exprimé en termes de mesure réciproque équivalente, PSNR est défini par :

$$\mathrm{PSNR}\ (f, f') = 10\ log_{10}\frac{(2^b - 1)^2}{MSE(f, f')}$$

Où b est le nombre de bits par pixel. Le PSNR est exprimé en dB (décibels) et il est basé sur l'erreur absolue entre les signaux d'entrée et de sortie. Le PSNR s'approche de l'infini tandis que le MSE s'approche de zéro, ce qui signifie qu'une valeur PSNR élevée fournit une qualité d'image élevée. A l'autre extrémité de l'échelle, une faible valeur du PSNR implique des différences numériques élevées entre les images.

SSIM (Structural SIMilarity)

Le SSIM utilisé pour mesurer la similarité entre deux images, cette métrique est un modèle basé sur la perception qui considère la dégradation de l'image comme un changement perçu dans les informations structurelles, tout en incorporant également d'importants phénomènes perceptuels, y compris les termes de masquage de luminance et de masquage de contraste. [3]

4.6. Analyse des résultats de simulation

Les résultats expérimentaux sont donnés dans cette section pour démontrer l'efficacité de la méthode de cryptage vidéo proposée. L'algorithme est effectué sur une vidéo en couleurs ayant 210 trames, les trames (images) ont une taille de 352*288 pixels chaque pixel est codée sur 24 bits (8 bits pour chaque couleurs RGB). La vidéo dure 8s avec une vitesse de 25 trames par seconde.

4.6.1 MSE (erreur quadratique moyenne) et PSNR (Peak Signal to Noise Ratio)

Nous allons calculer le MSE et le PSNR pour chaque trame, pour une analyse plus clair nous allons la moyenne de ces deux paramètres pour la totalité de la vidéo.

La compression par ondelette de Haar a donné un MSE de **58.5145** et un PSNR de **30.4953** en moyenne. Avec un taux de compression de **2.6**.

- Les résultats du MSE et du PSNR indique l'existence d'une dégradation acceptable de l'image compressée.

4.6.2 SSIM (Structural SIMilarity)

Une autre évaluation de la dégradation de l'image est le SSIM.

La moyenne du SSIM de la vidéo compressé est obtenues par : $\frac{1}{n}\sum SSIM_i$

Ou n est le nombre des images dans la vidéo et SSIMi le SSIM de chaque image comparée avec l'image original.

Nous avons obtenu un SSIM de **0.9066** indiquant une bonne qualité d'image par rapport à l'image originale.

4.6.3 Histogramme

L'un des buts du cryptage vidéo est d'avoir un histogramme avec une distribution uniforme des valeurs des pixels. Pour une analyse meilleure nous allons calculer l'histogramme cumulé de l'intégralité de la vidéo en cumulant les histogrammes de chaque image. Les figures 4.9 et 4.10 représentent successivement l'histogramme de la vidéo à l'entré et l'histogramme de la vidéo cryptée.

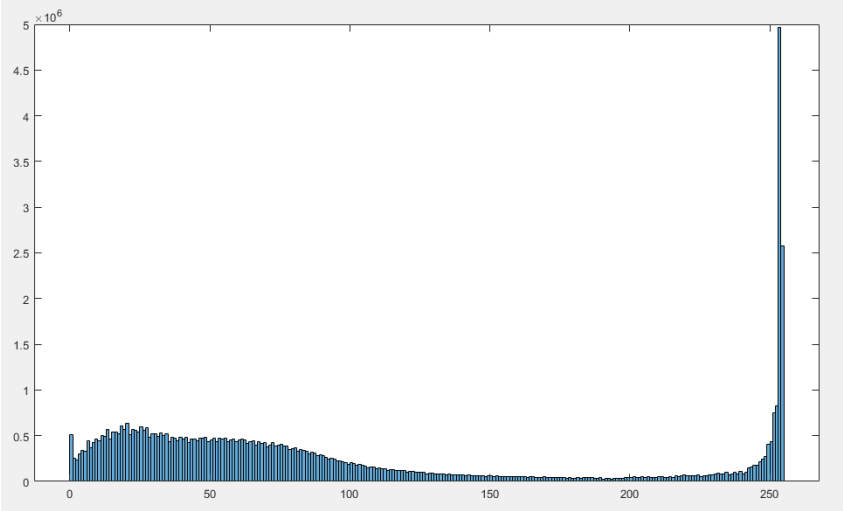

Figure 4.9: l'histogramme de la vidéo à l'entrée

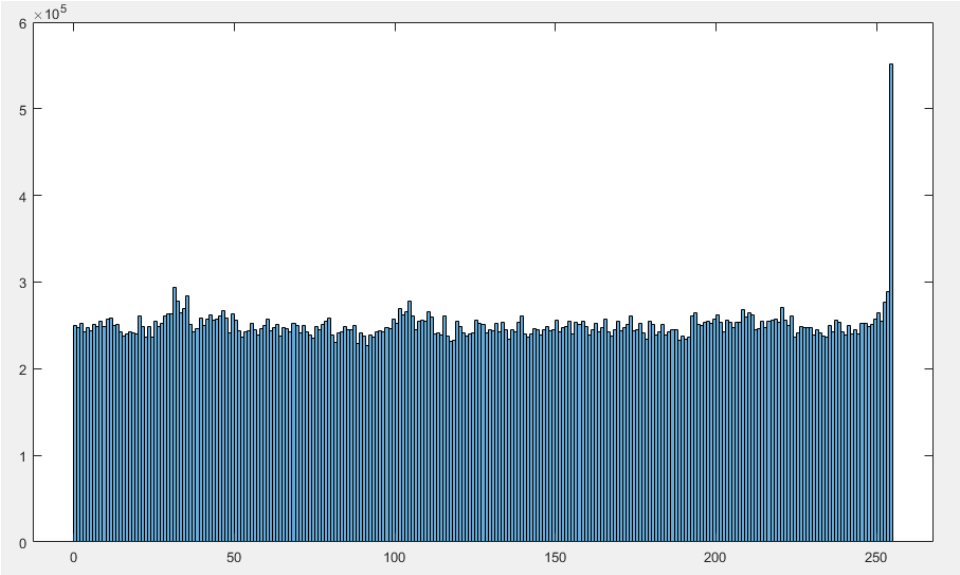

Figure 4.10: l'histogramme de la vidéo cryptée

- On a donc obtenu un histogramme ayant une distribution relativement uniforme
- Le pic à la dernière valeur est causé par la nature de la vidéo à l'entrée

4.6.4 Entropie

L'entropie de l'information est la caractéristique la plus significative de l'imprévisibilité. Il peut être utilisé pour mesurer la distribution de la valeur de gris dans l'image. L'entropie H(m) d'un m peut être calculée comme :

$$\mathrm{H(m)} = \frac{1}{n}\sum_{i=0}^{2^n-1} p(m_i)\, log_2(\frac{1}{p(m_i)}$$

où 2^n est le nombre total de symboles, et p(m_i) représente la probabilité du symbole mi. Pour une image aléatoire avec 256 niveaux de gris, l'entropie devrait idéalement être H(m) = 8. Par conséquent, un algorithme de cryptage efficace devrait produire une image cryptée d'entropie proche de 8.[4]

Comme pour l'histogramme nous allons calculer l'entropie moyenne de la vidéo.

On a obtenu une entropie égale à **7.9967**, qui est assez proche de 8, l'image crypté est donc assez imprévisible.

4.6.5 Coefficients de corrélation

Nous analysons les corrélations entre deux pixels adjacents horizontalement, verticalement et diagonalement. Les figures 4.11,4.12 et 4.13 montrent les corrélations horizontales, verticales et diagonales d'une image originale et d'une image cryptée produites par l'algorithme proposé.

Pour ce critère nous allons nous contenter d'analyser les 3 matrices de couleurs de la première image, cependant l'analyse des autres images donne plus ou moins les mêmes résultats.

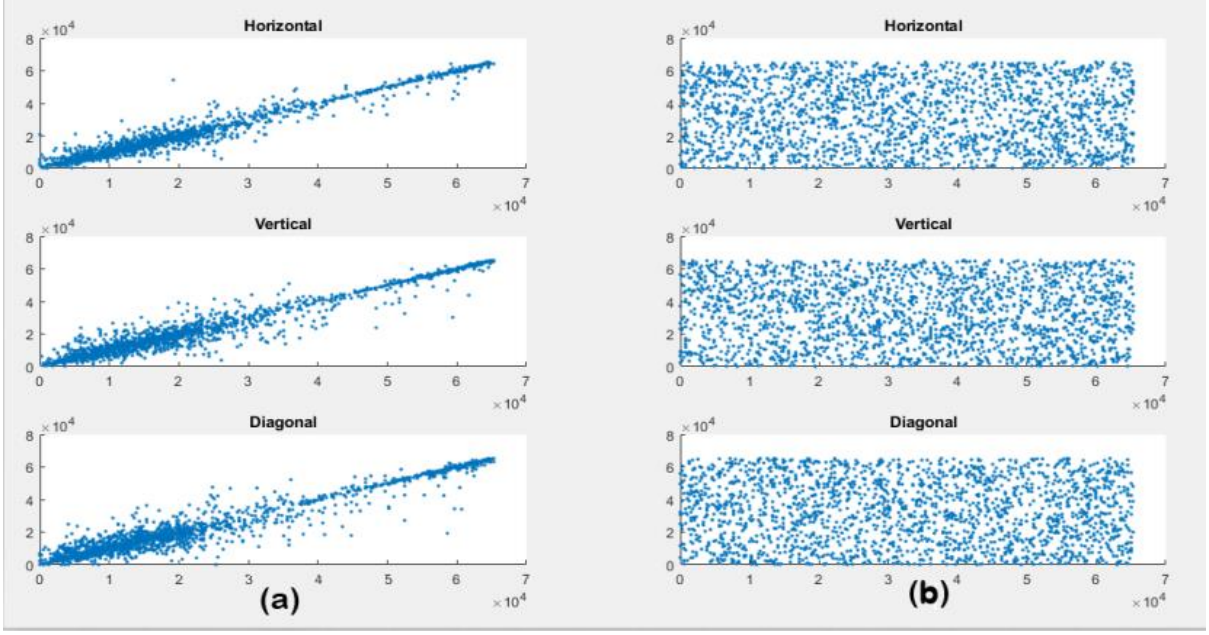

Figure 4.11. (a) corrélations de l'image original, (b) corrélations de l'image cryptée. (Pour la matrice de la couleur rouge)

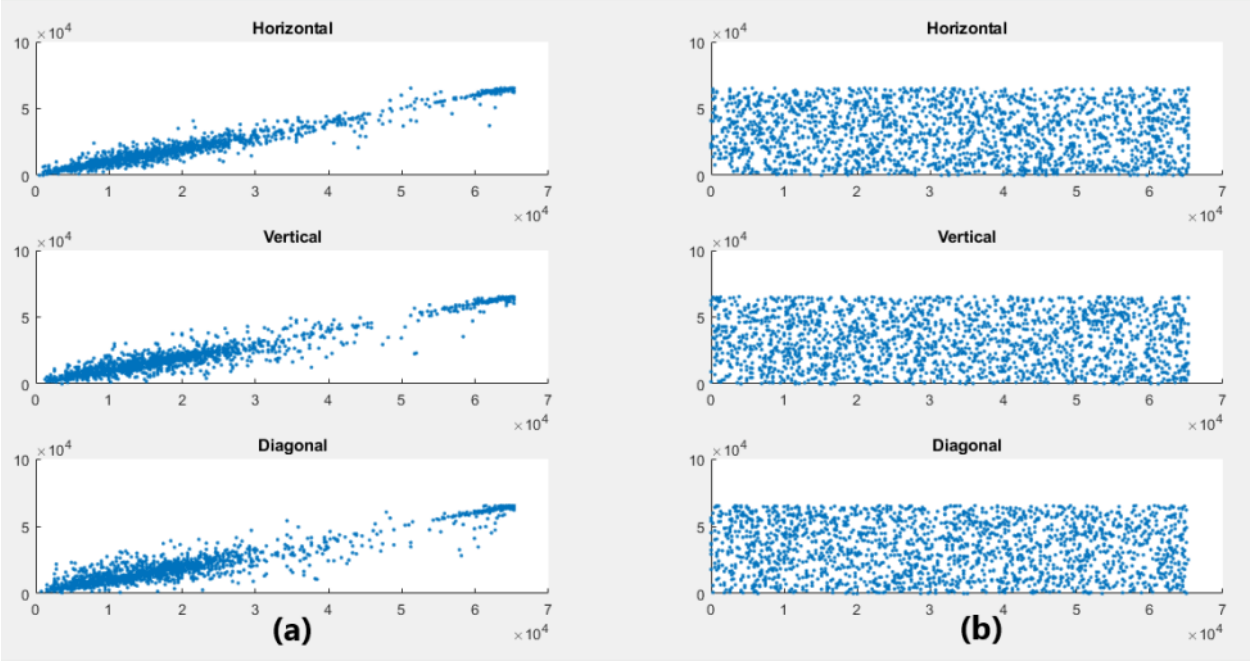

Figure 4.12 : (a) corrélations de l'image original, (b) corrélations de l'image cryptée. (Pour la matrice de la couleur verte)

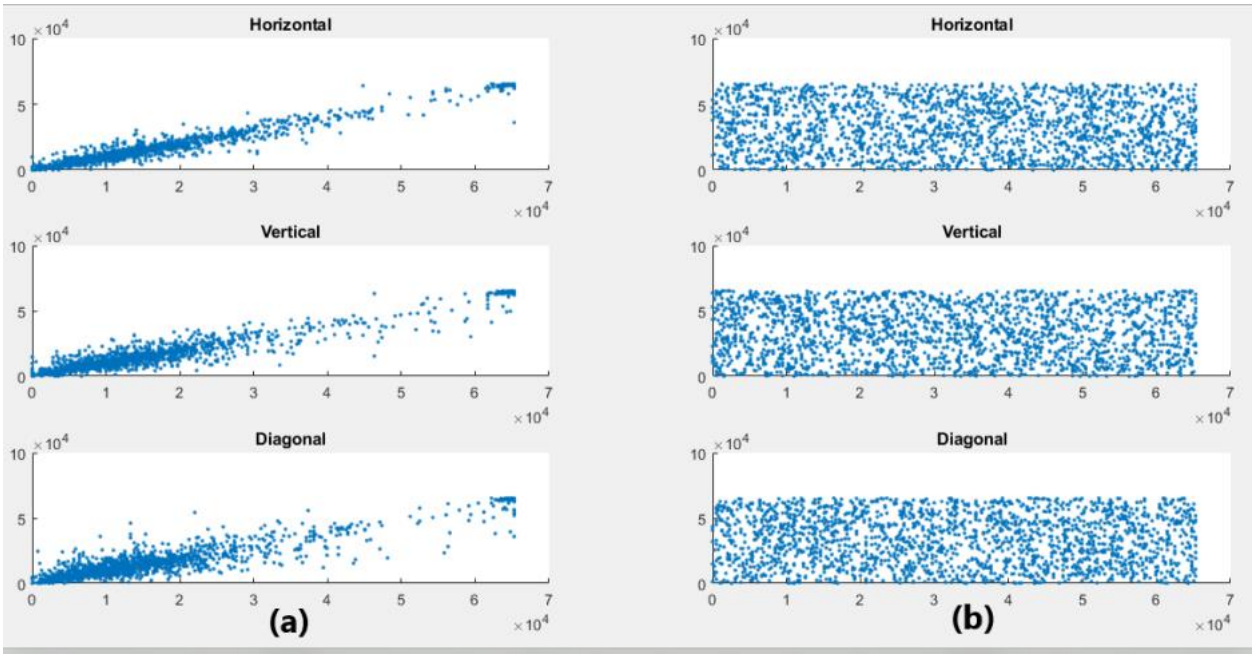

Figure 4.13: (a) corrélations de l'image original, (b) corrélations de l'image cryptée. (Pour la matrice de la couleur bleue)

- Les trois figures 4.11 (a) 4.12 (a) et 4.13 (a) affichent les trois corrélations dans l'image original (horizontal, vertical et diagonal), où les points représentatifs se concentrent près de la diagonale, donc le coefficient de corrélation est assez proche de 1, ce qui implique une forte corrélation entre les pixels adjacents.
- Les trois figures 4.11 (b) 4.12 (b) et 4.13 (b) montrent les trois corrélations dans l'image cryptée, où les pixels adjacents horizontaux, verticaux et diagonaux sont presque sans importance. Le coefficient de corrélation est donc proche de 0.

4.7. Conclusion

Dans ce chapitre nous avons présenté l'approche proposé en expliquant les étapes de décomposition de la vidéo, de la compression par transformé en ondelette et du cryptage chaotique. Nous avons ensuite discuté des Critères d'évaluation de la qualité de compression et du cryptage. Enfin nous avons présenté les résultats des simulations d'évaluation de la qualité de compression (PSNR, MSE et SSIM) et des simulations d'évaluation de la qualité de cryptage (histogramme, entropie, corrélation) les résultats ont confirmé l'efficacité de notre approche.

Références

[1] https://en.wikipedia.org/wiki/MATLAB.

[2] J. Shah and V. Saxena, "Performance Study on Image Encryption Schemes." 2011, [Online]. Available: http://arxiv.org/abs/1112.0836.

[3] E. Doutsi, "Retina-inspired Image and Video coding," Université Côte d'Azur, 2017.

[4] X. Zhang, L. Shao, Z. Zhao, and Z. Liang, "An image encryption scheme based on constructing large permutation with chaotic sequence," *Comput. Electr. Eng.*, vol. 40, no. 3, pp. 931–941, 2014, doi: 10.1016/j.compeleceng.2013.08.008.

Conclusion générale

Dans ce travail nous nous sommes intéressés à la compression et au cryptage vidéo dans le cas de l'Internet des objets. Ce travail nous a permis de renforcer les connaissances concernant l'internet des objets, la compression d'image et de vidéo en particulier la transformé en ondelette, et le cryptage vidéo, en particulier le cryptage chaotique.

Dans le premier chapitre nous avons présenté un état de l'art de l'internet des objets, on a d'abord donné une définition à l'IoT et aux objets IoT, on a expliqué le fonctionnement de cette nouvelle technologie et nous avons défini les éléments constituant un système IoT, on a aussi parlé des applications de l'IoT et des défis que posent certaines applications.

On s'est concentré ensuite sur la compression d'image vidéo, on a donné des notions sur la vidéo, expliqué les redondances dans les vidéos et discuté des différents types de compression ; sans perte comme le codage de Huffman et le codage arithmétique, et avec perte comme la transformé en cosinus ou la transformé en ondelette. On a aussi expliqué la compression par transformé en ondelettes et présenté quelques familles d'ondelettes. On a enfin présenté quelques standards de compression image et vidéo les plus utilisés, et ceci dans le deuxième chapitre.

Dans le troisième chapitre on s'est focalisé sur la cryptographie, on l'a définie, expliqué le besoin dans le cas des vidéos et parlé de la relation entre le cryptage et la compression, on a ensuite parlé des types de cryptage (à clé symétrique et à clé asymétrique). On a aussi défini la cryptanalyse et donné quelques types d'attaques cryptanalytiques, et puis on a présenté quelque approche pour le cryptage vidéo (approche naïve, permutation pure, cryptage basé sur le chaos…) enfin on a parlé de la cryptographie chaotique en définissant les systèmes chaotiques et leurs caractéristiques en plus des techniques de cryptage chaotique (par addition, par inclusion, par décalage…).

Nous avons présenté notre approche de compression et de cryptage vidéo dans le dernier chapitre, on a d'abord parlé de l'algorithme principale ou l'on décompose la vidéo,

ensuite on a expliqué l'algorithme de compression se basant sur la transformé en ondelette, ensuite on a présenté l'algorithme de cryptage par une clé générée par un système chaotique (fonction logistique). On a ensuite présenté les critères d'évaluation de qualité de compression et de cryptage. Et enfin on a présenté et discuté les résultats des simulations de notre algorithme, on a d'abord réalisé des évaluations de qualité de compression (PSNR, MSE et SSIM) ensuite on a réalisé des évaluation de qualité de cryptage (histogramme, entropie, corrélation). Les résultats obtenus ont indiqué que notre méthode est efficace pour la compression et pour le cryptage.

Les perspectives qui peuvent être envisagé consistent à améliorer le taux de compression par la compression des redondances temporelles, et à implémenter cet algorithme dans une carte FPGA pour une performance plus rapide et plus souhaitable pour les applications de l'IoT.