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

Université Abou Bekr Belkaid de Tlemcen
Faculté de Technologie
Département de Génie Biomédical
Laboratoire de Génie Biomédical

Master En
IMAGERIE MEDICALE

(2 ème Année)

"BM 941"

POLYCOPIE DE COURS & TD

INFORMATIQUE MEDICALE

Filière de Génie Biomédical

Elaboré par :

Mr /BOUKLI HACENE Ismail

Couriel: ismail.bouklihacene@univ-tlem.dz

Année universitaire : 2020 – 2021

Préface :

L'informatisation des images médicale s'est progressivement affirmée en tant que discipline scientifique moderne d'une importance capitale dans le processus d'amélioration de la qualité de soin, de la performance de service de radiologie et hospitalier.

Cet ouvrage de cours et de travaux dirigé s'adresse aux étudiants de licence professionnelle en Génie Biomédicale, spécialité « informatique dans un milieu hospitalier », aux étudiants de Master M2 en IMAGERIE MEDICALE et aux chercheurs ou ingénieurs débutant une activité dans le domaine de la radiologie et le système d'information hospitalier et en santé ; et qui souhaitent d'améliorer la qualité des soins en Algérie. Il pourra également intéresser les enseignants pour la préparation de travaux pratiques.

Il permet d'offrir une formation interdisciplinaire généraliste qui aborde les différents enjeux de la mise en œuvre et de l'utilisation appropriée d'outils informatiques pour soutenir la pratique médicale et soignante, et plus largement le fonctionnement des systèmes de santé (Système d'information en Santé 'SIS', Système d'information Hospitalier 'SIH', Système d'Information en Radiologie 'SIR').

Notre ouvrage est scindé en six (06) chapitres ; le premier a pour objectif l'étude des principes des SGBD relationnels et la mise en pratique de ces principes tels que Conception d'un schéma relationnel et sur le langage d'interrogation et de manipulation, ou l'accent est mis sur SQL et ses fondements. Le deuxième chapitre fera l'objet d'une analyse empirique dans l'objectif est d'analyser la contribution du SIH dans l'amélioration de la performance au sein de nos hôpitaux. Il sera consacré à expliquer quels sont les objectifs d'un système d'information hospitalier et lister les principaux sous système et ensemble de fonctions pouvant faire l'objet d'une informatisation ; tel que le dossier patient informatisé.

Le gros challenge pour les hôpitaux actuellement est la mise en place d'un système d'information permettant l'échange, l'archivage et de partage de données numérisées, et en particulier des images médicales. Ces systèmes appelés PACS (Picture Archiving and Communication System) pour les images ou RIS (Radiology Information System) pour les autres données. Le troisième chapitre vous invite à découvrir ces réseaux de partage d'images numériques, leurs avantages pour les établissements de santé et les patients et leurs enjeux.

L'existence de plusieurs problèmes liés à l'archivage des images médicales et à la communication entre les machines des différents constructeurs a été résoudre par la naissance de standard DICOM '**D**igital **I**maging and **Co**mmunication in **M**edicine' qui fait l'objet du **4**eme chapitre. Il permet d'obtenir des images du patient ainsi que toutes les informations associées dans un format identique permettant l'interconnexion et l'interopérabilité des équipements et le transfert des données médicales.

Le transfert et archivage de ces images médicales provoque la saturation de système PACS, ou il est nécessaire de compresser ces images pour une transmission fiable et rapide.

A f i n de Familiariser l'étudiant sur les techniques de codage et de compression des images médicale ; le chapitre **5** viser a données aux étudiants les fondements de base pour l'évaluation des avantages et les inconvénients des différentes techniques de compression des images médicales en utilisant la transformée en ondelette par les codeurs de sous bande EZW,SPIHT; ainsi que les critères de choix d'une technique de compression des images médicales.

En fin, l'objectif de dernier chapitre est de sensibiliser l'étudiant sur l'importance de la sécurité informatique et le lui apprendre à maîtriser les technologies et les algorithmes robustes utilisés en sécurité informatique dont le but est la protection des images médicale.

Tout commentaire ou proposition ou critique constructive permettant l'amélioration des textes ainsi élaborés sera recueillie avec grand intérêt.

Je tiens à remercier Mr CHIKH Mohammed el-Amine, et Mr ABDERRAHIM Mohammed elAmine , pour tout l'intérêt qu'ils ont témoignés pour examiner ce travail.

Mr. BOUKLI HACENE Ismail

Table des matières

1. Introduction :

L'informatique évolue vers le traitement de masses d'informations médicale de plus en plus grandes dans des environnements répartis géographiquement ou doivent cohabiter des matériels hétérogènes, tel que nous trouve dans les systèmes d'information hospitaliers (SIH) en générale, et le système d'information en radiologie (SIR) en particulier les images médicale de grandes volumes.

Les bases de données sont utilisées de façon intensive pour de nombreux domaines d'application telle que le domaine médical, les administrations ou les associations. Les applications concernées par l'utilisation d'un SGBDM possèdent des caractéristiques différentes tant au niveau de volume du données concernées qu'un niveau de la complexité de ces données et des traitements informatique à réaliser.

On distingue classiquement l'information au sens usuel de renseignement, et la notion de donnée, information codée et stockée sur un support informatique en vue d'un traitement ultérieur. L'utilisation des données en informatique médicale tente de répondre à deux objectifs plus ou moins contradictoires :1) rester proche de la structure naturelle de l'information ; et 2) adopter la représentation informatique la plus efficace.

Ainsi, deux problèmes doivent être résolus :1) comment organiser les informations de façon à obtenir le système le plus efficace et le plus informatif (problème de structuration de l'information médicale) ;2) Comment représenter les informations afin d'en conserver le maximum de richesse sans s'interdire les possibilités de traitement automatique de l'information (problème de standardisation du langage médical).

Leur maîtrise permet d'envisager l'informatisation du dossier du malade. Par contre, en l'absence de structuration et d'organisation préalables de l'information en vue de son utilisation ultérieure, on est confronté à ce qu'on appelle un cimetière de données. La gestion et le traitement de ces données se faisant par la méthode classique à laquelle on a pu dégager les défauts suivants :

- ✓ La redondance des données
- ✓ La dépendance pleine entre donnée et traitement
- ✓ Le manque de normalisation au niveau de stockage des données

2. Gestion Informatique des données Médicales

: Une structure de données correspond à une manière d'organiser et de représenter les données. Les deux types de renseignements contenus dans une structure de données sont les données proprement dites et les liens qui peuvent exister entre elles, formalisés par leur organisation. L'organisation de ces données en informatique est essentiellement celui de leur stockage et de leur accès sur une mémoire secondaire. Deux classes de systèmes peuvent être utilisées : les fichiers et les bases de données.

2.1 Qu'est-ce qu'une base de données ?

Le concept de base de données (BDD) est apparu vers 1960, face au nombre croissant d'informations que les entreprises devaient gérer et partager :

- ***Base de données***- Un ensemble organisé d'informations avec objectif commun. Plus précisément, on appelle base de données un ensemble structuré et organisé des données permettent le stockage de grandes quantités d'informations afin d'en faciliter l'exploitation (ajout, mise à jour, recherche et consultations des données) accessibles à la demande pour plusieurs utilisateurs et des besoins divers.
- ***Base de données informatisée***-est un ensemble structuré de données enregistrées sur des supports accessibles par ordinateur, représentant des informations du monde réel et pouvant être interrogées et mises par une communauté d'utilisateurs.

La gestion et l'accès à une base de données sont assurés par un ensemble de programme que constitue le système de gestion de base de données (SGBD).Ainsi la notion de base est généralement couplée à celle des réseaux informatiques afin de pouvoir mettre en commun les informations d'où le nom « base ».

On parle souvent de système d'information pour désigner toute structure regroupant les moyens mis en place pour partager les données **[1]**

On appelle l'ensemble de données organisées par FICHIER (enregistrement, article ou fiche) en vue d'une application déterminée comme par exemple un répertoire téléphonique, un carnet d'adresses, un dictionnaire ou une fiche de malade qui seront tous représentés par des entités tel leur nom, leur prénom, leur date de naissance et leur sexe, seules changeant les valeurs de ces caractéristiques pour chaque individu.

La multiplication des fichiers entrainait la redondance des données, ce qui rende difficile les mise à jours, d'où l'idée d'intégration et de partage des données.

2.2.But d'une base de données médicale?

1. Récolter des données dans un but spécifique :
   - Suivie médicale du patient (antécédents, traitements administrés, symptômes observés.
   - Etude clinique : analyse d'une population pour améliorer le traitement ou le diagnostique d'une maladie, d'un protocole.
2. Stocker des informations pour faciliter l'exploitation (ajout, suppression, recherche,…)
3. Résultats : décrire les données.

3. SYSTEME DE GESTION DE BASE DE DONNEES

3.1- Définition : Un SGBD peut être vu comme un système informatique (ensemble des programmes et logiciels) spécialisé dans le traitement de gros volumes d'informations et permettant à différents utilisateurs d'interagir avec la base de données.

On peut aussi définir le SGBD par un ensemble de programme qui :

- Gere un ensemble de fichier (base de donnée)
- Permet aux utilisateurs d'extraire ou de stockées des données ; ainsi il permet de crées, modifier (mettre à jours), interroger, visualiser, administrer une BD.

3.2- L'objectif des SGBD :

Les bases de données et les systèmes de gestion de bases de données ont été créés pour répondre à un certain nombre de besoin et pour résoudre un certain nombre de problèmes**.**

Leurs principaux objectifs sont les suivants :

1. Garantir l'**indépendance** physique et logique entre les données et les programmes d'application :
   - Les données et les programmes étant séparés, ce ne sont plus les applications qui sont chargées de structurer, d'organiser et de vérifier les données et de les stocker dans un fichier.
   - Les données sont définies et structurées par le SGBD qui offre cette structure aux applications.
   - L'indépendance est à la fois logique (au niveau de la définition des données) et physique (au niveau de stockage et de la gestion de la mémoire)
     - ✓ **Indépendance physique** : La façon dont les données sont définies doit être indépendante des structure de stockages utilisées.
     - ✓ **Indépendance logique** : Un même ensemble de données peut être vu différemment par des utilisateurs différents. Toutes ces visions personnelles des données **doivent être intégrées** dans une **vision globale**
2. Assurer la persistance des données :
   - ✓ alors que les résultats d'une application sont liés à l'exécution de l'application, **l'existence des données d'une base est assurée indépendamment de leur utilisateur.**
   - ✓ Les données d'une base **ont donc une durée de vie supérieure** à la durée de vie du programme qui les crée ou qui les utilise

3. Permettre une **administration centralisée** des données :
   - ✓ Une des fonctions essentielles des SGBD est la définition des structures de données, la définition et l'organisation des structures de stockage, les modifications de ces structures, les contrôles de validité et de cohérence.
   - ✓ **Il est essentiel de centraliser ces fonctions :** c'est l'administrateur du système qui gère l'ensemble des données, indépendamment de leur utilisation et des applications.
   - ✓ Les **usagers** ou les **applications sont déchargés** de toute tache d'administration, et peuvent utiliser les données de la base sans se préoccuper de l'administration de ces données tout en étant **assurés** de leur validité et leur cohérence.
   - ✓ Un SGBD permet **d'optimiser l'administration des données** en centralisant ces taches dans l'entreprise
4. Gérer la mémoire de façon optimale et assurer l'efficacité de l'accès aux données :

Chaque SGBD optimise le stockage et l'accès aux données, en utilisant des techniques complexes inaccessibles aux programmes d'application eux-mêmes. En évitant les redondances, il optimise également le volume des données stockées. Avec un SGBD, on est donc sur d'avoir accès à de volumineux ensembles de données de manière efficace car :

- ✓ Un SGBD permet d'obtenir des réponses aux interrogations en un temps « raisonnable ».
- ✓ Un SGBD utilise un mécanisme permettant de minimiser le nombre d'accès disques.
- ✓ Tout ceci, bien sûr, de façon complètement transparente pour l'utilisateur

5. Gérer le partage des données entre utilisateurs et les accès concurrents : il s'agit de permettre à plusieurs utilisateurs d'accéder aux mêmes données au même moment. Si ce problème est simple à résoudre quand il s'agit uniquement d'interrogations et quand on est dans un contexte mono-utilisateur, cela n'est plus le cas quand il s'agit de modifications dans un contexte multi-utilisateurs. **Il s'agit alors de pouvoir :**
   - ✓ Permettre à deux ou plus utilisateurs de modifier la même donnée en même temps
   - ✓ Assurer un résultat d'interrogation cohérent pour un utilisateur consultant une table pendant qu'un autre la modifie.

C'est le SGBD qui va se changer de **gérer** les accès **concurrents**, les **mises à jours**, le tout en fonction des **droits de chacun**. Chaque usager aura **l'illusion d'être seul à utiliser** les données de la base, qu'il verra assemblées et structurées comme il le souhaite.

6. Assurer la fiabilité, l'intégrité et la cohérence des données, éviter les redondances :
   - ✓ La description du schéma des données contient un certain nombre de règles qui permettent de vérifier la fiabilité, l'intégrité, la cohérence de tous les objets présents dans la base.

Par exemple, l'âge d'une personne doit être compris entre 0 et 120 ; et l'âge d'un enfant ne peut être supérieur à celui de ses parents, ect….

- ✓ Le SGBD contient des procédures spéciales permettant d'effectuer l'ensemble de ces tests. Comme par exemple, les contraintes d'intégrité sont des règles qui précisent la cohérence sémantique des données entre elles.
  - Les données sont soumises à un certain nombre de contraintes d'intégrité qui définissent un état cohérent de la base
  - Elles doivent pouvoir être exprimées simplement et vérifiées automatiquement à chaque insertion, modification ou suppression des données.
- ✓ Eviter la redondance des données : afin d'éviter les problèmes lors des mises à jour, chaque donnée ne doit être présente qu'une seules fois dans la base.

7. Assurer la **sécurité** des données : Tous les utilisateurs d'une même base n'ont pas nécessairement les mêmes droits d'accès aux données. il est utile de pouvoir **définir de tels droits** pour assurer la sécurité de certaines données confidentielles et réservées à certains groupes d'utilisateurs.
8. Résistance aux pannes :

   Que se passe-t-il :

   - Si une panne survient au milieu d'une modification,
   - Si certain fichiers contenant les données deviennent illisibles ?

Les pannes, bien qu'étant assez rares, se produisent quand même de temps en temps .il faut pouvoir, lorsque l'une d'elles arrive, récupérer **une base dans un état « sain ».** Ainsi, après une panne intervenant au milieu d'une modification deux solutions sont possibles :

- ✓ Soit récupérer les données dans l'état dans lequel elles étaient avant la modification ;
- ✓ Soit terminer l'opération interrompue.

9. Assurer les interrogations interactives, la consultation déclarative, et l'accès à de non-informaticiens : les données de la base sont bien gérées et bien organisées. Il ne reste plus qu'à les consulter sans avoir à se préoccuper du stockage ou de l'organisation interne. Le SGBD offre un certain nombre de fonctions pour accéder aux données de façon déclarative, aussi bien pour les programmes d'applications que pour l'usager, **sans avoir à effectuer le moindre développement** informatique particulier.

Malheureusement, ces objectifs ne sont pas toujours atteints !!!

3.3.Composants des SGBD :

Un SGBD va donc posséder un certain nombre de composants logiciels et ce, quelque soit le modèle de données qu'il supporte. On trouve donc des composants chargés de :

1. ***La description des données :*** cette partie sera constituée des outils (en gros des langages) permettant de décrire la vision des données de chaque utilisateur et l'intégration dans une vision globale .On y trouve aussi les outils permettant de décrire le stockage physique des données.
2. ***La récupération des données :*** Cette partie prend en charge l'interrogation et la modification des données et ce, de façon optimisée. Elle est composés de langages de manipulation de données spécifiques et d'extensions de langages « classiques » . Elle gère aussi les problèmes de sécurité.
3. **La sauvegarde et la récupération après pannes :** Cette partie comporte des outils permettant de sauvegarder et de restaurer de façon explicite une base de données. Elle comporte aussi des mécanismes permettant, tant qu'une modification n'est pas finie, de pouvoir revenir à l'état de la base avant le début de cette modification.
4. ***Les accès concurrents aux données :*** C'est la partie chargée du contrôle de la concurrence des accès aux données .Elle doit être telle que chaque utilisateur attende le moins possible ses données tout en étant certain d'obtenir des données cohérentes en cas de mises à jour simultanées de la base.

3.4.Fonctions Principales d'un SGBD : un SGBD doit permettre, De définir la structure de la base ; d'y introduire les données correspondantes, et une fois la base créée, il faudra d'une part la mettre à jour et d'autre part l'exploiter ou l'interroger.

Un SGBD possède donc 3 Fonctions principales : Fonction **Description ;** Fonction **Manipulation et la** Fonction **Utilisation**

1- **Description des données :** la modélisation conduit à :
   - La définition des entités qui vont constituer les données de la base.
   - De préciser leurs caractéristiques
   - Ainsi que les liaisons qui existent entre elles.

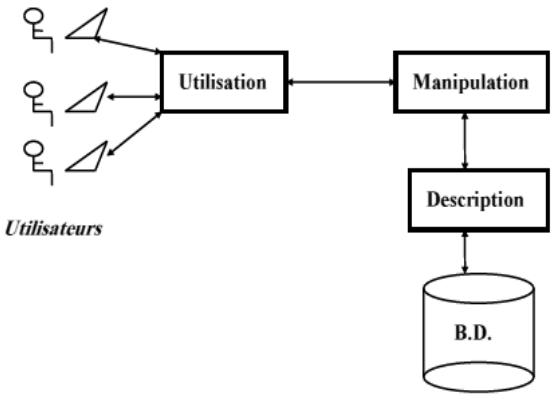
Pour ce faire, le SGBD fournit un langage de description de donnée ou LDD (Data Definition Langage ou DDL en anglais) .

Le but essentiel de ces langages est de fournir une indépendance totale des données vis-à-vis des supports ou elles seront stockées. Le LDD est propre à chaque SGBD et dépend du type de modèle de données supporté par le SGBD.

2- **Fonction manipulation des données :** lorsque la structure de la base est décrite, il faut pouvoir stocker les informations correspondantes. Ceci nécessitera des mécanismes pour construire des enregistrements correctement structurés et qu'il faut ensuite écrire sur un support physique (mémoire secondaire). De plus, il faudra pouvoir **accéder à de tels enregistrements** pour tous les problèmes de mise à jour et d'interrogation.

Pour ce faire, le SGBD fournit un langage de manipulation de données ou **LMD** (Data Manipulation Language en anglais). Nous citons l'exemple de SQL que nous décrivons en détail à la fin de ce chapitre.

3- **Fonction utilisation des données :** A ce niveau, il s'agira d'interroger la base de données, c'est-à-dire rechercher parmi l'ensemble des entités stockées celles qui répondent à des critéres de choix très divers. C'est une fonction qui définit directement le lien entre l'utilisateur et les données au sein d'une **application.**



3.5.Qui intervient sur la BDD ?

Le terme **« utilisateurs »** fait référence à une panoplie d'individus ayant chacun un rôle à jouer dans le processus de mise en place et d'exploitation d'une BD. Parmi les différents types d'utilisateurs d'un SGBD qu'il est important de distinguer, on peut citer :

- **l'administrateur de la base de données :**

La ou les personnes chargées d'établir une description des données constituant la base. Elles sont chargées de décrire les entités de la base de données et indiquer les liaisons existant entre ces entités, ceci au moyen du DDL offert par le SGBD. Le choix de la structure est primordial pour l'avenir de la base de données car une fois fixée et une fois la base créée, il est très difficile pour ne pas dire impossible dans de nombreux SGBD, de modifier cette structure.

Souvent ,on utilise le terme « administrateur de l'entreprise » pour désigner les personnes chargées de la description formelle des données de la base pour souligner l'ouverture vers le monde réel de ce rôle , et on réserve le terme « administrateur de la base » pour désigner les personne chargées de l'aspect plus technique de la création de la base :choix de l'organisation des fichiers, des structures de mémoires secondaires, des méthodes d'accès aux données, etc…

- **l'administrateur d'application :**

Il est chargé de décrire la portion de la base de données concernée par une application particulière. **Dans la pratique chaque application n'est concernée par une portion plus ou moins importante des données de la base**. Cette description sera utilisée par les programmes qui vont constituer l'application en question. Ces programmes ne verront la base de données que par cette description.

L'administrateur d'application utilise le DLL offert par le SGBD pour décrire la portion de la base de données qui concerne une application donnée (appelée **sous schéma ou vue**).

- **le programmeur d'application :**

Chargé d'élaborer les programmes pour exploiter la base de données en fonction de la description qui a été faite par l'administrateur d'application. Le programmeur d'application utilise le **LMD** offert par le SGBD ainsi que d'autre sous programmes conservés généralement dans une librairie (i.e. Bibliothèque de sous-programmes).

- **l'utilisateur final (End User)**

Représente la personne qui se sert simplement de la base de données. Notons deux exemples :

- Dans une agence de réservation de billets d'avion, la personne qui tape sur son terminal quelques commandes pour effectuer une réservation est un utilisateur final.
- De même qu'un chef d'entreprise qui demande de temps en temps à une base de données de son entreprise un certain nombre d'informations reflétant l'état de son entreprise (produits non vendus, commandes en attente, etc,…)
- Le point commun des utilisateurs de ce type est qu'ils ne sont pas informaticiens. C'est donc pour cette catégorie là que **l'administrateur et le programmeur d'application ont conçu et réalisé des programmes** qu'ils n'ont plus qu'à activer au moyen d'un langage de commandes qui devrait être le plus naturel possible.

3.6.Architectures de SGBD

Un programme d'application est écrit à partir des connaissances qu'on a sur la base de données c'est à dire au travers d'un schéma externe (vue).l'application ne voit la B.D qu'à travers un schéma externe. Le SGBD devra interpréter les instructions exprimées en termes de schéma externe, pour les convertir en termes du schéma conceptuel, puis en ordres sur la base de données physique.

3.6.1. Architecture Client –Serveur : Depuis les années 80, les SGBD sont basée sur une architecture clients –serveur

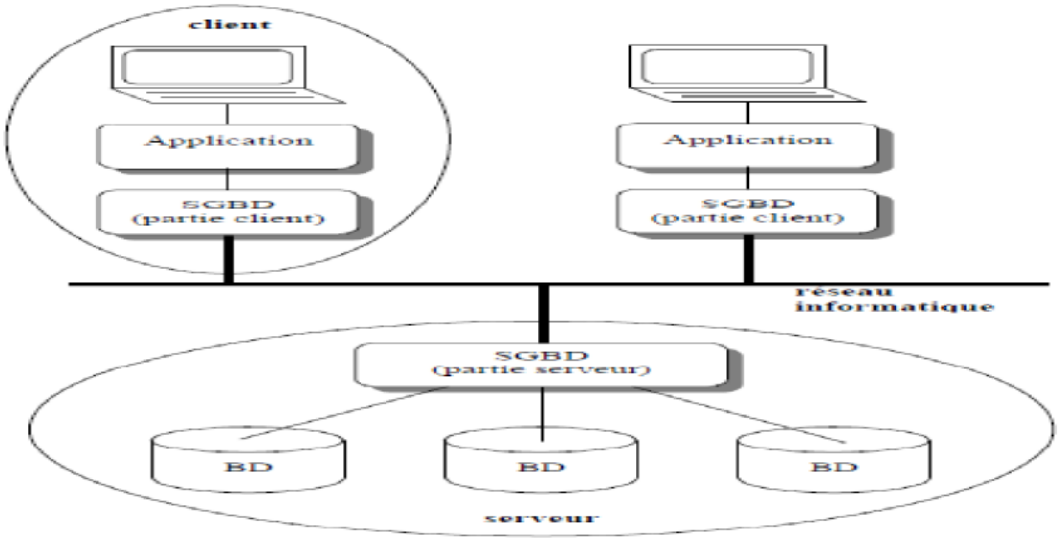


Figure I.1 : architecture Client –Serveur

Serveur : on appelle logiciel serveur un programme qui offre un service sur le réseau .le serveur accepte des requêtes, les traite et renvoie le résultat au demandeur. Le terme serveur s'applique à la machine sur lequel s'exécute le logiciel serveur. (Gere les données partagées et exécute le code du SGBD).

Clients : on appelle logiciel client un programme qui utilise le service offert par un serveur. Le client communiquent avec le serveur envoie une requête et reçoit la réponse. Le client peut être raccordé par une liaison temporaire

Qu'appelle –t-on architecture client / serveur ?

C'est la description du fonctionnement coopératif entre le serveur et le client. Les services internet sont conçus selon cette architecture. Ainsi, chaque application est composée de logiciel serveur et logiciel client. A un logiciel serveur, peut correspondre plusieurs logiciels clients développés dans différents environnements :Unix, Mac, PC…. ; la seule obligation est le respect du protocole entre les deux processus communicants. Ce protocole étant décrit dans un RFC (Request For Comment).

3.6.2. Architecture centralisée :

Ce type d'architecture est appelée solution sur site central (Mainframe).Historiquement, les applications sur site central ont été les premières à proposer un accès multiutilisateurs. Dans ce contexte, les utilisateurs se connectent aux applications exécutées par le serveur central à l'aide des terminaux se comportant en esclaves.

C'est le serveur central qui prend en charge l'intégrité des traitements y compris l'affichage qui est simplement déporté sur des terminaux.

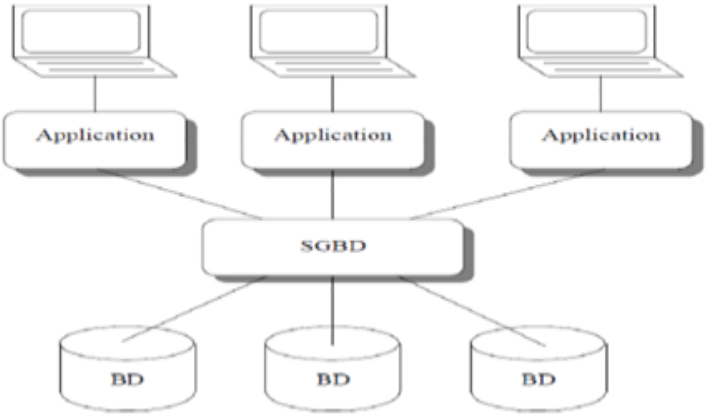


Figure I.2: Architecture centralisé

3.6.3. Architecture trischématique (ANSI / SPARC):

Dans cette architecture on établit quatre niveaux de description du système de base de données qui sont : Le niveau interne, le niveau conceptuel, le niveau externe et le niveau physique.

- ***Niveau externe* :** Vues ; comprend une quantité de vues utilisateurs ; chaque utilisateurs décrit une partie de la base qui convient à ses besoin .Environnement de programmation (intégration avec un langage de programmation) ; Interfaces conviviales et Langages de 4e Génération (L4G) ; Outils d'aides (e.g. conception de schémas) ; Outils de saisie, d'impression d'états.
- ***Niveau conceptuelle ou logique* :** Définition de la structure de données : Langage de Description de Données (LDD) ; Consultation et Mise à Jour des données : Langages de Requêtes (LR) et Langage de Manipulation de Données (LMD) ; Gestion de la confidentialité (sécurité) ; Maintien de l'intégrité ;

Le processus de transformation des requêtes et des résultats qui sortent d'un niveau à un autre s'appelle : **correspondance** ou **mapping .**

- ***Niveau interne ou physiques* :** gestion sur mémoire secondaire (fichiers) des données, du schéma, des index ; Partage de données et gestion de la concurrence d'accès ; Reprise sur pannes (fiabilité) ; Distribution des données et interopérabilité (accès aux réseaux).

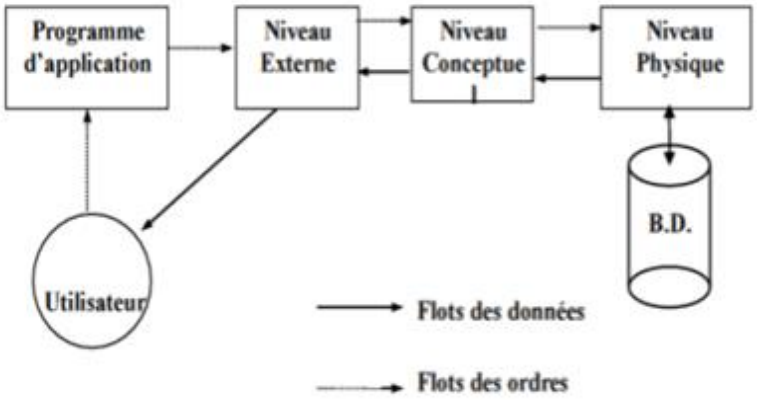


Figure I.3 : Architecture **ANSI / SPARC**

3.7.Historique de l'évolution des SGBD :

Historiquement, plusieurs générations de systèmes se sont succédé. Les premières applications informatiques nécessitant les fonctions d'un SGBD furent les applications de gestion : gestion de stocks, comptabilité, paye,etc….Les deux premières générations de SGBD (réseaux et relationnels) ont donc été conçues à la mesure de ces applications.

- **Les années 70 : Les systèmes de première génération, « réseaux » ou « hiérarchiques »**. Les travaux du DBTG (CODASYL), puis la norme ANSI(1981) ont normalise le modèle de données et les systèmes qui le supportent.

Dans ces systèmes, les données sont modélisées par des structure de type graphe (modèle réseau) ou arbre (modèle hiérarchique)

Les systèmes **IDS II, IDMS et Adabas** font partie des systèmes CODASYL diffusés à ce jour. Avec **IMS** et son modèle dit hiérarchique, **IBM** est le seul acteur important à ne pas avoir respecté cette norme.

La navigation constitue le principal inconvénient de ces systèmes :

- On manipule les données en suivant des pointeurs physiques vers l'information recherchée.
- Les programmes sont donc **dépendants de l'organisation physique** des fichiers sur le disque et les applications doivent donc être profondément modifiées à chaque réorganisation physique.

- **Les années 80 : les systèmes relationnels :**

Le modèle relationnel représente toutes les informations sous forme de tables et offre quelques opérations simples pour manipuler ces tables. La simplicité du modèle en tant qu'interface externe a permis la définition de langages de requêtes simple, faciles d'utilisation et puissants, ainsi que de méthodes de conception d'applications basées sur des méthodologies systématiques. La technologie des SGBD relationnels est parvenue à un degré de standardisation et de maturité tel que les systèmes sont difficilement différentiables tant en fonctionnalités qu'en performances.

Le langage d'interrogation SQL a fait l'objet d'une norme et constitue un standard de fait auquel aucun vendeur ne peut maintenant échapper.

- **Les années 90 : les systèmes orientés – objet :** A partir des années 80 apparaissent de nouvelles application (CAO, PAO, productique, multimédia, génie logiciel, etc.)

nécessitant l'utilisation de bases de données .ces nouvelles applications ont mis en évidence les insuffisances majeures des systèmes relationnels :

- L'inadéquation du modèle relationnel à représenter directement des données complexes, comme : des dossiers médicaux structuré, ou multimédia, des images radiographiques ou des textes annotés,
- Les performances insuffisantes dans la manipulation de données complexes
- La pauvreté graphique et ergonomique des outils d'interface homme-machine.

Les SGBD orienté – objet sont la réponse directe aux problèmes des nouvelles applications. Ils répondent au problème de pauvreté du modèle en proposant un plus riche et extensible. Ils offrent de bonnes performances pour manipuler les données complexes. Ils offrent l'intégration complète des concepts de la programmation par objet et des bases de données. Les vertus de la programmation par objet sont largement reconnues :

- Puissance des concepts.
- Programmation modulaire
- Réutilisation du code (notamment par le biais de boites à outils)
- Et maintenance aisée du code

La productivité du programmeur en est considérablement améliorée.

La première apparition du concept date de 84 avec la proposition de DAVID MAIER et GEORGE COPELAND de construire un SGBD à partir de smalltalk. A partir de ce prototype, Servio Logic construit un produit commercial, **GEMSTONE**, mis sur le marché en 88. Parallèlement, Ontologique, réalise un produit ,**VBASE**, mis sur le marché à peu près au même moment et retiré de la vente un an plus tard pour de nombreuses raisons.

Dans le laboratoire de Hewlett Packard, un projet de prototypage d'un SGBD de type fonctionnel, IRIS, démarré en 83 **évolue** progressivement vers un produit de type **SGBD orienté objet**.

Parallèlement, en Europe, la communauté scientifique s'intéresse aux SGBD permettant de stocker des objets à structure complexe et de nombreux prototypes voient le jour. Deux grands projets de recherche en SGBD orientés-Objet débutent : le projet ORION à Austin, Texas en 85, et le projet Altair, à Rocquencourt, France en 86. Des start-up : Object Design, Versant et objectivity sont créées aux USA en 89, ainsi que O2 Technology en France en 90. Ces compagnies mettent des produits sur le marché fin 90 et début 91.

4. Le modèle Entité/Association (E/A)

Dans un SGBD, les données sont organisées selon un modèle appelé modèle de données. Il existe plusieurs types de modèles. Chacun est basé sur un type de constructeur utilisé pour organiser les données. Parmi les modèles utilisés :

Modèle	Structure
Hiérarchique	Arbres (année 60)
Réseau	Graphe (début des années 70)
Relationnel	Relations (début des années 80)
Orienté objet	Objets

Le modèle de données le plus répandu est le **modèle de données relationnel**, qui utilise un constructeur appelé « relation », au sens mathématique d'ensemble, ou on appelle aussi le modèle Entité/Association (E/A) qui est utilisé à peu près universellement pour la *conception* de bases de données relationnelles principalement.. La conception d'un schéma correct est essentielle pour le développement d'une application viable. Dans la mesure où la base de données est le fondement de tout le système, une erreur pendant sa conception est difficilement récupérable par la suite. Le modèle E/A a pour caractéristiques d'être simple et suffisamment puissant pour représenter des structures relationnelles. Surtout, il repose sur une représentation graphique qui facilite considérablement sa compréhension.

Le modèle E/A souffre également de nombreuses insuffisances : la principale est de ne proposer que des *structures*. Il n'existe pas d'opération permettant de manipuler les données, et pas (ou peu) de moyen d'exprimer des contraintes. Un autre inconvénient du modèle E/A est de mener à certaines ambiguités pour des schémas complexes.

4.1.Modèle conceptuel de données 'Entité-association' (Format Merise)

Il repose sur la perception du monde réel forme d'un ensemble d'objets « entité » associés au moyen d'un ensemble d' « association » entre ces objets.

Voici le schéma décrivant cette base de données *étudiant* (figure 3.1). Sans entrer dans les détails pour l'instant, on distingue ; Une relation qui est représentée par une table à double entrée. Une relation est sous-ensemble du produit cartésien d'une liste de domaines caractérisé par **un nom unique**

Chaque colonne est un **attribut**, encore appelé **champ**. **Un attribut** est caractérisé par un nom.

Chaque ligne est appelée **nuplet** ou **enregistrement**. **Les nuplets** d'une relation sont tous différents

Une relation regroupe une collection d'éléments (lignes) définis par les mêmes attributs (colonnes).

Schéma : descripteur d'une relation : son nom, suivi de la liste des noms des attributs.

Domaine : ensemble des valeurs caractérisé par un nom que peut prendre l'attribut d'une relation.

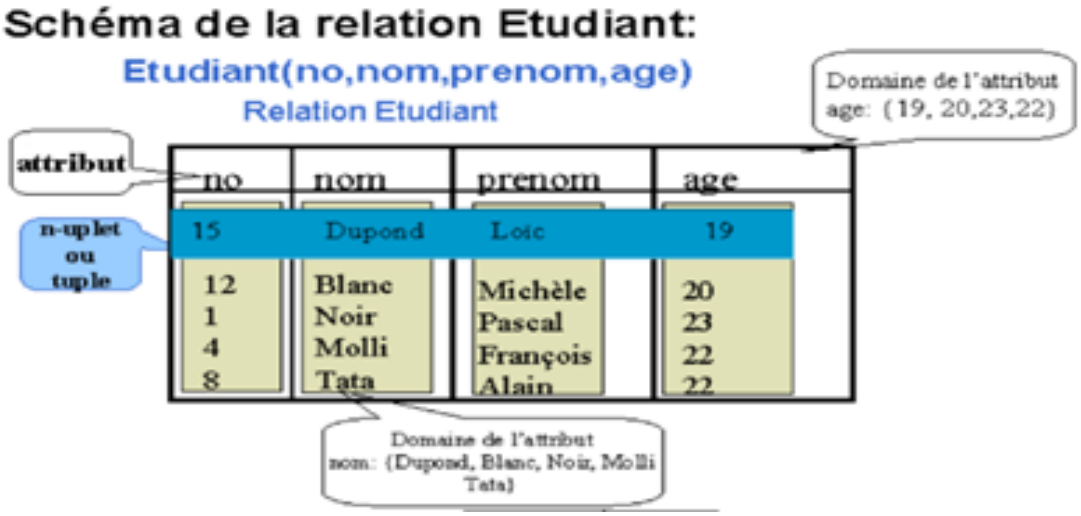


Figure I.4 : modèle réel

Il s'agit d'une description :

- ***Statique :*** les entités et les associations sont décrites par leurs propriétés (attribut)
- ***Dynamique :*** *les associations traduisent les règles de gestion entre les entités* identifiées.

Exemple :

Un **Coureur** fait partie d'une **Equipe**

Numéro	Code
Nom	Nom
Nationalité	Directeur Sportif

4.2.Modèle entité –association –Représentation graphique :

4.2.1. **Entité :** chaque entité est décrite par des propriétés (ou attributs). Chaque occurrence de l'entité est définie par les valeurs de ses différents attributs.

Exemple : dans cette table de Coureur ; l'entité Coureur à 3attributs.

Le coureur (Ismail, Boukli, N°8) est une occurrence de l'entité coureur

Numéro	Prénom	NOM
8	Ismail	BOUKLI
31	Lotfi	Hamza-cherif
61	Morad	Kholkhal

4.2.2. **Association :** Met en relation plusieurs entités. Une association n'existe que par les entités qu'elle met en correspondance .Elle peut être caractérisée par des attributs qui dépendent des occurrences que l'association met en relation. Une association est aussi appelée 'relation'

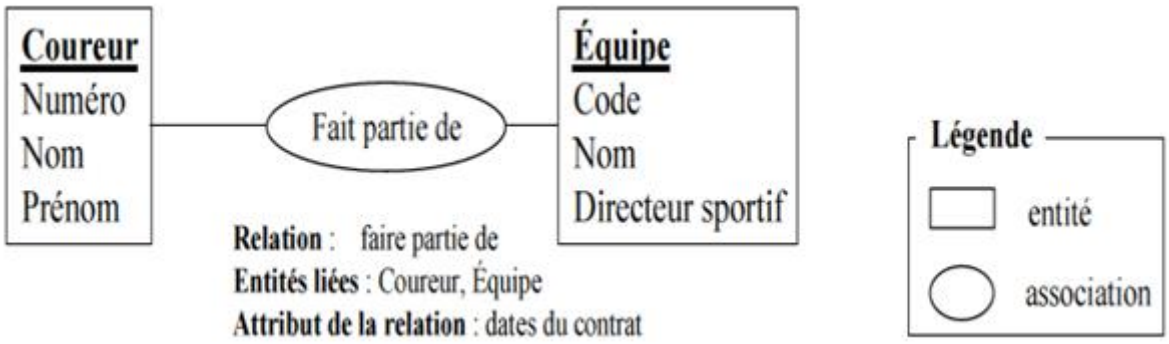


Figure I.5 : Diagramme entité –association

4.2.3. **Cardinalité :** Pour une entité A en relation avec une entité B, il s'agit du nombre d'occurrences d'associations que possède une occurrence de l'entité A avec l'entité B

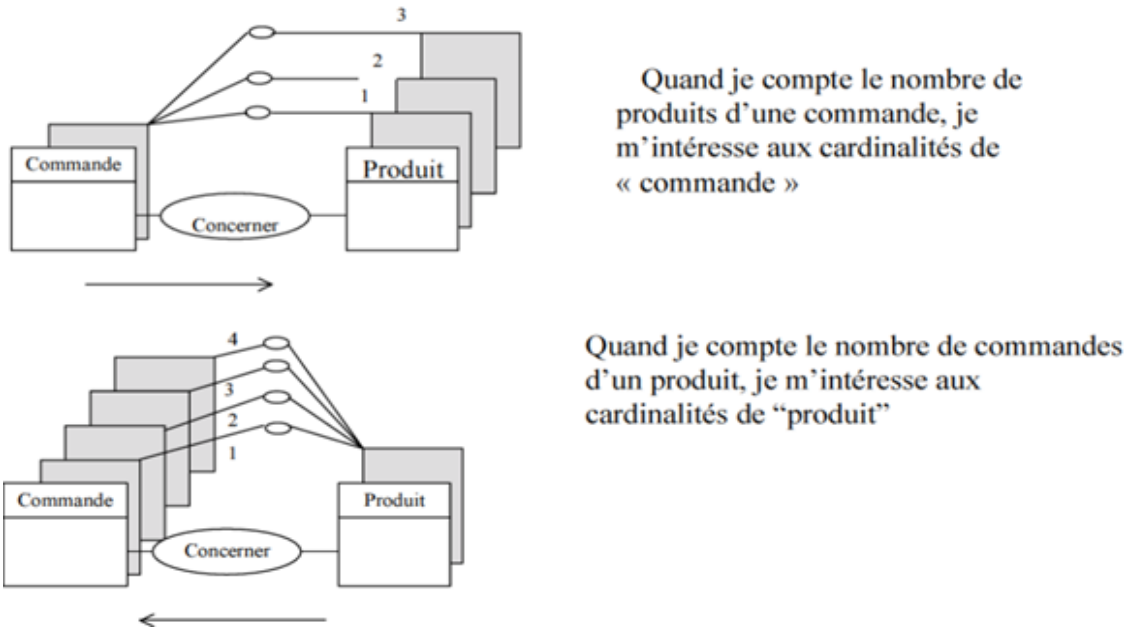
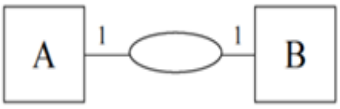
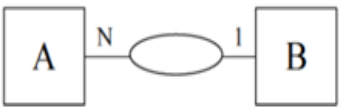


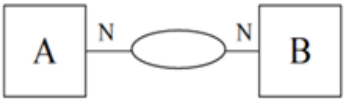
Figure I.6 : cardinalité d'une association

1- Association un-un (1,1) entre une entité A et une entité B : Une occurrence de l'entité A ne peut être liée qu'à une occurrence de l'entité B et réciproquement.



2- Association un-plusieurs (1,N) entre une entité A et une entité B :
   - Une occurrence de l'entité B ne peut être associée à plusieurs occurrences de l'entité A.
   - Une occurrence de l'entité A ne peut être associée qu'à une occurrence de l'entité B .





3- Association Plusieurs-Plusieurs (N,N) entre une entité A et une entité B : Une occurrence de l'entité A peut être liée à plusieurs occurrences de l'entité B et réciproquement

Exemple :

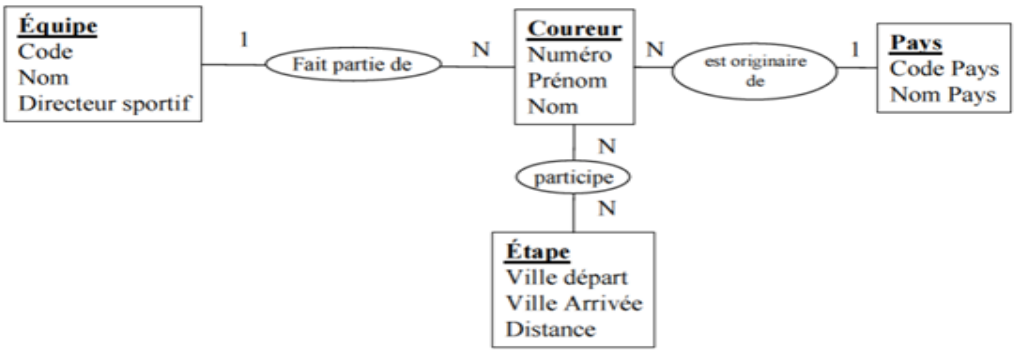


Figure I.7 : Diagramme entité association

Un **coureur** Participe à plusieurs **Etapes** ……..Une **Etape** fait participer plusieurs **Coureurs**

Un **Coureur** appartient à une **Equipe**……Une **Equipe** est composée de plusieurs **Coureurs**

Un **coureur** est Origine d'un **Pays** ……Un **Pays** est représenté par plusieurs **Coureurs.**

- **Cardinalité minimale :** Nombre de fois minimum qu'une occurrence d'entité participe à une Relation.

Exemple : la commande peut-elle ne concerner **aucun** produit ?

OUI : cardinalité minimale =0

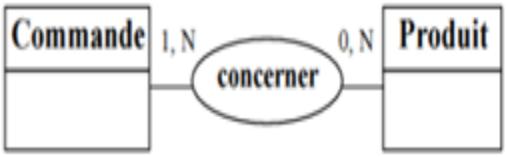
NON : Cardinalité minimale =1

- **Cardinalité maximale :** Nombre de fois maximum qu'une occurrence d'entité participe à une Relation.

Exemple : la commande concerne-t-elle **un seul** produit **au maximum** ?

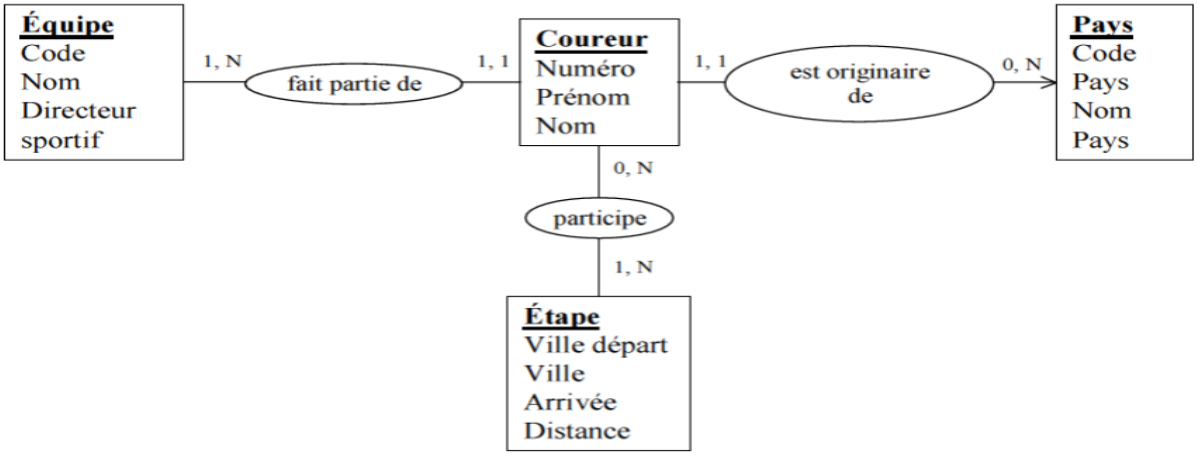
OUI : cardinalité maximale =1

NON : Cardinalité maximale =N

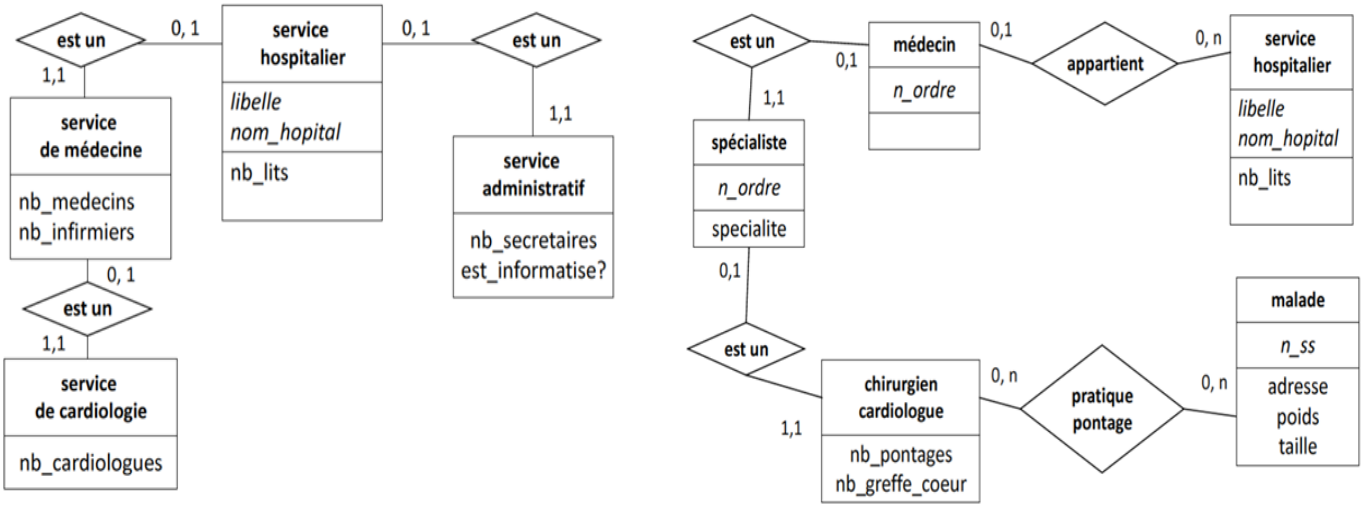


Quand une cardinalité maximale pour une entité =1, on représente une flèche partant de l'entité, et on parle d'une dépendance fonctionnelle (DF) : Commande dépend du client, Chaque commande est associée à un client. Si on supprime un client, ses commandes n'ont plus besoin d'être mémorisées, mais on peut annuler les commandes et conserver le client.

Exemple : diagramme entité-association avec des cardinalités max et min



Exemple 2 : représentations des cardinalités pour un service hospitalier



4.2.4. Identifiant (clé) d'une entité :

Chaque entité ou association possède une clé qui permet d'identifier de façon unique chacune de ses occurrences. L'existence de cette clé garantit l'accès à n'importe quelle occurrence de l'entité. La clé (dite primaire) est définit par un ou plusieurs attributs.

Exemple : soit l'entité Coureur (numéro, nom, prénom)

Aucun coureur n'a le même numéro. Par contre, on pourrait avoir deux coureurs ayant le même nom.

- L'attribut numéro est retenu comme clé primaire de l'entité Coureur

Dans la plus part des cas, un attribut ou un groupe d'attributs de l'entité pourront être utilisés comme clé. Dans le cas contraire, il est toujours possible de créer un nouvel attribut (code séquentiel par exemple) qui sera utilisé comme clé. Les clés primaires sont utilisées pour les associations entre des occurrences de deux entités.

4.3.Concevoir un bon modèle conceptuel de donnée

1- Sélection de l'identifiant (clé primaire) de chaque entité :

- Attributs avec une valeur nulle ne peuvent être candidats.
- Le nombre d'attributs entrant dans la composition de la clé doit être minimal. En effet, plus le nombre d'attributs de la clé est grand, plus les opérations de recherche d'information dans la base de données seront complexes.
- Si pas de bon candidat, on peut toujours créer un attribut code

2- **Analyse des redondances :** un attribut dont la valeur peut etre déduite à partir d'autre données :

- Calcul à partir d'autre attributs de la même occurrence : on prend l'exemple suivant ; **lignecommande** (N°Commande, Article , Prix Unitaire, Nombre, Prix total)

  Le prix total peut facilement calculer par le Prix unitaire *Nombre
- Agrégation d'un attribut d'une autre entité associée :

  Exemple : **Commande** (N° ,Client , Montant,nombre d'articles)

  lignecommande (N°Commande, Article , Prix Unitaire, Nombre, Prix total)

  Le montant de la commande peut être calculé en additionnant les valeurs de prix total de ligne de la commande
- Comptage d'occurrences d'une entité associée ; nous prenons le même exemple ; le nombre d'articles peut être calculé en comptant le nombre de ligne de la commande
- Relations pouvant être déduite d'une autre relation

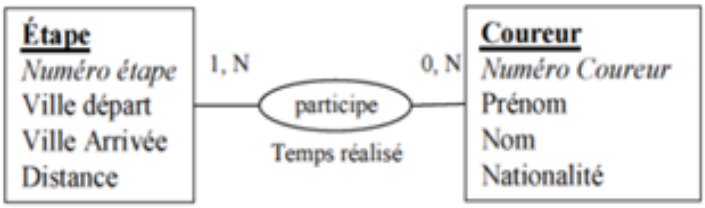
4.3.1. Traduction du modèle conceptuel au modèle relationnel

1. Relation plusieurs –Plusieurs

- Pour chaque entité, une relation (table) ayant les mêmes attributs et la même clé primaire.
- Pour la relation, une relation (table) ayant pour attributs les éventuels attributs de l'association ainsi que les attributs identifiant des deux entités de l'association. L'ensemble de ces deux attributs identifiant constituent la clé primaire de la table.

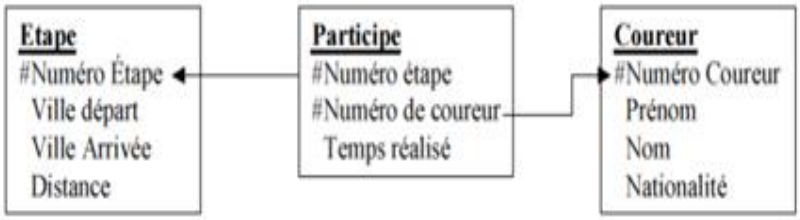
Exemple :

Modèle conceptuel :



Modèle logique relationnel

: Attribut faisant partie de la clé primaire



Schémas relationnels de la base de donnés :

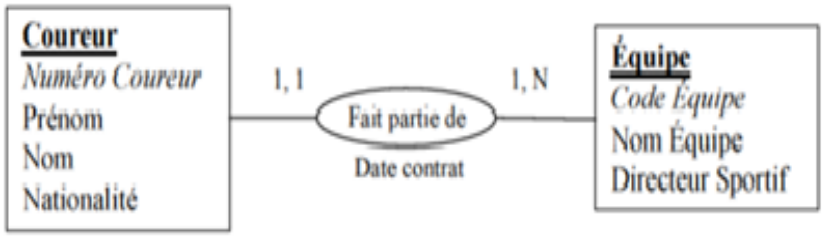
Etape (**NuméroÉtape** , Ville départ, Ville arrivée, Distance)
Coureur (**NuméroCoureur** ,Prénom,Nom)
Participe (**NuméroCoureur , NuméroÉtape** ,TempsRéalisé) ;

2. *Relation Un –Plusieurs*

- Pour chaque entité, une relation (table) ayant les mêmes attributs et la même clé primaire.
- La clé primaire de l'entité dépendante est ajoutée aux attributs de l'entité dont elle dépend (clé étrangère)
- Les attributs de l'association sont aussi ajoutés comme attributs de l'entité dépendante.

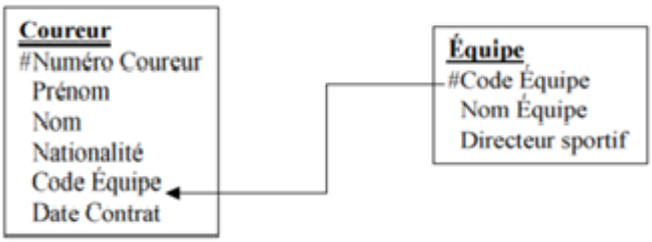
Exemple :

Modèle conceptuel :



Modèle logique relationnel

: Attribut faisant partie de la clé primaire



Schémas relationnels de la base de donnés :

Coureur (**Numéro Coureur**, Prénom, Nom, Nationalité, Code Equipe, Date Contrat)
Equipe (**Code Equipe,** Nom Equipe, Directeur Sportif) ;

3. *Relation Un –Un (Association Binaire)*

- Pour chaque entité, une relation (table) ayant les mêmes attributs et la même clé primaire.
- Une des deux relations doit inclure les attributs de la clé primaire de l'autre (clé étrangère)

Une alternative est de regrouper les deux entités en une seule relation, regroupant tous les attributs des deux entités, et ayant pour clé primaire la clé primaire de l'une des entités de la relation. Cette solution

n'est a priori pas souhaitable dans la mesure où elle ne reflète pas la volonté exprimée au niveau conceptuel de voir apparaitre les deux entités de façon distincte

Exemple :

Modèle conceptuel :

Modèle logique relationnel

: Attribut faisant partie de la clé primaire

Schémas relationnels de la base de donnés :

Employé (Identifiant, Prénom, Nom, salaire)
Département (Nom département, Téléphone, Identifiant directeur) ;

4.3.2. Normalisation du modèle relationnel : Nous prenons l'exemple suivant qui présente la table de stock produit qui définit par les champs suivant :

Stock_produit (code_Produit , Nom_Produit, Poids_Unitaire, quantité, N°Dépôt, Adresse_Dépot, Volume_Stock) .

Code Produit	NomProduit	PoidsUnitaire	Quantité	NuméroDépot	AdresseDépot	VolumeStock
P1	Scie	25	34	1	Tunis	23
P1	Scie	25	2	2	Monastir	45
P2	Marteau	53	433	3	Sfax	654
...	...	...	...	...	...	...

Une telle relation présente différent problèmes :

- ✓ ***Redondance :*** répétition d'information comme le nom du produit associé à un code produit [perte d'espace disque ; difficulté de mise à jour, avec risque d'introduire des inconsistances dans la base de données] .
- ✓ ***Risques de perte d'information :*** si l'on supprime l'information sur le produit P2, on supprime aussi l'information sur le Dépôt 3
- ✓ **Inaptitude à la gestion de l'information :** il n'est pas possible d'ajouter un produit sans ajouter les informations sur un des dépôts qui le stocke.

5. EXEMPLES DE CLASSIFICATION des SGBDM :

Il existe de multiples nomenclatures et classifications, certaines d'usage universel et international tandis que d'autres sont limitées à une spécialité voire à un service ; chacune répondant (plus ou moins bien) à un besoin particulier ; nous nous limiterons donc aux plus représentatives, tel que par exemple la plus connu **PUBMED**, qui est un moteur de recherche bibliographique gratuit en biologie et médecine scientifique. Cette interface donnant accès à la base de données MEDLINE, ou vous pouvez trouver plus de 19 millions de citations, résumés d'article scientifiques et même des textes complets depuis 1950 dans 5000 revue biomédicales

CIM ET DERIVEES

La Classification Internationale des Maladies (CIM ou ICD en anglais) de l'Organisation Mondiale de la Santé (OMS ou WHO) a été originellement conçue pour coder les causes de décès dans une optique épidémiologique. Elle est maintenant également utilisée pour l'évaluation des soins médicaux et l'indexation des dossiers. Il s'agit d'une classification monoaxiale avec 21 chapitres principaux dont 17 concernent des maladies et quatre concernent les signes et résultats anormaux, les causes de traumatismes, d'empoisonnement ou de morbidité, l'état de santé et les facteurs de recours aux soins. Les catégories de maladies sont définies en fonction d'un caractère commun qui peut être l'étiologie (1 = Maladies infectieuses, lettres A et B), la topographie (9 = maladies de l'appareil circulatoire, lettre I), la physiologie (15 =Grossesse et accouchement, lettre O) ou la pathologie (II = Tumeurs). La classification aboutit par subdivisions successives à un code à 3 caractères (une lettre correspondant au chapitre puis 2 chiffres) pour les maladies définies à un niveau général, décliné par l'ajout d'un quatrième chiffre (derrière un point) pour désigner les diagnostics précis et les formes cliniques ; le sous-code 9 désignant l'absence de précision (SAI = sans autre indication) et le sous-code 8 les autres formes non précédemment définies. Dans certains cas, un cinquième chiffre a été rajouté afin d'améliorer la finesse de description. La CIM-10 a introduit la notion de troubles iatrogènes. Elle compte au total 80.000 termes.Les tumeurs sont extraites de leur chapitre et regroupées dans un chapitre spécial. Parfois cependant, une même maladie peut apparaître en deux

places distinctes (avec deux codes). C'est le cas lorsqu'une maladie appartient à un processus pathologique initial général (code associé à une dague), par exemple la tuberculose, et correspond à des manifestations localisées à un appareil (code associé à un astérisque), par exemple une tuberculose rachidienne. D'autre part, le principe de différenciation n'est pas constant.

SNOMED : (Systematized Nomenclature of Medicine) combine une nomenclature de plus de 50.000 termes et une classification multiaxiale comportant à l'origine 7 axes : topographie, morphologie, étiologie, altération fonctionnelle, nosologie, actes médicaux. La 3ème édition compte désormais 200.000 termes et 11 axes. Chaque axe est défini par une lettre (par exemple, T pour topographie, E pour étiologie) et organisé de façon hiérarchique, chaque élément étant associé à un code numérique à 4 ou 5 chiffres. Ainsi un diagnostic est traduit par plus d'un élément signifiant, mais chaque axe ne doit pas être obligatoirement validé. Par exemple, la juxtaposition : "T2856 (lobe supérieur du poumon gauche) / M4100 (inflammation) / F0300 (fièvre) / E2012 (pneumocoque)" correspond à la phrase "Pneumonie fébrile à pneumocoque du lobe supérieur gauche". L'ajout de connecteurs concernant notamment les liens de causalité permet de décrire un fait complexe en plusieurs phrases. SNOMED est largement utilisé car précis, cependant ce modèle pose encore des problèmes : les termes des différents axes ne sont pas complètement indépendants entre eux, l'axe Maladie fait souvent double emploi, certains concepts peuvent apparaître dans plusieurs axes.

MESH : (Medical Subject Headings) sert à indexer, cataloguer et retrouver des références de bibliographie dans le domaine de la Santé. Il a été conçu à la National Library of Medicine (NLM) aux Etats-Unis comme support de l'Index Medicus, répertoire des principales publications scientifiques, et est utilisé par les systèmes de recherche bibliographique Medlars et Medline. MeSH est organisé en deux parties : une liste alphabétique de termes (lexique) et une structure multiaxiale. Les 200.000 termes du lexique sont distribués selon 19 axes, allant de l'anatomie, maladie, psychiatrie et à la géographie. Les termes équivalents sont rapportés à celui des 20.000 termes principaux

(descripteurs) qui exprime le mieux le concept, termes auxquels sont associés un code alphanumérique. Les descripteurs s'organisent selon une structure hiérarchique. En outre, des connecteurs permettant des références explicites entre termes expriment les relations de synonymie, de voisinage ou d'association tandis que des qualificatifs permettent de considérer les différentes facettes d'un concept (par exemple : tuberculose/traitement). Ce système qui indexe actuellement plusieurs centaines de milliers de références est mis à jour régulièrement pour suivre l'évolution des connaissances.

Figure I.8 :Interface de SGBDM « MESH »

6. SQL (Structured Query Language)

Introduit par IBM, évolution du langage SEQUEL, commercialisé tout d'abord par ORACLE. SQL est devenu le langage standard pour décrire et manipuler les Base de Données Relationnelle. SQL est un langage *déclaratif* qui permet d'interroger une base de données sans se soucier de la représentation interne (physique) des données, de leur localisation, des chemins d'accès ou des algorithmes nécessaires. A ce titre il s'adresse à une large communauté d'utilisateurs potentiels (pas seulement des informaticiens) et constitue un des atouts les plus spectaculaires (et le plus connu) des SGBDR.

6.1.SQL a différentes fonctions:

- **Langage de définition et de validation de données:** pour créer, modifier et supprimer des tables dans une base de données, ou encore pour définir des valeurs par défaut pour certaines zones et règles de contrôle pour l'encodage,
- **Langage de manipulation de données:** pour sélectionner, modifier, insérer, combiner, trier ou supprimer des données dans les tables d'une base de données ou encore pour lier des tables entre elles via des zones clés,
- **Langage de contrôle d'accès aux données:** pour définir les permissions accordées aux différents utilisateurs de la base de données.

6.2.Les commandes en SQL :

Catégorie	Commandes SQL	
Description des données(LDD)	**CREATE**	Création de tables
	ALTER	Modification de tables
	DROP	Suppression de tables
Ex : CREATE TABLE table (colonne 1 INTEGER,colonne 2 INTEGER,colonne3 DATE)		
Manipulation des données (LMD)	**INSERT**	Insertion de lignes dans une table
	UPDATE	Mise à jour de lignes dans une table
	DELETE	Suppression de lignes dans une table
Ex: SELECT name ,service ;**FROM** employees, **WHERE** statut =’stragiaire’;**ORDER BY** name;		
Contrôle des données (LCD)	**GRANT**	Attribution de droits d'accès
	REVOKE	Suppression de droits d'accès
	COMMIT	Prise en compte des mises à jour
	ROLLBACK	Suppression des mises à jour
Interrogation des données	**SELECT**	Interrogations diverses

6.3.Les contraintes d’intégrité :

Une contrainte d'intégrité est une clause permettant de contraindre la modification de tables, faite par l'intermédiaire de requêtes d'utilisateurs, afin que les données saisies dans la base soient conformes aux données attendues.

Ces contraintes doivent être exprimées dès la création de la table grâce aux mots clés suivants :

PRIMARY KEY ; FOREIGN KEY ; REFERENCES ; DEFAULT ; NOT NULL ,UNIQUE ; CHECK

6.4. Types de donnée :

Type de donnée	Syntaxe	Description
Type alphanumérique	CHAR(n)	Chaîne de caractères de longueur fixe n (n<16383)
Type alphanumérique	VARCHAR(n)	Chaîne de caractères de n caractères maximum (n<16383)
Type alphanumérique	TEXT	chaînes de caractères de longueur variable
Type numérique	DECIMAL(n)	Nombre de n chiffres
Type numérique	SMALLINT	Type numérique Entier signé de 16 bits (-32768 à 32757)
Type numérique	INTEGER	Entier signé de 32 bits (-2E31 à 2E31-1)
Type numérique	FLOAT	Nombre à virgule flottante
Type horaire	DATE	Date sous la forme 16/07/99
Type horaire	TIME	Heure sous la forme 12:54:24

6.5. Syntaxes pour la description des données en SQL

Création d'une table

```
CREATE TABLE `Table1`
(`NumTable1` INT PRIMARY KEY,
`colonne2` TEXT(25),
`colonne3` DATE,
`colonne4` DOUBLE,
`NumTable2` INT REFERENCES Table2
);
```

Suppression d'une table : DROP TABLE Nom_de_la_table

Suppression des données d'une table : TRUNCATE TABLE Nom_de_la_table

Suppression de colonnes : ALTER TABLE Nom_de_la_table

DROP COLUMN Nom_de_la_colonne

Ajout une colonne : ALTER TABLE Nom_de_la_table

ADD Nom_de_la_colonne Type_de_donnees

Modification d'une colonne : ALTER TABLE Nom_de_la_table

CHANGE Nom_de_la_colonne TO nouveau nom

colonne Type_de_donnees

Modification du type de données d'une colonne

ALTER TABLE Nom_de_la_table

MODIFY Nom_de_la_colonne Type_de_donnees

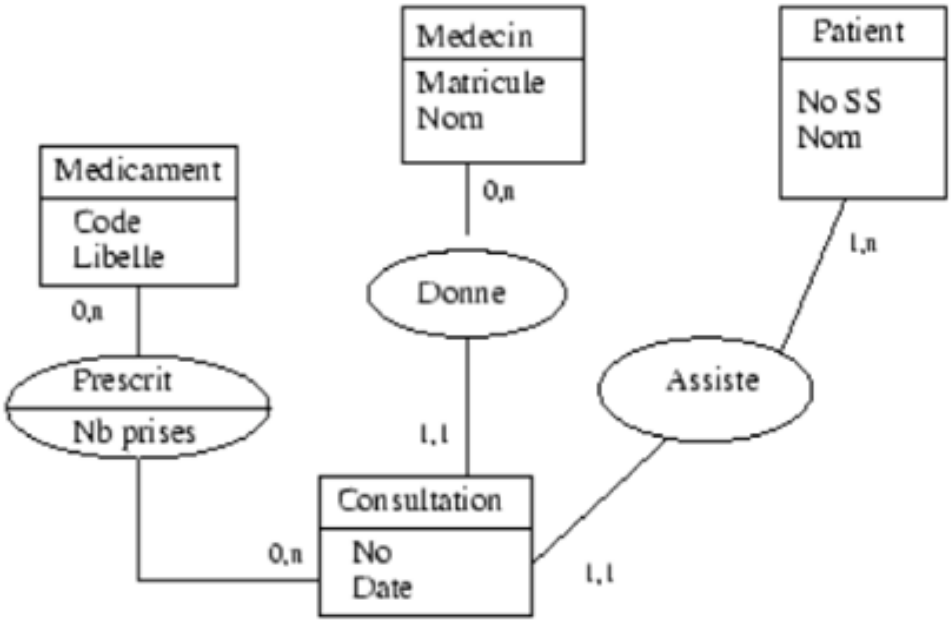
Changement du nom d'une table : RENAME TABLE Ancien_Nom TO Nouveau_Nom

7. Conclusion :

Dans le secteur de la santé en générale, et avec le développement technologique outils informatiques pour le traitement d'une grande masse d'information médicales. Il est important de savoir l'utilisation et la conception de systèmes de gestion de base de données (SGBD) pour gérer le système d'information hospitalier qu'on va l'entamer dans le chapitre 2 ; d'où le besoin de ces bases de données assurent une gestion de données médicales exactes, complètes et disponibles à tout moment, depuis n'importe où (accessible à un grand nombre d'utilisateurs) et dans la forme voulue sachant que les applications concernées par l'utilisation d'un SGBDM possèdent des caractéristiques différentes tant au niveau de volume du données (image médicale de différentes modalité 3D) concernées qu'un niveau de la complexité de ces données et des traitements informatique à réaliser.

SERIE TD N°1 : SGBDM & SQL

Exercice 1 : On vous donne le schéma Entité /Association suivant représentant des visites dans un centre médical. Répondez aux questions suivantes en fonction des caractéristiques de ce schéma (i.e : indiquez si la situation décrite est représentable, indépendamment de sa vraisemblance)



I. Cardinalité

1. Un patient peut –il effectuer plusieurs visites ?
2. Un médecin peut-il recevoir plusieurs patients dans la même consultation ?
3. peut-on prescrire plusieurs médicaments dans la même consultation ?
4. deux médecins différents peuvent-ils prescrire le même médicament

II. Clé primaire et étrangère

Indiquez précisément : la clé primaire, les clés étrangères et les contraintes éventuelles

Exercice 2 : Soit le schéma relationnel (gestion d'un hôpital) :

Patient (Num-Patient, Prenom-Patient, âge, sexe, Num-Mutuelle)
Mutuelle (Num-Mutuelle, Nom-Mutuelle)
Médecin (Num-Médecin, Nom-Médecin, Spécialité-Médecin, grade-Médecin, Salaire- Médecin)
Maladie (Num-Maladie, Nom- Maladie)
Hospitaliser (Num-Patient, Num-Maladie, Num-Médecin, Date-Entrée, Chambre, Durée-Hospitalisation)

1. Créez les cinq tables avec les contraintes d'intégrités relatives à chaque table (Patient, Mutuelle, Médecin, Affection et Hospitaliser)

Cet hôpital a accueilli 10 patients et 15 hospitalisations depuis le début de l'année 2013; Il comporte 10 chambres ; Il traite 5 types de maladies ; Certain patients sont toujours hospitalisés ; 10 médecins de spécialités différentes travaillent dans cet hôpital, leur salaire dépend de leur grade (L'ordre croissant de ce grade est : Docteur, résident, Maitre-Assistant puis Professeur) et il existe uniquement deux type de mutuelle : la CNAS et la CASNOS (codés avec 3 chiffres). Le premier chiffre de gauche indique le type de mutuelle. Le 1 est réservé pour la CNAS et le 2 pour CASNOS).

Table patient				
Num-patient	Prenom patient	Age	sex	Num-Mutuelle
26	fouad	80	M	2256
25	hanane	36	F	1426
24	Salim	80	M	2346
23	marwan	80	M	2244
22	Hafida	36	F	1588

Table Mutuelle	
Num-Mutuelle	Nom-Mutuelle
2346	CASNOS
2244	CASNOS
1588	CNAS
2256	CASNOS
1426	CNAS

Table Médecin				
Num-M	NOM_M	Spécialité_M	Grade_M	Salaire_M
12	Brixi	dermatologue	résident	60000
11	Boukli	psychologue	Professeur	97651
10	Azouni	ophtalmologue	Maitre -assistant	70860
9	Charaf	Med interne	Généraliste	45000
8	slimani	Radiologue	Professeur	97651

Table Maladie	
Num-Maladie	Nom-Maladie
1	Diabete
2	Cancer de sein
3	Hyper tension
4	Grippe
5	Anémie

Table hospitalisation					
Num-patient	Num-Maladie	Num-Medecin	Date –entrée	Num chamber	Durée-hospitalisation
6	2	7	12.02.2000	21	Null
3	9	1	22.01.2002	24	15
8	8	5	11.03.2004	25	12
11	15	10	14.01.2011	12	6

2. Ecrire en SQL les différentes tables données ?
3. Dr « Ghambaza » est un résident en cardiologie (n°18), Dr « Ghambaza » est un autre résident en radiologie (n°19). Ajoutez ces informations à votre BDD.
4. Le médecin qui porte le numéro « 01 » vient de sortir en retraite. Supprimez-le de votre BDD.
5. Lors de la vérification des informations personnelles, le médecin qui porte le numéro « 02 » a trouvé qu'il y a une erreur sur son grade, il est en réalité maitre-assistant. Corrigez cette erreur.
6. Les résidents ont eu une promotion de 10%. Mettez à jour votre BDD.
7. Afficher les prénoms des patients encore hospitalisés.
8. Afficher le numéro, le nom et le salaire des médecins dont le salaire dépasse 60 000 DA.
9. Afficher les noms et le salaire des médecins dont le salaire est entre 30 000 DA et 60 000 DA.
10. Afficher les numéros et les noms des médecins qui le grade "Maitre-Assistant" ou "professeur".
11. Afficher les prénoms des patients qui commencent par un "a" ou/et se termine par un "a".
12. Afficher les numéros des patients qui ont été hospitalisé la première quinzaine de février 2011.
13. Afficher le nombre de patient traités par chaque médecin
14. Afficher le numéro des patients hospitalisé en 2011.
15. Afficher le prénom des patients, le nom de maladie et la spécialité du médecin traitant des patients âgés de moins 14 ans

Solution série TDN°1

Exercice 1:

I. Cardinalité

1. oui, cardinalité maximale N de l'association patient-Consultation
2. Non : Cardinalité maximale 1 de l'association Consultation-Patient (un patient par consultation).
3. oui, cardinalité maximale N de l'association Consultation-Médicament
4. oui, pas d'association entre médecin et un médicament

II. Clé primaire et étrangère

Médicament (**Code**,Libellé)

Consultation (**ID-Consultation**,Matricule,NO-SS,Date)

Matricule et NO-SS sont les clés étrangeres .

Prescription (**Code-médicament**,**ID-consultation**,Nb-prises)

Médecin (**Matricule**,Nom)

Patient (**NO-SS**,Nom)

Les attributs entrant dans la composition de la clé primaire sont indiqués en caractères gras et soulignés.

Exercice 2 :

1) Voilà les syntaxes de la création des tables :

Pour créer la base et le nom de la base

```
CREATE DATABASE `gesion_hopital`
CREATE TABLE `Patient`
(`Num-patient` INT PRIMARY KEY,
`Prenom-patient` TEXT(25),
`Age` INT,
`sexe` TEXT(10),
`Num-Mutuelle` INT REFERENCES `Mutuelle`
);
```

1ér table de patient

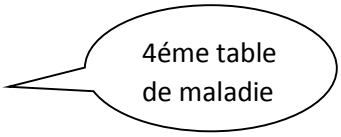
```
CREATE TABLE `Mutuelle`
(`Num-mutuelle ` INT PRIMARY KEY,
`Nom-Mutuelle ` TEXT(25)
);
```

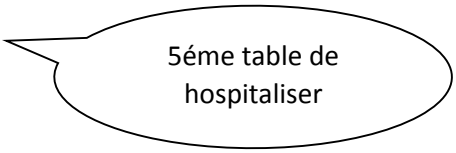
2éme table de mutuelle

```
CREATE TABLE `Medecin`
(`Num-medecin` INT PRIMARY KEY,
`Nom-Medecin` TEXT(25),
```

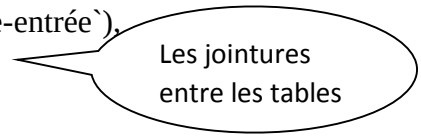
3éme table de médecin

```
        `specialité-Medecin`    TEXT(20),
        `Grad-Medecin`          TEXT(20),
        `salaire-Medecin`       int
        );
CREATE  TABLE                   `Maladie`
        (`Num-Maladie`          INT PRIMARY KEY,
        `Nom-Maladie`           TEXT(25)
        );
CREATE  TABLE                   `Hospitaliser`
        (`Num-patient`          INT,
        `Num-Maladie`           INT,
        `Num-Medecin`           INT,
        `Date-entrée`           DATE,
        `Chambre`               INT,
        `Durée-hospitalisation` INT,
```






```
PRIMARY KEY (`Num-patient`,`Num-Maladie`,`Num-Medecin`,`Date-entrée`),
FOREIGN KEY (`Num-patient`) REFERENCES `Patient`,
FOREIGN KEY (`Num-Maladie`) REFERENCES `Maladie`,
FOREIGN KEY (`Num-Medecin`) REFERENCES `Medecin`);
```



2) Dans cette partie on va remplir les 5 tables précédant :

- **La table de patient :**

```
INSERT      INTO    `patient`
            Values  (26,"fouad",80,"masculin",2256) ;
            Values  (25,"hanane",36,"féminin",1426) ;
            Values  (24,"salim",80,"masculin",2346) ;
            Values  (23,"marwan",80,"masculin",2244) ;
            Values  (22,"hafida",36,"féminin",1588) ;
```

- **La table de la mutuelle :**

```
Insert      into    `mutuelle`
            Values  (2256,"casnos");
            values  (1426,"cnas");
            Values  (2346,"casnos");
            values  (2244,"casnos");
```

```
        values      (1588,"cnas");
```

- **La table de médecin**

```
INSERT      INTO      `medecin`
        Values      (7,"Slimani","radiologue","professeur",97651) ;
        Values      (9,"charaf","med-interne","maitre-assistant",97651) ;
        Values      (10,"azouni","ophtalmologue", "maitre-assistant",70860) ;
        Values      (11,"Boukli","psychologue","professeur",97651) ;
        Values      (12,"Brixi","dermatologue","résident",60000) ;
```

- **La table de la maladie :**

```
INSERT      INTO      `maladie`
        Values      (1,"diabéte") ;
        Values      (2,"cancer de sein") ;
        Values      (3,"hyper tension") ;
        Values      (4,"grippe") ;
        Values      (5,"anémie ") ;
```

- **La table d'hospitaliser :**

```
INSERT      INTO      `hospitaliser`
        Values      (6,2,7,"12.02.2000",21,null) ;
        values      (3,9,1,"22.01.2002",24,15) ;
        values      (8,8,5," 11.03.2004",25,12) ;
        values      (11,15,10,"14.01.2011 ",12,6) ;
```

3) Dr « Ghambaza » est un résident en cardiologie (n°18), Dr « Ghambaza » est un autre résident en radiologie (n°19). Ajoutez ces informations à votre BDD.

```
Insert      into      `medecin`
        values      (18,"Ghambaza","cardiologie","resident",null);
insert      into      `medecin`
        values      (19,"Ghambaza","radiologie","resident",null);
```

4) Le médecin qui porte le numéro « 01 » vient de sortir en retraite. Supprimez-le de votre BDD.

```
Delete      from      `medecin`  Where      `Num-medecin`=01
```

5) Lors de la vérification des informations personnelles, le médecin qui porte le numéro « 02 » a trouvé qu'il y a une erreur sur son grade, il est en réalité maitre-assistant. Corrigez cette erreur.

```
Update `medecin`  Set  `Grad-medecin`="maitre assistant"  Where  `Num-medecin`=2
```

6) Les résidents ont eu une promotion de 10%. Mettez à jour votre BDD.

```
Update  `medecin` Set  `Salaire_medecin`=`Salaire_medecin`+ (0.1*`Salaire_medecin`)
Where  `Grade_medecin`="resident"
```

7) Afficher les prénoms des patients encore hospitalisés.

```
Select `prenom-patient`  from `patient` p where p.`num-patient`  In ( select `num-patient`  from
`hospitaliser` where `durée-hospitalisation` is NULL)
```

8) Afficher le numéro, le nom et le salaire des médecins dont le salaire dépasse 60 000 DA.

```
Select `num-medecin`,`nom-medecin`,`salaire-medecin` from medecin  where `salaire-
medecin`>60000
```

9) Afficher les noms et le salaire des médecins dont le salaire est entre 30 000 DA et 60 000 DA.

```
Select `nom-medecin`,`salaire-medecin` from medecin  where `salaire-medecin`>3000 and `salaire-
medecin`<80000
```

10) Afficher les numéros et les noms des médecins qui ont le grade "Maitre-Assistant" ou "professeur".

```
Select `num-medecin`,`nom-medecin` from medecin  where `grad-medecin`="maitre-
assistant"or`grad-medecin`="professeur"
```

11) Afficher les prénoms des patients qui commencent par un "a" ou (et) se termine par un "a".

```
Select distinct `prenom-patient` from `patient` where `prenom-patient` like 'a%' or (and) `prenom-
patient` like '%a'
```

12) Afficher les numéros des patients qui ont été hospitalisé la première quinzaine de février 2011.

```
Select `num-patient`,`date-entrée` from `hospitaliser`  where `date-entrée`>="2011/02/01" and `date-
entrée`<="2011/02/15"
```

13) Afficher le numéro des patients hospitalisé en 2011.

```
Select `num-patient` from `hospitaliser`  where `date-entrée`>="2011/01/01"and`date-entrée`<="2011/12/31"
```

14) Afficher le nombre de patient traités par chaque médecin

```
Select `nom-medecin`,count(distinct(`num-patient`))as `nb-patient` from `medecin` m,`hospitaliser` h where m.`num-medecin`=h.`num-medecin`  group by `nom-medecin`
```

15) Le prénom des patients, le nom de maladie et la spécialité du médecin traitant des patients âgés de moins 14 ans

```
Select `prenom-patient`,`nom-maladie`,`specialité-medecin`
from `patient` p,`maladie` ma,`hospitaliser` h,`medecin` me
where p.`num-patient`=h.`num-patient`
and h.`num-maladie`=ma.`num-maladie`
and h.`num-medecin`=me.`num-medecin`
and `age`>14
```

1. Introduction – Histoire

Un système d'information c'est un système qui permet d'exécuter sur des informations, tout ou une partie des actions suivantes : recueil, archivage, extraction, traitement, interprétation, réduction, évaluation, présentation, communication. Certain de ces systèmes intègrent des sous-systèmes d'informations ou communiquent avec d'autre systèmes tel que SIS qui englobe le SIH et SIR qui s'agissent a des données médicales, individuelles ou collectives dont la plus grande attention devra être portée à : la fiabilité de la technologie, la validité des données recueillies puis enregistrées ou transmises, la représentativité des données, la protection des données et le respect du secret médical.

Le développement des premiers SIH, essentiellement aux Etats-Unis et dans quelques pays d'Europe comme les Pays-Bas, la Suède ou la Suisse, remonte au milieu des années 1960. Il a suivi l'évolution générale des technologies de l'information (TI) (fig. II.1) : développement des ordinateurs centraux, apparition des mini-ordinateurs pouvant être relies en réseau, arrivée des microordinateurs, développement de l'internet puis du « cloud computing ».

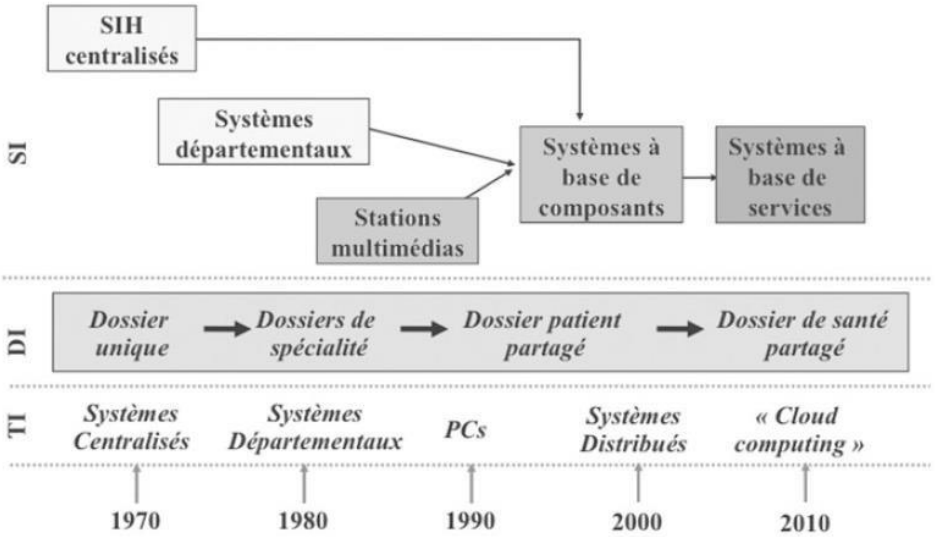


Figure.II.1 : Evolution des concepts en matière de systèmes d'information en sante.
SI = Système d'information ; DI = Dossier informatique ; TI = Technologie de l'information.

C'est ainsi que les premiers SIH, développés pour des ordinateurs centraux, ont permis de gérer bases de données centralisées de dossiers patients.

Le développement des mini-ordinateurs et en particulier du système d'exploitation « Unix » permet apparition de multiples applications départementales dédiées à des structures plus petites qu'un hôpital, en particulier au niveau des plateaux techniques (biologie, pathologie, imagerie, pharmacie) et de quelques spécialités médicales.

L'arrivée des premiers micro-ordinateurs démocratise l'accès aux fonctions informatiques plus large et permet le développement d'interfaces plus conviviales. Car le micro-ordinateur est à la fois un outil d'accès au SI et de travail personnel (« Personal Computer ») et bureautique.

Les années 2000 correspondent à l'intégration en réseau des ordinateurs personnels avec les ordinateurs centraux ou départementaux.

Avec le développement de l'internet haut débit, l'accès à des applications à distance sur la toile (« Cloud computing ») devient possible et les serveurs informatiques peuvent en théorie quitter les salles machines des hôpitaux. L'informatique hospitalière peut s'ouvrir vers l'extérieur et participer à la constitution de dossiers partages a un niveau régional, national ou international.

Alors que plusieurs centaines de SIH sont commercialisées dans le monde, peu d'hôpitaux ont atteint un niveau d'intégration et de maturité (sagesse) suffisant pour faciliter le partage des données individuelles des patients entre professionnels de santé et l'accès aux connaissances contextuelles nécessaires à l'application des règles de bonne pratique de la médecine. Cela revient à la diversité des taches à assurer, des acteurs impliqués, des organisations existantes…ect. Malgré ces difficultés, la mise en place d'un SIH apparait désormais comme une nécessité et bénéficie d'un large consensus (acceptation) de la part des différents acteurs du système de santé et tout particulièrement des décideurs.

La réussite d'un SIH est soumise à plusieurs conditions. Parmi les plus importantes, nous citons :

- La mise en œuvre d'une gouvernance informatique adaptée à la complexité des taches d'informatisation;(Une connaissance approfondie du système d'information de l'hôpital.)
- Un plan d'urbanisation du système d'information de l'hôpital à partir d'une analyse fine des processus métiers;
- Une informatisation par étapes progressives avec des calendriers de mise en œuvre réalistes et une stratégie de conduite du changement;
- Une estimation juste des ressources nécessaires au déploiement puis à l'exploitation du SIH ; (Une stratégie matérielle et logicielle adaptée).
- Une bonne compréhension de la sociologie des organisations de l'hôpital et une bonne communication, interne entre les différents acteurs de l'hôpital et externe avec son environnement; (nature de la production, condition de travail collectif articulé autour de métiers bien identifiés)

– Une analyse des risques et un plan précis de continuité de service.

2. Organisation et gestion de systemes d'information hospitalieres

Avant d'aller plus loin, commençons d'abord par une introduction sur la définition d'une information.

2.1. Qu'est-ce qu'une information ?

L'informaticien parle souvent de « données » (data en anglais). Il ne parle pas «d'informations ». En effet, une donnée se caractérise principalement par son type : alphabétique, alphanumérique, numérique, temporelle (date, heure), binaire, etc. Par contre une information se caractérise par son sens : elle signifie quelque chose.

L'information ne prend son sens que dans un cerveau: elle implique une compréhension de la donnée, et l'idée de son utilisation.

a- Compréhension

Pour comprendre une donnée, il convient de connaître souvent d'autres données connexes, qui constituent ensemble un contexte cohérent pour un mécanisme de déductions successives, autrement appelées «inférences».

Prenons un exemple : si je vous dis «85», vous savez que c'est un nombre, mais vous ne savez pas si c'est une quantité, un poids, une longueur, etc.

Je rajoute une autre donnée : « kg ». Vous savez maintenant que je vous parle d'un poids, mais vous ne savez pas encore si c'est un poids important ou non, car vous ne savez pas ce que nous pesons.

Autre donnée : «Fayçal ». Ah, nous parlons d'une personne' homme'. 85 kg,. Il doit être grassouillet, ou costaud. Autre donnée : « cm». Je m'en doutais, c'est sa taille. Finalement, il est plutôt mince. Ce doit être un sportif en pleine forme. Autre donnée: «11 ». Allons bon, qu'est-ce que c'est encore ? Autre donnée: « ans ». Quoi, il a 11 ans ? Mais alors, cet enfant a un problème de croissance ! Cet exemple montre qu'une donnée en soi n'a pas de signification, qu'elle soit d'ailleurs fournie par un individu, un dossier papier ou un ordinateur.

« Si on prend chaque donnée fournie individuellement, on ne sait pas la qualifier objectivement ».

Heureusement, lorsque nous sommes renseignés, nous recevons simultanément beaucoup de données cohérentes. Nous sommes donc capables de confronter toutes ces données pour en tirer un certain nombre d'informations. Mais il manque parfois des données pour véritablement en tirer des informations. C'est le cas lorsque le message transmis est

incomplet, négligé, ou qu'il faut encore recueillir des données au cours d'une enquête complémentaire (en mettant le patient en observation, par exemple, ou en procédant à des recherches dans les dossiers).

2.2. Quelques Définitions :

a- ***Système d'information*** : ensemble organisé de ressources, des moyens matériels, logiciels, organisationnels et humains visant à acquérir, stocker, traiter, diffuser ou détruire de l'information.

Ces ressources interagissent entre elles pour traiter l'information et la diffuser de façon adéquate en fonction des objectifs d'une organisation.

La qualité d'un système d'information se mesurera donc en fonction de sa capacité à fournir des données cohérentes et complètes. Nous venons de voir qu'une donnée ne peut produire une information que si elle est confrontée à d'autres données constituant un contexte cohérent. Ce contexte est indispensable pour la qualification des données, mais **la valeur des informations se mesure à leur finalité**. Une information qui ne sert à rien… ne sert à rien. Par contre, elle coûte, en moyens de transmissions (ne serait-ce que du temps, du papier, etc.), en charge intellectuelle (pour son interprétation, sa mémorisation), en moyens d'archivage, etc.

Le Système d'Information se construit autour de processus "métier" et ses interactions, et non simplement autour de bases de données ou de logiciels informatiques. Le Système d'Information doit réaliser l'alignement de la stratégie d'entreprise par un management spécifique.

b- ***Système informatique*** : tout ou partie d'un système d'information réalisant des traitements d'informations ; ensemble formé par un équipement informatique et les différents éléments qui lui sont rattachés, matériels et logiciels

c- **Un Système d'Information Hospitalier (SIH)** peut être défini **comme un système informatique destine à faciliter la gestion de l'ensemble des informations médicales et administratives d'un hôpital.** Il s'agit d'améliorer la qualité des soins distribués dans l'hôpital tout en augmentant son efficience. Un SIH peut être aussi considéré comme de système intégré de communication et de traitement de l'information hospitalière.

d- **Le système d'information de l'hôpital** est définit comme un Ensemble des éléments en interaction ayant pour objectif de rassembler, traiter et fournir les informations nécessaires à son activité.

e- ***Qu'est-ce que l'hôpital :*** L'hôpital 'H' est une institution ou une organisation très complexe qui est à la fois bureautique et technocratique générant des quantités

considérables d'information ; dont l'objectif est de soigner et si possible de guérir des malades. Deux modes s'y côtoient :

- ***Mode médical :*** qui met en œuvre son savoir, ses compétences et sa technologie au sein de petites unités de production (les services)
- ***Mode administratif :*** qui organise et donne les moyens de fonctionnement aux unités médicales en effectuant les contrôles budgétaires et en allouant les ressources (personnels finances)

S'il est en quelque sorte un producteur de santé, il assure deux fonctions : une fonction d'accueil et une fonction technique qui prédomine de plus en plus. Pour accomplir ces fonctions, l'hôpital dispose de certaines ressources et emploi de nombreux personne, réparti en catégorie aux fonctions distinctes.

En conséquence, l'hôpital est une énorme machine économique et financière .Les hôpitaux représentent environ 50% des dépenses de soins, lesquelles sont encore croissantes, dépassant 10% du PIB. Une meilleure connaissance de leur fonctionnement, notamment par la mise en place d'un système d'information adapté, devrait permettre une meilleure gestion et utilisation des ressources tout en contribuant à améliorer la qualité des soins

f- **Système d'Information de Santé (SIS)** : Système d'information global, regroupant tous les types d'acteurs et ressources de santé.

Ceci pose une série de problèmes que nous détaillerons également plus loin. À ce stade de notre démonstration, **il convient de prendre conscience que le système d'information est susceptible de fournir des données nombreuses et variées, mais que cela ne suffit pas à son efficacité. Un bon système d'information se caractérise donc par sa pertinence**.

Le système d'information doit aussi intégrer une dimension sémantique, en fournissant des données constituant un contexte compréhensible pour le destinataire. Il doit enfin prendre en compte la finalité de ces données pour la réalisation d'une tâche sans saturer le destinataire de données surnuméraires finissant par constituer un bruit de fond nuisible à son efficacité.

3. Pourquoi un système d'information est important

La constitution d'un système d'information est souvent considérée d'abord comme une tâche technique, par là même peu politique, et donc peu intéressante pour un dirigeant. Cependant, c'est une erreur de la considérer comme neutre, et ce pour trois raisons principales que nous allons détailler :

1. c'est que le système d'information participe à l'augmentation de la valeur de votre établissement.
2. c'est que s'il est encore considéré comme essentiellement technique, le domaine de l'information est le terrain d'expression d'une nouvelle culture d'entreprise qui place la technologie, le développement du savoir et l'optimisation des méthodes au centre des enjeux stratégiques.
3. c'est qu'il est un levier important pour repenser l'organisation de l'hôpital non plus autour de l'offre de soins, mais autour de la demande de soins. Nous passons d'une culture du possible à une culture du souhaitable.

4. La valorisation d'un établissement

Le système d'information devient important si ce dernier représente une valeur, un capital, une richesse à l'établissement (raisonnements ; comptables ;traditionnels)

Mais la valeur d'un hôpital ne se mesure pas uniquement de manière comptable. Un hôpital est doté d'une valeur liée à des biens immatériels, qu'on appelle aussi « actifs intangibles », Ces biens intangibles (immatériels) sont classés selon plusieurs catégories :

- ✓ Les actifs liés à l'innovation, tels que ceux qui résultent d'une activité de recherche et de développement pour une entreprise, ou de la recherche scientifique pour un hôpital. La supériorité perçue par ces établissements est largement liée à une tradition ancienne de recherche scientifique bien médiatisée.
- ✓ Les actifs structurels, liés à la constitution de l'hôpital, et à sa façon de répondre à la demande. Il s'agit en gros de ses méthodes de travail et de sa manière d'être.
- ✓ La qualité de l'accueil, ce qui n'a que peu de choses à voir avec le système d'information.
- ✓ La qualité de prise en charge des patients, ce qui implique une logistique sans faille, et donc souvent un système d'information performant.
- ✓ Une absence d'erreurs dans les transmissions et l'exécution des tâches, une bonne fluidité des processus, une capacité à fédérer les compétences autour du patient. Là aussi, le système d'information joue son rôle, comme une aide à la coordination.
- ✓ Une bonne information du patient et de son entourage. Il faut faire constater par le patient combien votre établissement est performant, à la fois par des résultats réels, mais aussi par des explications sur les moyens qui ont été mis en œuvre pour le soigner.

- ✓ Une véritable capacité à gérer les problèmes complexes, en vous attachant les services de personnes de grande compétence. L'établissement, perçu comme maîtrisant la haute technicité de la médecine moderne, présente un aspect rassurant. Là aussi, il faut non seulement une culture de l'enseignement et de la recherche, mais aussi des moyens informatiques, ne serait-ce qu'une connexion à Internet.

- D'une manière générale, la satisfaction de la demande, est l'objectif de tout système d'information.

5. Objectifs des systèmes d'information hospitaliers

Les objectifs du SI comme les objectifs de l'entreprise, à savoir soigner au mieux et au moindre cout pour un établissement hospitalier (tableau II.1).

Parmi Les objectifs d'un SIH :

- La conservation et l'échange des données ; Le partage de l'information
- La disponibilité de l'information
- L'amélioration de la qualité des soins
- Le gain de temps : diminution de la durée de séjour de patient
- La maitrise des couts et la réduction des erreurs

Selon Kohler, le SIH s'oriente sur deux objectifs principaux : l'amélioration de qualité des soins et la maitrise des coûts.

Tableau II.1-Objectifs des systèmes d'information hospitaliers

Objectifs principaux	**Objectifs contributifs**
Amélioration de la qualité et de la continuité des soins	- Uniformisation des pratiques - Aide à la prise de décisions - Réduction de l'iatrogénie médicale - Amélioration des résultats (Outcome)
Maitrise des couts	- Optimisation des processus médicaux - Réduction des tâches administratives - Réduction de la durée des séjours - Mise à disposition d'outils de pilotage médico économique

La qualité des soins est définie par l'Institut de médecine (IOM) aux Etats-Unis comme « la capacité des services de sante destinés aux individus et aux populations d'augmenter la probabilité d'atteindre les résultats de sante souhaités, en conformité avec les connaissances

professionnelles du moment ».

Le développement d'outils d'aide à la décision médicale est un élément contributif majeur de la qualité et peut être utile à toutes les étapes de la démarche médicale (préventive, diagnostique, thérapeutique, pronostique). Il s'agit, à la fois, d'améliorer les résultats (outcome) et de réduire l'iatrogénie médicale. Avec l'augmentation de la durée de vie et l'apparition de nouvelles thérapeutiques, la maitrise des couts de sante devient un paramètre essentiel dans la décision d'informatiser les processus de sante.

6. Le plan d'urbanisation du SI

6.1. *Le modèle des quatre cadrans*

Sous le terme d'urbanisation du SI, on regroupe habituellement différentes étapes de mise en œuvre allant de l'analyse du système d'information à la sélection des composants informatiques et des conditions de déploiement (fig.II.2) :

– La compréhension des finalités de l'entreprise concernée (ici l'hôpital) et des acteurs concernés (intra- et extrahospitaliers);

– L'analyse des activités et de l'enchainement des taches (processus métiers);

– L'analyse des données et informations échangées;

– L'analyse du choix d'applications informatiques pouvant servir de support aux processus métiers et à leur intégration;

– Le choix d'une stratégie de conduite du changement et de déploiement.

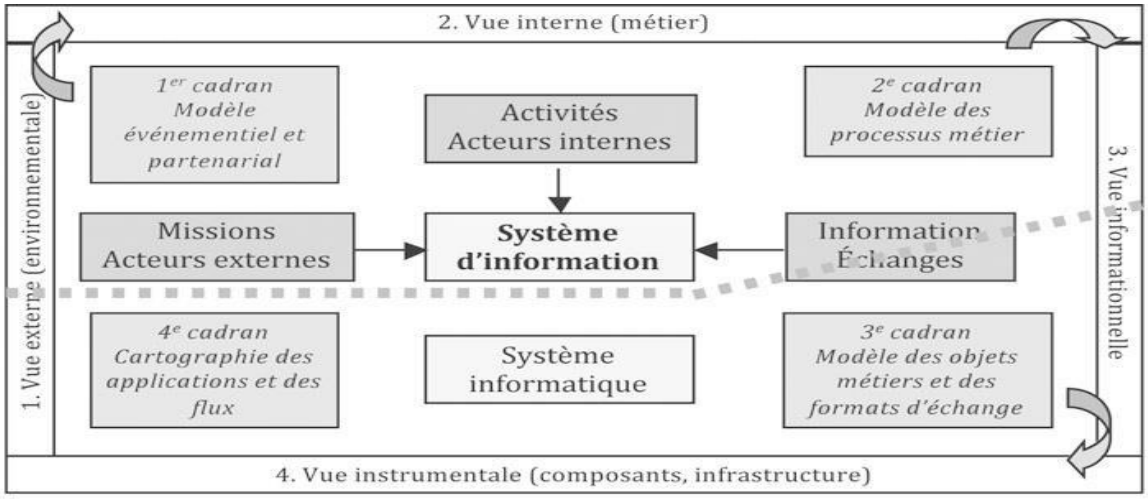


Figure. II.2–Le modèle des quatre cadrans (d'après Le Roux B (2009) La transformation stratégique du système d'information. Paris, Lavoisier). Les activités en dessous de la ligne en pointilles ont une forte connotation informatique.

6.1.1. *Environnement du système d'information, la vue externe*

Dans un modèle d'environnement, l'entreprise est considérée comme une boite noire (black box) en partenariat avec le système d'information de sante (médecine libérale ou organismes d'assurance par exemple). Les consultations, les admissions ou les sorties, les avis médicaux représentent les interactions principales liées au cœur du métier hospitalier. La figure II.3 illustre la diversité des acteurs impliqués de façon directe ou indirecte par le système d'information hospitalier. Les acteurs extérieurs se situent au niveau des organismes de tutelle mais également des assurances, des industriels ou des medias. . Les patients interviennent comme clients de l'entreprise traites en interne mais également comme groupes de pression externes au travers d'associations de patients ou des réseaux sociaux ; quant aux acteurs intérieurs il s'agit à l'évidence des patients des personnels de soins (médecins, infirmiers…etc.)[1], des personnels administratifs ces acteurs sont présentés dans la figure II.3.

Les missions de l'hôpital sont à l'évidence le soin mais également l'enseignement et la recherche pour les hôpitaux universitaires.

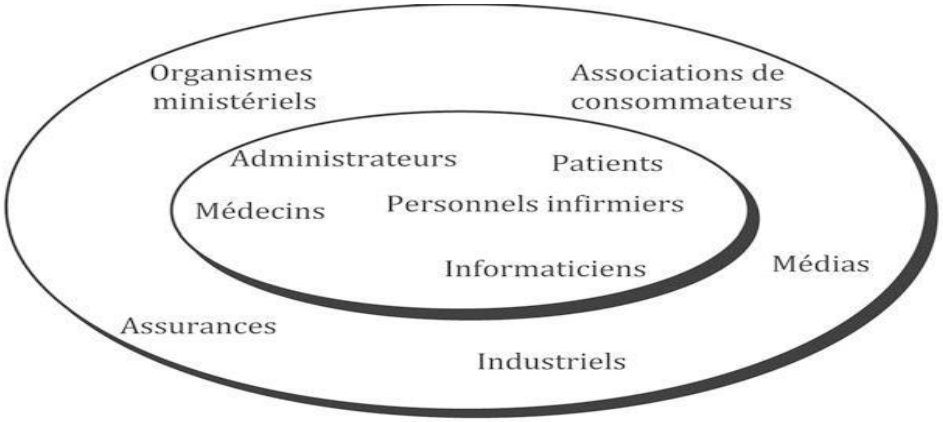


Figure.II.3 – Les acteurs d'un système d'information hospitalier (SIH). (D'après Degoulet P, Fieschi M (1998) Informatique médicale. 3e Edition. Paris, Masson.)

Le système d'information de l'hôpital, quelle qu'en soit sa complexité, doit être analysé dans le cadre plus large du système d'information de santé, afin de ne pas sous-estimer les besoins de communication entre les différents sous-systèmes (médecine libérale ou organismes d'assurance par exemple). C'est une composante essentielle des réseaux de soins et doit s'intégrer harmonieusement dans leur mise en place.
La figure II.4 donne des exemples de niveaux d'analyse du système d'information. La plupart des fonctionnalités recherchées (par exemple l'évaluation de la qualité, la planification financière) peuvent être envisagées à plusieurs niveaux d'agrégation (service, hôpital, réseau de soins, etc.).

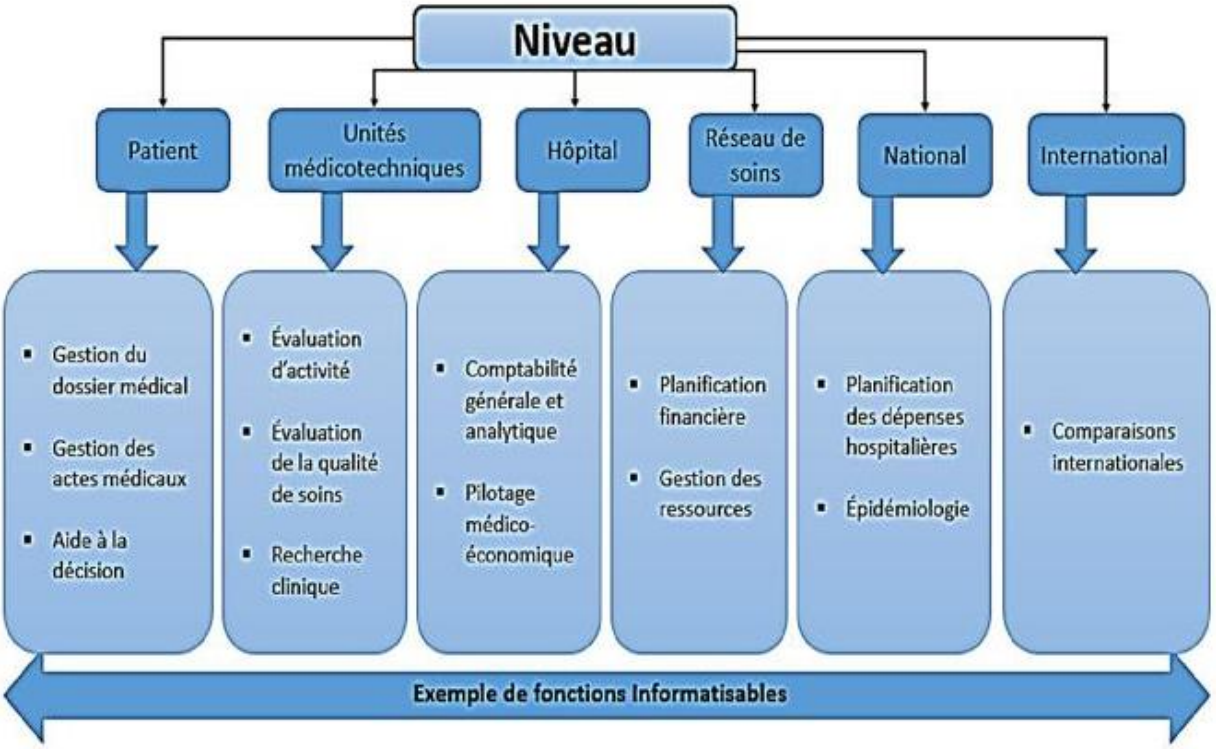


Figure II.4: Exemples de niveau d'analyse du système d'information

6.1.2. *Vue interne, les structures et les processus métier*

Au niveau interne de l'hôpital, les acteurs sont à l'évidence les personnels de soins (médecins, personnels infirmiers, paramédicaux, pharmaciens et biologistes, ingénieurs biomédicaux, etc.) et les personnels administratifs et logistiques. L'analyse structurelle considère l'entreprise comme une boite de verre (« glass box ») et fournit une représentation détaillée de l'organisation, des ressources matérielles et humaines. La France est caractérisée par une dépendance étroite entre des structures matérielles et humaines fortement hiérarchisées (pôles, services, unités fonctionnelles), a l'inverse des pays nord-américains ou les ressources matérielles (lits, plateaux techniques) sont plus volontiers partagées par des ensembles de ressources humaines (départements) (fig.II.5).

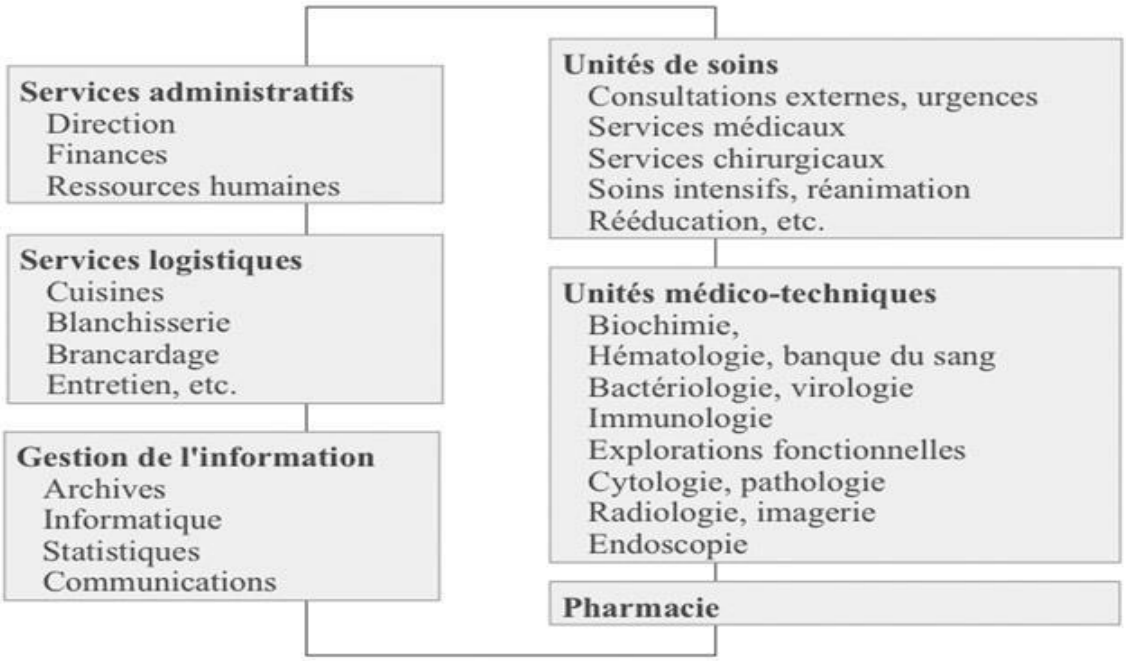


Figure.II.5 – Les structures hospitalières. (D'après Degoulet P, Fieschi M (1998) Informatique médicale. 3e édition. Paris, Masson.)

En principe, un service medico-technique n'est pas, comme une unité de soins classique, destiné à prendre en charge le suivi des malades. En pratique, l'expérience des dernières années montre que la distinction entre service médicotechnique et service clinique n'est pas toujours nette. Un laboratoire peut prendre en charge des catégories particulières de malades (par exemple des hémophiles ou des malades sous anticoagulants pour un service d'hématologie). Inversement, il arrive qu'un service clinique développe une activité d'exploration pour le reste de l'hôpital ou pour des structures extérieures (par ex. échocardiographie, endoscopie...). En termes d'analyse du système d'information, chacune de ces structures, médicales ou médicotechniques, devient une ressource mise à la disposition des autres structures ou de l'extérieur, générant des actes, produisant de l'information et consommant d'autres ressources. L'analyse fonctionnelle part de l'activité hospitalière pour en déduire des circuits de gestion de l'information qui permettront de déterminer les différentes fonctions du SI puis de choisir celles qui feront l'objet d'une informatisation.

La topologique de l'Approche structurelle c'est une division du SIH selon le découpage organisationnel : unités de soins, plateau technique, services administratifs.

Avantage :

- ✓ Permet de gérer un projet ciblé.
- ✓ Permet de superposer le groupe de travail au service.

Exemple : mise en place d'un dossier de spécialité dans un service de cardiologie.

Inconvénient :

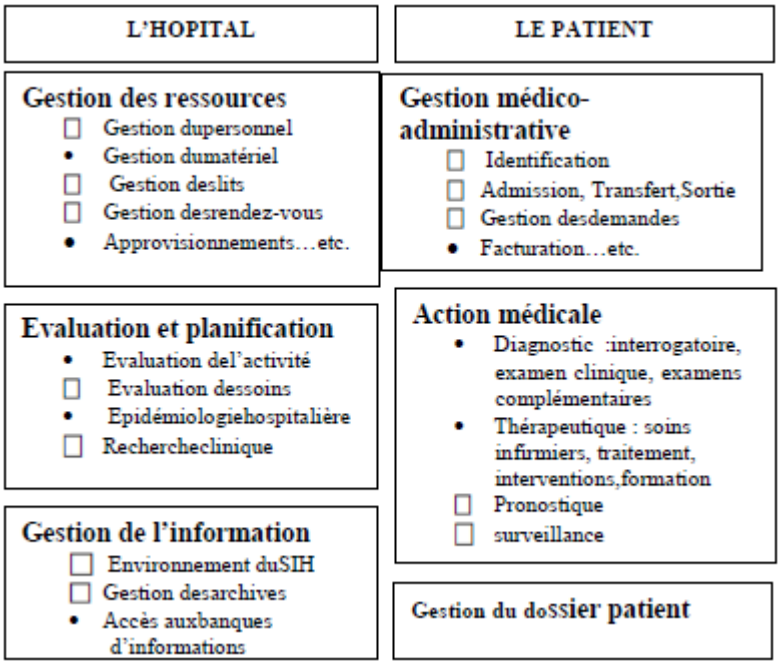
- ✓ Risque d'arriver à un SIH départementalisé.
- ✓ Difficulté pour faire avancer la logique d'intégration.
- ✓ *Illustration* : un dossier médical par unité de soins, sans communication avec l'informatique administrative et encore moins entre eux (continuité des soins dans une filière de soins).

6.1.3. Analyse fonctionnelle

L'analyse fonctionnelle permet de déterminer les différentes fonctions d'un système (action médicale diagnostique ou thérapeutique, gestion des ressources…), c'est-à-dire le "quoi" du système d'information.

Toute division du système d'information de l'hôpital en sous-systèmes est arbitraire. De façon schématique, trois grandes approches peuvent être proposées :

- La première approche consiste à projeter les fonctions sur les acteurs (hospitaliers) du système d'information. Elle permet de mieux cerner les besoins des différentes catégories de personnels hospitaliers. On peut ainsi parler de sous-systèmes d'information administratifs, médicale, infirmier, etc.
- La deuxième approche, fréquemment utilisée en France, calque les sous-systèmes sur les structures de l'hôpital. Elle revient donc à distinguer le sous-système d'information médico-administrative des sous-systèmes de gestion des unités de soins ou ceux des plateaux technique (biologie, radiologie, etc.).
- La dernière approche consiste à individualiser le système d'information du patient (tout ce qui concerne le patient et qui peut être stocké dans le dossier patient) de ce qui concerne le reste de l'hôpital. La figure II.6 illustre cette approche.



Figue II.6: Analyse fonctionnelle du SIH « Source: STACCINI, Pascal**.** *Cours Système d'information hospitalier(S.I.H),* Université Nice-Sophia Antipolis, 2006-2007. »

Dans cette approche, le SIH est subdivisé en grandes fonctions, sous fonctions, tels que les : fonctions médicales (dossier médical informatisé, prescription des actes), fonctions logistiques, fonctions financières, etc.

Avantage :

- ✓ Vision simple à appréhender car on a un découpage par métier, donc lecteur immédiate.
- ✓ Correspond souvent à l'offre des fournisseurs.

Inconvénient :

- ✓ Ne permet pas d'informatiser les processus qui sont à cheval sur plusieurs domaines.
- ✓ *Illustration* : prescription des médicaments par le médecin, indissociable de son administration par l'infirmière, indissociable de la dispensation ou la validation par le pharmacien.

7. Composants d'un système d'information hospitalier

Nous présenterons les composants classiques des SIH sous forme de schémas synthétiques. [4]

a. Gestion administrative : Elle permet l'admission des malades, la gestion de leurs mouvements au sein de l'hôpital (lits, mutations entre services) dite « gestion opérationnelle » , elle comporte principalement les sous-systèmes de gestion médico-administrative des malades (figure II.7).

Figure II.7 : Le sous-système de gestion administrative

b. Gestion des unités de soins

Elle regroupe toutes les fonctions liées aux soins d'un patient donné et à l'action médicale en général (figure II.8.a). Elle est de ce fait très complexe et difficile à modéliser. De façon schématique, on peut y distinguer trois sous-systèmes :

- ✓ Le sous-système lié à la production des actes (demande des examens, retour des résultats, gestion et optimisation des rendez-vous) ;
- ✓ Le sous-système lié à la constitution et à la mise à jour du dossier permanent du patient ;
- ✓ Le sous-système lié au contrôle et au pilotage de ces activités.

Les fonctions de communication sont très importantes. Une partie de la complexité est liée à la nécessité de chainer les informations concernant les différents épisodes de soins intra, mais également extrahospitaliers afin d'éviter les examens redondants et de garantir la cohérence des soins.

c. Gestion des plateaux techniques

On regroupe sous cette dénomination toutes les activités de laboratoires de biologie, des services d'exploitations fonctionnelles, des services d'imagerie et de la pharmacie. La figure II.8.b schématise les fonctions assurées par ces unités.

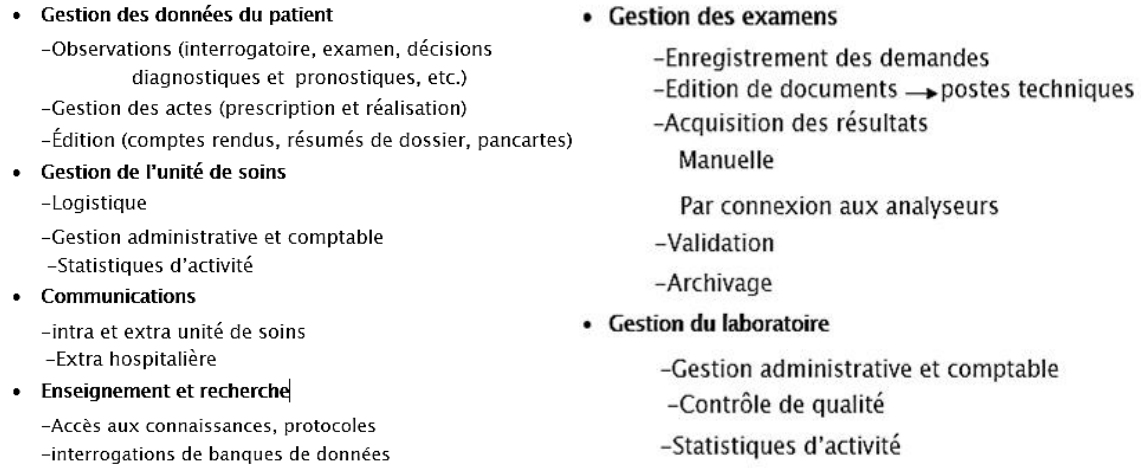


Figure II.8 : Le sous-système de a) gestion des soins b) de l'information biologique

8. La stratégie d'informatisation

8.1. Le processus d'informatisation

Le processus d'informatisation consiste à regrouper des ensembles de fonctions ou de processus dans des applications informatiques qu'il sera nécessaire de les faire communiquer entre elles. A cet effet, le choix d'une approche appropriée est très important. Une approche inappropriée peut conduire à des impasses technologiques, à des blocages organisationnels et finalement à des dépenses inutiles. Généralement, deux approches peuvent être suivies dans l'installation d'un SI : une approche verticale et une approche horizontale.

8.2. Approches verticale, par structures ou centralisée (1970)

Le SIH peut être construit sur la base d'une architecture centralisée (approche verticale), où les fonctions de l'ensemble de l'hôpital seront pris en charge dans une même architecture matérielle et logicielle. Le principe dominant de ce type d'architecture est que l'information est saisie une seule fois et stockée en un point unique de la base de données centrale.

Tenant compte d'une augmentation progressive du nombre d'applications à gérer au fil des années ainsi que du développement technologique, les dirigeants sont lancés depuis une dizaine d'années dans un processus d'évolution de leur système d'information.

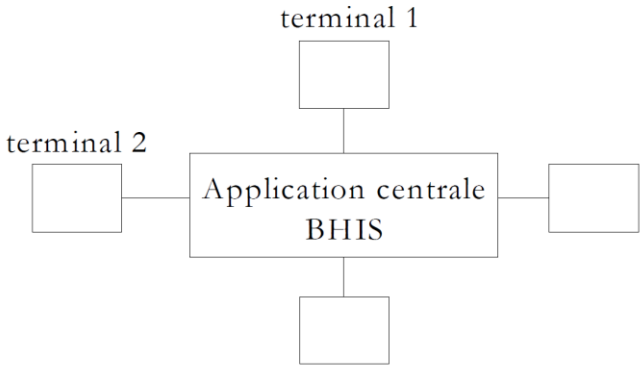


Figure.II.9 – Informatisation des structures et application « verticales ».

Le modèle d'une architecture centralisée ne répondait plus aux besoins de l'hôpital. Par conséquent, le SIH est dirigé progressivement vers un système décentralisé (approche horizontale).

- **Avantages**
  - Système intégré centré sur le patient.
  - Mise en service et maintenance facilitée des modules applicatifs
  - Contrôle facile du système
  - Système clé en main
- **Inconvénients**
  - Forte dépendance face à un constructeur ou couple constructeur/vendeur de SIH
  - Évolution non progressive. L'évolution en peut se faire que par à-coups lors d'un changement de version
  - Peu de prise en compte des besoins périphériques spécifiques
  - Standardisation élevée

8.3. Approches horizontales, par processus ou départemental (1980)

En d'autres termes, il s'agit de l'informatisation de modules indépendants dans différents départements, donnant ainsi naissance aux systèmes départementaux. Les premières unités concernées ont été les laboratoires, l'anatomo-pathologie et la radiologie, suivies d'autres unités comme la gynécologie, les soins intensifs, etc.

Initialement, il n'y avait pas d'interconnexion des systèmes entre eux. La cohérence des données patients a été assurée par des interfaces du type point à point, c'est-à-dire que chaque système départemental était relié directement à BHIS (AXYA) (Figure II. 10).

Le mécanisme d'interfaces a permis d'avoir des références uniques pour un patient mais sa maintenance était complexe car chaque système possédait son propre mode de communication et le moindre changement entraînait des frais importants.

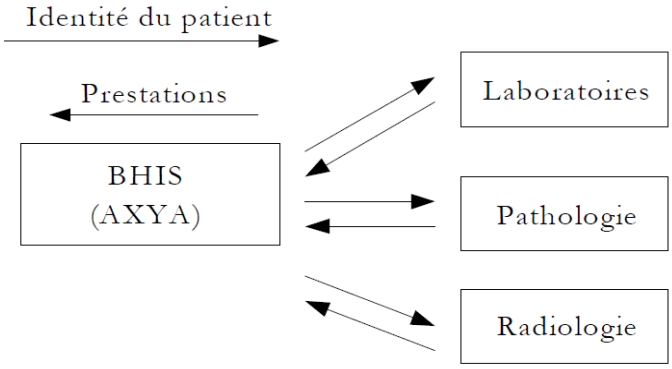


Figure.II.10 – Informatisation par processus et application « horizontales ».

Le changement d'une information au niveau du système source (BHIS) impliquait un changement de cette information pour chaque interface. Dans le cas de la figure II.10, on devait ainsi annoncer le changement de nom d'un patient, par exemple, à l'interface des laboratoires, à celui de la pathologie et à celui de la radiologie, répétant ainsi trois fois la modification de la même information.

- **Avantages**
  - Meilleurs adaptation des produits à la demande des utilisateurs.
  - Dissociation du matériel et du logiciel
  - Investissement progressif
  - Applications multi-hospitalières (notion de filières)
- **Inconvénients**
  - Babélisation du SIH
  - Redondance de l'information
  - Difficulté de maintenir l'intégrité et la cohérence de l'information
  - Coût élevé de l'intégration en l'absence de standard de communication (norme HL7) (voir *chapitre 4 sur le DICOM*)

8.4. Approches mixtes horizontales et verticales ou distribuée

Tenant compte des inconvénients de l'architecture décentralisée, les dirigeants se sont orientés à la fin des années 90, vers un SIH distribué. Il s'agit d'une combinaison des deux approches précédentes, centralisée (verticale) et décentralisée (horizontale). La nouvelle approche permet un investissement progressif par acquisitions successives de différentes applications, reparties sur plusieurs processeurs. La nouvelle architecture a fourni un moteur d'intégration connu sous le nom « middleware » permettant le contrôle du flux de

l'information ainsi que la communication entre les différentes applications du SIH (Fig II.11).

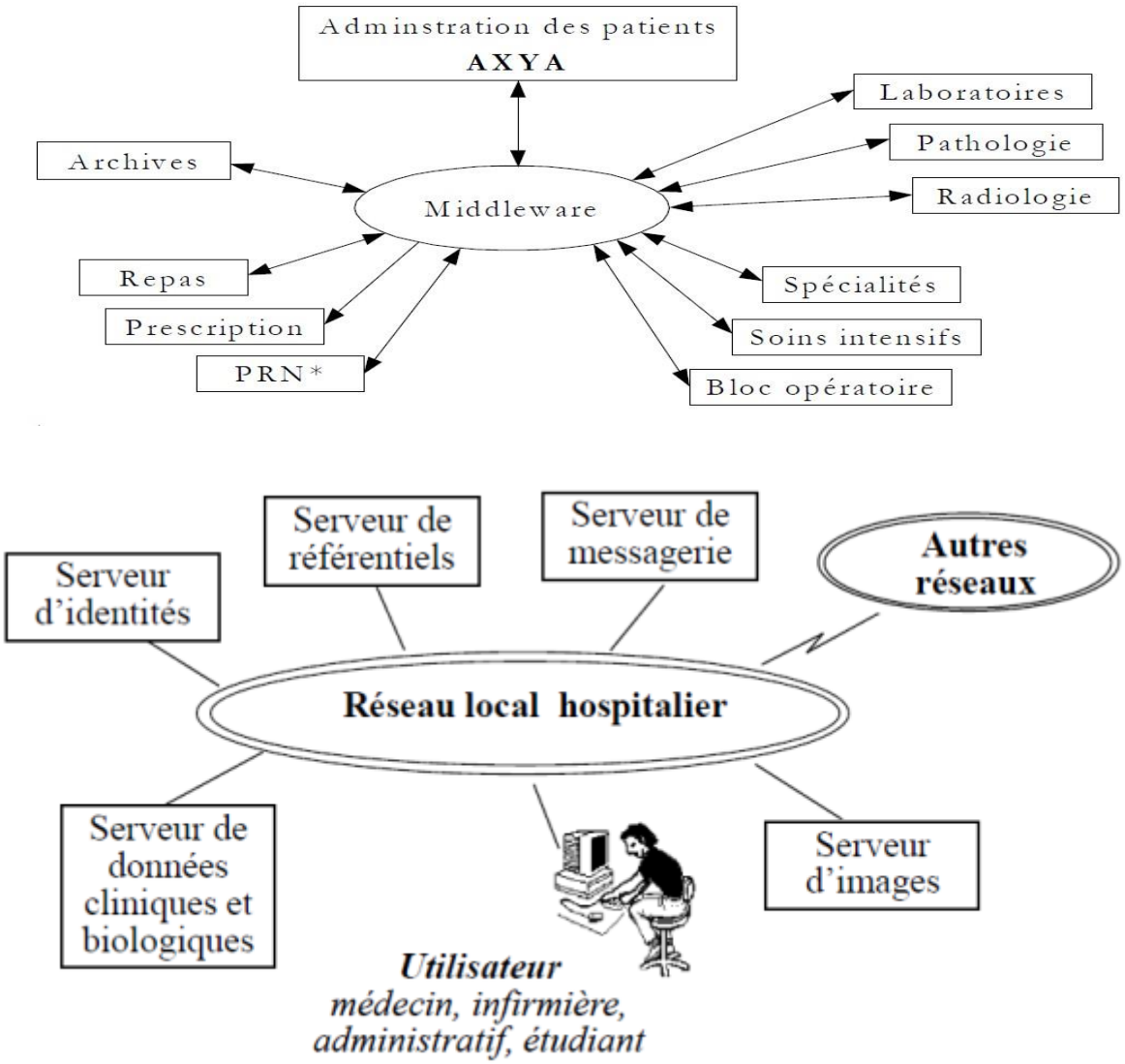


Figure.II.11 – Approche mixte « horizontale » et « verticale ».

Un des avantages majeurs de l'architecture distribuée consiste dans le fait que le changement d'un des modules ne remet pas en cause l'ensemble du système.

Le middleware (anglicisme) ou intergiciel en architecture informatique est un logiciel tiers qui crée un réseau d'échange d'informations entre différentes applications informatiques. Le réseau est mis en œuvre par l'utilisation d'une même technique d'échange d'informations dans toutes les applications impliquées à l'aide de composants logiciels.

Les composants logiciels du middleware assurent la communication entre les applications quels que soient les ordinateurs impliqués et quelles que soient les caractéristiques matérielles et logicielles des réseaux informatiques, des protocoles

réseau, des systèmes d'exploitation impliqués.

✓ **Avantages**

- Choix du meilleur couple matériel-logiciel
- Investissement progressif.
- Évolution par « retouches ».
- Indépendance accrue (constructeurs, SSII)

✓ **Inconvénients**

✓ Complexité accrue ; - Nécessité de standards.

✓ Terminologie ; - Présentation - Communication

8.5. Les bénéfices attendus d'un SIH :

Table II.2.bénifices attendus d'un SIH

Gain du temps	- Réduction ou suppression des transcriptions - Réduction de la durée du cycle des examens complémentaires (2 à 5 heures) - Réduction des taches cléricales effectuées par le personnel médical et/ou infirmier (7-10%) - Accès facilité aux données médicales - Diminution de la durée des séjours
Réduction des erreurs	- Prescriptions médicales inappropriées (20%) - Prescription incomplètes (25%) - Erreurs de transcription des résultats (sup 50%)
Accés facilité aux connaissances	- Réduction de la variabilité des comportements médicaux (25%)
Gains de productivité	- Diminution des pics d'activité et optimisation des ressources - Réduction de personnels (inf à 5%)

8.6. Conception de système informatique de l'hôpital

Le système d'information est une réalité intrinsèque à l'hôpital, indépendante de toute informatisation. Il se situe au cœur du fonctionnement de l'établissement de santé, il couvre l'ensemble des informations utilisées dans l'hôpital.

La mise en place d'un système d'informatique est souvent l'occasion de son réexamen, en vue de son automatisation plus au moins complète, aboutissant à la constitution d'un SIH. Cette automatisation recouvre généralement les fonctions de mémorisation et de communication, voire de traitement.

L'informatisation (la réorganisation), la formalisation et automatisation des flux d'information devraient apporter une gestion plus rationnelle de son activité, une meilleure connaissance du fonctionnement de l'hôpital, une amélioration de la qualité des soins, un meilleur support pour la recherche et l'enseignement.

Quelques principes doivent guider la mise en place du système informatique de l'hôpital :

- Conception globale;

- Position centrale du Malade et de son dossier;
- Saisie unique de l'information à la source, partage et retour de l'information;
- Souplesse : interface accessible par le commun des utilisateurs;
- Mémorisation et communication ;
- Protection des données ;
- Disponibilité.

D'autre part, l'analyse des flux comme le respect de ses principes conduit à proposer une organisation structurelle du SI concentré sur :

- L'identification des malades ;
- Déplacements;
- Fonctions cliniques ;
- Administration;
- Gestion.

Cette organisation ne préjuge pas de la configuration matérielle du système informatique, laquelle est également conditionnée par la taille et le mode de fonctionnement de l'hôpital, l'indentification et le mouvement des malades.

8.7. Le dossier Patient informatisé

Le Dossier Patient est l'ensemble de toutes les informations du patient lorsqu'il est hospitalisé ou en consultation à l'hôpital. Dans le langage informatique, le Dossier Patient représente l'ensemble de toutes les fonctionnalités du logiciel qui contiennent les informations propres au patient :

- Son dossier administratif ;
- Son dossier médical ;
- Son dossier de Soins ;
- Ses prescriptions ;
- Toutes les correspondances (courriers entre Professionnels de Santé, comptes-rendus…).

Le Dossier Patient assure la traçabilité de toutes les actions effectuées par les Professionnels de Santé. Il est un outil de communication, de coordination et d'information entre les Professionnels et avec les patients. Il permet de suivre et de comprendre le parcours hospitalier du patient. Il est un élément primordial de la qualité des soins en permettant leur continuité dans le cadre d'une prise en charge pluri-professionnelle et pluridisciplinaire.

8.7.1. Les fonctionnalités du Dossier Patient

Une fonctionnalité est un ensemble de données qui seront informatisées dans un langage propre. Plusieurs fonctionnalités peuvent être intégrées de manière à former un module ayant une cohérence fonctionnelle.

A titre d'exemple les fonctionnalités suivantes forment le module de la Prescription (Figure II.12) :

- Prescrire un médicament ;
- Choisir la posologie (dosage) ;
- Choisir la fréquence d'administration ;
- Choisir la durée de la prescription ;
- Signer la Prescription et visualiser les alertes données par la base scientifique éventuellement interfacée.

Dans le SIH, il est fréquent que les modules soient imbriqués les uns dans les autres. Il est nécessaire de mettre en œuvre un plan d'urbanisation de ces modules afin qu'ils sachent communiquer entre eux. L'urbanisation d'un SIH est matérialisée par sa cartographie. La cartographie est en réalité la cible de fonctionnement que l'on souhaite atteindre dans l'utilisation standard du SIH. L'urbanisation du Système d'Information permet entre autre de décrire le Système d'Information de façon complète, générique, et de fournir une articulation judicieuse des modules entre eux.

Figure II.12 : Représentation schématique du module de Prescription d'un SIH

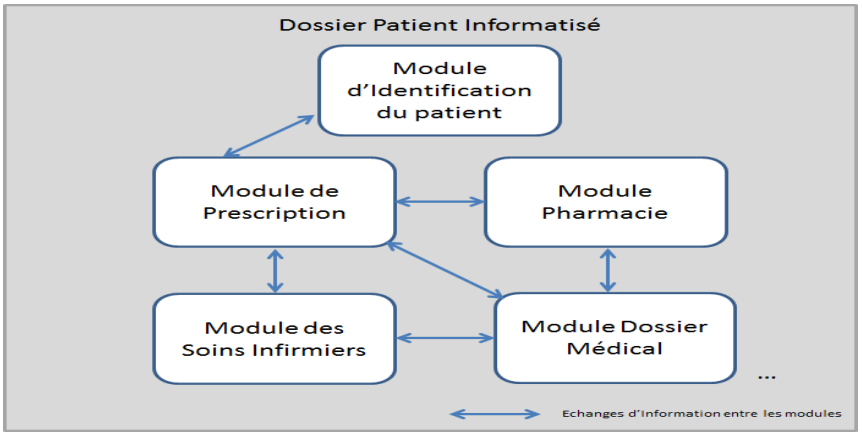


Figure II.13 : Représentation schématique non-exhaustive de la cartographie d'un SIH (Dossier Patient)

Les modules sont capables de communiquer entre eux ou savent, pour certains, fonctionner de manière autonome (Figure II.13). Cette problématique de communication ou non des modules entre eux est un point d'attention fort lorsqu'un Système d'Information Hospitalier est développé. Il faut anticiper la communication des modules, d'autant qu'il est possible que deux modules soient développés dans des langages informatiques différents et ceux pour des raisons de fonctionnalités.

La classification des Systèmes d'Information par modules est la plus utilisée en termes de pilotage de projets puisqu'elle traite des fonctionnalités métiers des utilisateurs. Elle est commune et utilisée par :

- Les Equipes « Projet » hospitalières en charge de la spécification et du déploiement d'un SIH ;
- Les personnels soignants et personnels non-soignants ;
- Le personnel administratif ;
- Les équipes fonctionnelles en charge du projet du côté de l'éditeur et/ou de l'intégrateur du SIH.

Un établissement de santé a la possibilité de n'acheter que certains des modules proposés par l'éditeur. Cela permet à l'établissement :

- D'engager un moindre coût dans le projet d'informatisation en ne choisissant que les modules jugés nécessaires par la Direction Générale et/ou l'équipe « projet » ;
- Ou d'informatiser son Etablissement de manière progressive ;
- Ou d'informatiser son Etablissement en interfaçant avec des SI éventuellement existants.

Un ensemble de fonctionnalités = Un module

Un ensemble de modules = Dossier Patient Informatisé

Chaque établissement peut choisir les modules dont il souhaite disposer dans son Dossier Patient.

Pour que les systèmes d'information en santé soient **interopérables**, certaines conditions, d'ordre technique ou relevant de l'organisation des soins, doivent être satisfaites.

Les modules classiquement représentés dans un Système d'Information Hospitalier sont :

- L'identification du patient
- Le dossier médical du patient
- Le dossier de soins
- La prescription
- La gestion de la Pharmacie à Usage Interne
- L'administration du produit de santé au malade

8.7.2. L'identification du patient

Il s'agit d'un module nommé « Dossier Administratif ». Il permet de renseigner le nom du patient, sa date et lieu de naissance, son adresse, son sexe, les identités particulières (patient confidentiel, inconscient, s'il est éventuellement né sous X), mais aussi son médecin traitant, la personne de confiance et/ou la personne à prévenir en cas d'urgence (Figure II.14).
Ces informations sont généralement saisies par le Bureau des Entrées (agents administratifs).

La création d'un Dossier Administratif permet de générer un numéro unique de dossier, spécifique au patient. Lorsque le Système d'Information Hospitalier permet aux hôpitaux d'un même groupement ou d'une même ville de communiquer entre eux, ce numéro unique de patient permet de l'identifier toute sa vie à chacune de ses venues ou consultations dans ce même groupement d'Hôpitaux. Ce numéro unique de patient permet d'éviter les doublonnages de dossier et d'identité, les erreurs de saisie, et permet également une meilleure coordination des soins.

8.7.3. Le dossier médical du patient

Il est renseigné par le médecin qui prend en charge le patient lors de son hospitalisation. Il permet de stocker les informations suivantes :

- Motif d'entrée ou de consultation ;
- Antécédents et allergies ;
- Les lettres et compte-rendu d'examens complémentaires…

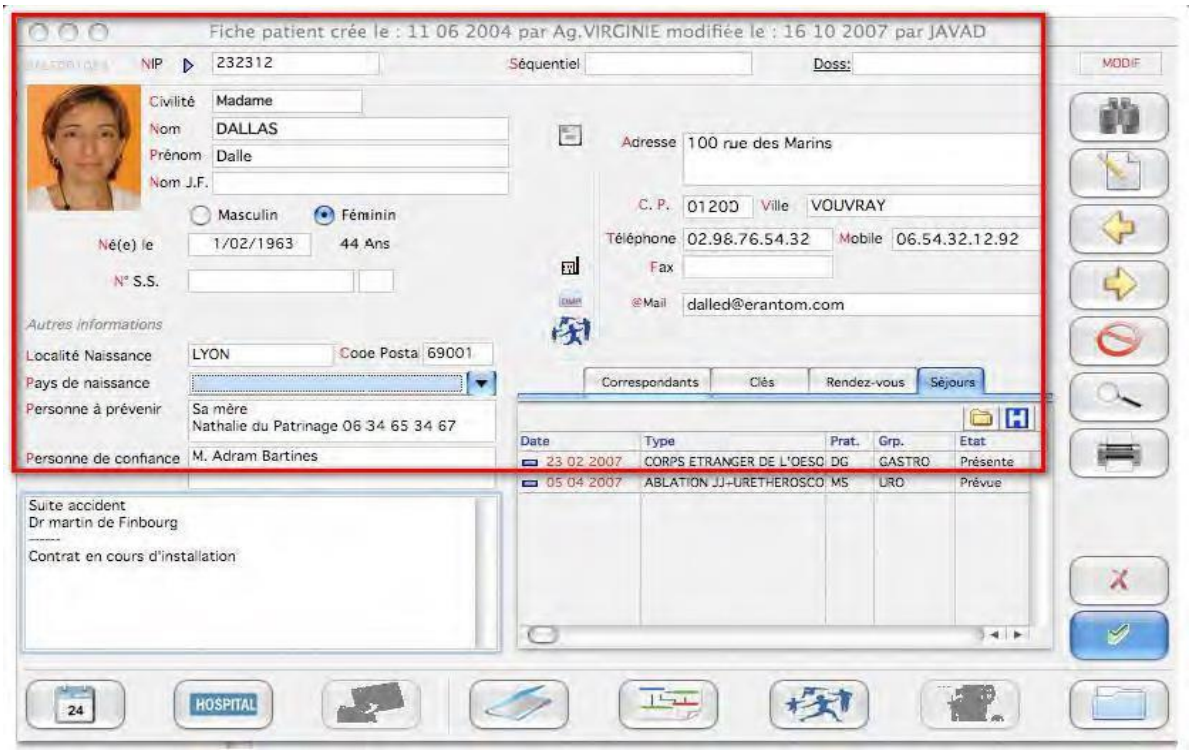


Figure II.14 : Exemple d'écran d'Identité du Patient (partie haute de l'écran), Osoft de Medibase

8.7.4. Le dossier de soins

Il permet de recueillir les données de soins du patient, telles que :

- La feuille de surveillance ou relevé des constantes (poids, taille, tension artérielle) qui permet d'enregistrer et suivre leur évolution. Informatiquement, ce relevé de constantes remplace le dossier papier, historiquement accroché au fond du lit du patient. Elle est souvent appelée pancarte dans le cadre informatique;
- Les fiches de transmission des infirmières donnant des informations générales ou spécifiques de l'état du patient : c'est le résumé qui est saisi après la réunion faite entre les Infirmiers travaillant la nuit et ceux qui prennent la relève de jour ;
- La fiche de liaison infirmière : il s'agit du document destiné à être remis au service ou à l'établissement receveur lors de la sortie ou du transfert du patient.

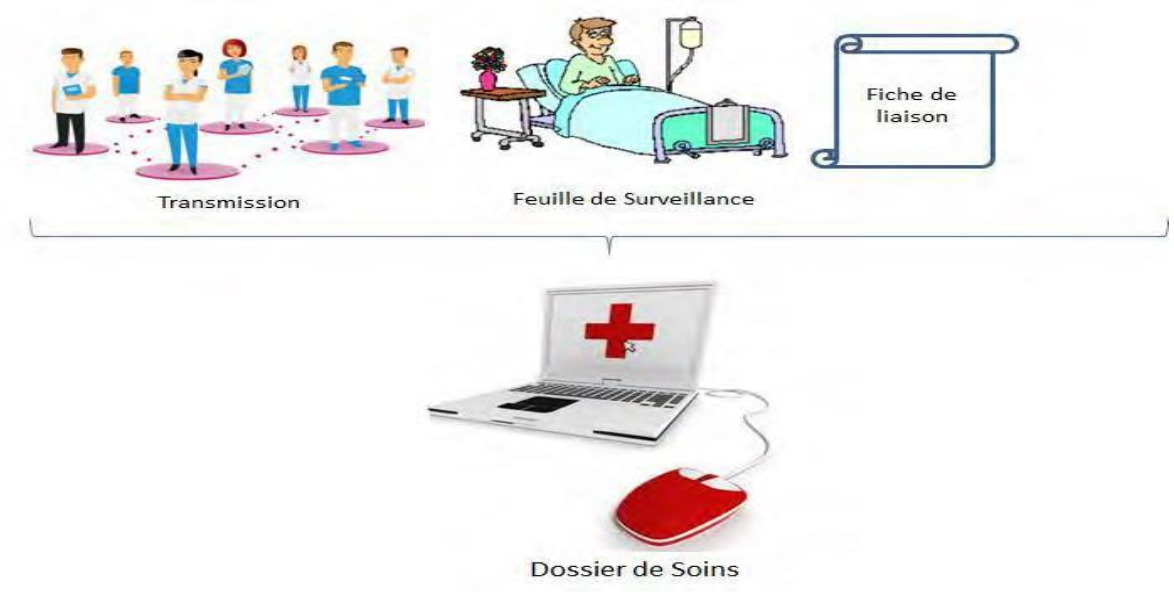


Figure II.15 : Représentation schématique du Dossier de Soins

8.7.5. La prescription

La prescription fait partie du dossier médical dans l'arborescence d'un Système d'Information Hospitalier. Elle peut aussi être présente de manière autonome.

Il s'agit de la prescription faite par un médecin habilité. La prescription est un acte médical réalisé par un médecin en situation d'exercice (inscrit au Tableau de l'Ordre). Elle se fait sur ordonnance. Elle est l'ensemble de conduite écrite pour le malade. La prescription peut être de plusieurs types :

- La prescription de produits de santé (médicaments et/ou dispositifs médicaux) ;
- La prescription d'actes de biologie médicale. Ce sont les examens de biologie médicale (Biochimie, Hématologie, Génétique, Biologie Cellulaire, Biologie Moléculaire, Onco-Biologie, Pharmacotoxicologie, Immunologie, Radio-immuno-analyse, et Biologie de la Reproduction), d'Infectiologie, d'Anatomo-pathologie et de Neuropathologie ;
- La demande d'examens de radiologie et d'imagerie médicale (radiologie conventionnelle, échographie, scanner à rayon X et Imagerie par Résonnance Magnétique (IRM)) ;
- La prescription d'actes médicaux Infirmiers et de séances de soins Infirmiers ;
- La prescription d'actes paramédicaux. Les kinésithérapeutes, les ambulanciers et les diététiciens (expert en nutrition et alimentation) sont les professions paramédicales principalement représentées dans les établissements de santé et qui font l'objet d'une prescription d'acte paramédical.

Lorsque les différents types de prescriptions sont gérés sur un même écran, il s'agit alors d'une prescription « multimodale » ou « complexe ». Lorsque les différents types sont gérés sur des

écrans séparés, il s'agit de prescriptions unitaires.

Les modules de prescription sont classiquement interfacés avec des référentiels :

- Référentiel médicamenteux (Vidal, Thériaque, Thesorimed…) ;
- Référentiel des actes de Biologie (Nomenclature des Actes de Biologie Médicale);
- Référentiel des actes de radiologie (Classification Commune des Actes Médicaux Figure 16).

Figure II.16 : Extrait de la Classification Commune des Actes Médicaux, Focus sur des Actes de Radiologie17

Un référentiel, qu'il soit pour des médicaments, des actes de Biologie ou de Radiologie, a une double fonction :

- Il permet au Médecin qui prescrit de retrouver la dénomination exacte recherchée en tapant les premières lettres du médicament ou de l'acte. Le logiciel propose alors une ou plusieurs réponses. Le Médecin n'a plus qu'à valider son choix (c'est le principe de l'écriture intuitive que l'on retrouve dans l'écriture des SMS) ;

A titre d'exemple, le Médecin tape les lettres (Figure II.17):

- SPASF, le référentiel Thériaque propose 5 références du médicament Spasfon ;
- CARDIO, le référentiel propose 6 références soient 4 médicaments différents.

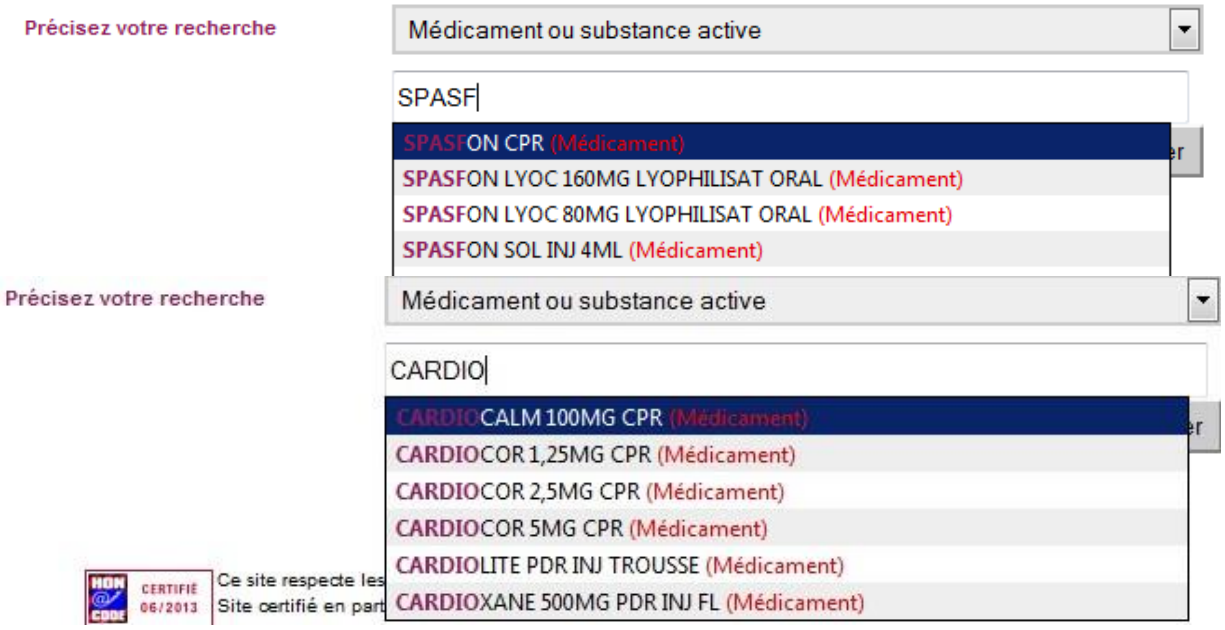


Figure II.17 : Extrait du référentiel Thériaque - illustrations de l'écriture intuitive dans la recherche d'un médicament

- Il permet au médicament ou à l'acte d'être codé dans le logiciel (Figure II.18 pour exemple : Code LHQH002-Scanographie de plusieurs segments de la colonne vertébrale, avec injection intraveineuse de produit de contraste). Ce code peut être ensuite exploité pour la facturation du séjour du patient.

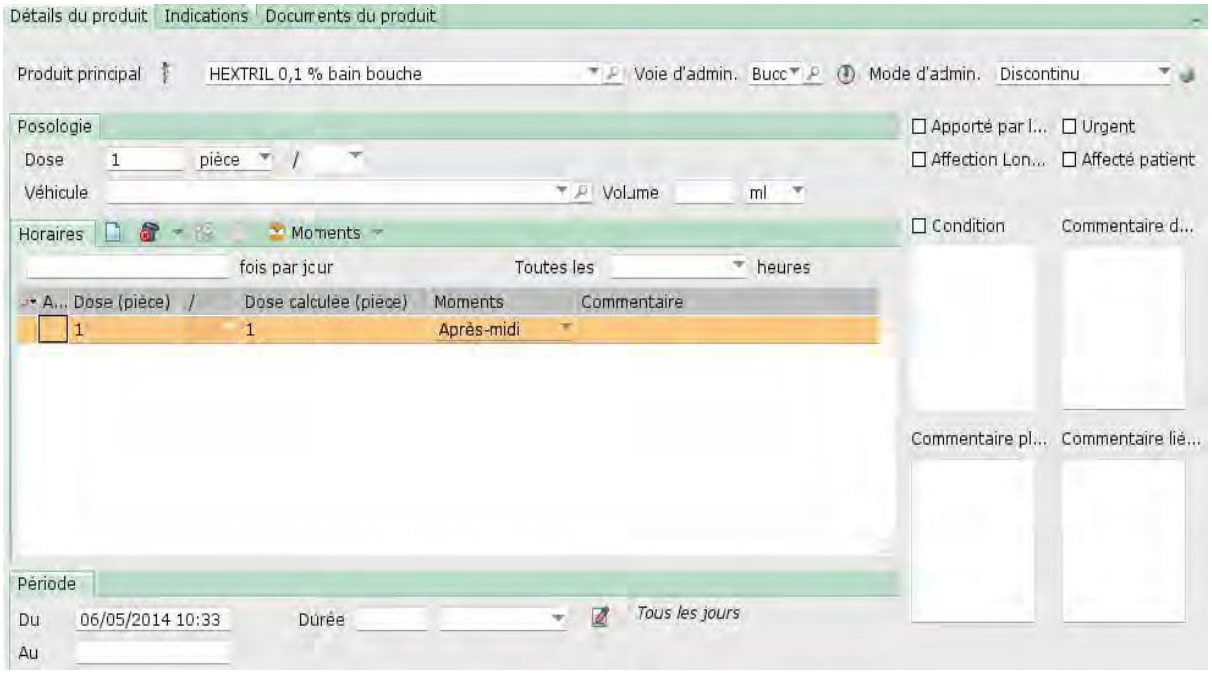


Figure II.18: Exemple d'écran de prescription, Orbis Agfa Healthcare

8.7.6. La mise en œuvre des conditions d'interopérabilité

Dans la mesure où les systèmes d'information en santé font intervenir un grand nombre d'acteurs (professionnels de santé, établissements de santé, éditeurs de logiciels, sociétés de service, administration…), la mise en œuvre des conditions d'interopérabilité doit être organisée pour que celle-ci soit effective. C'est l'objet des référentiels d'interopérabilité.

En premier lieu, la définition d'un référentiel général d'interopérabilité qui déterminera les règles permettant d'assurer l'interopérabilité des systèmes d'information des administrations de l'Etat, des collectivités territoriales, des établissements publics à caractère administratif et des organismes de sécurité sociale. Ces règles portent notamment sur les répertoires de données, sur les normes et les standards.

Le référentiel général d'interopérabilité devra ensuite être décliné pour le domaine de la santé. D'ailleurs étendu l'obligation du respect du référentiel d'interopérabilité spécifique à la santé à tous les acteurs du système de santé (professionnels de santé, établissements, hébergeurs de données de santé).

Ce dispositif pour le domaine de la santé doit encore être finalisé :

- les règles minimales d'interopérabilité, limitées dans un premier temps aux fonctions nécessaires à la mise en œuvre du dossier médical partagé, n'ont pas encore été publiées;
- les modalités de vérification du respect de ces règles restent à définir ainsi que les dispositions relatives aux sanctions en cas de non-respect.

9. Les apports attendus de l'informatisation du système de santé

Les avantages attendus d'une informatisation généralisée du secteur de la santé d'un pays ont été identifiés par les pouvoirs publics et, de plus en plus, par les professionnels de santé eux-mêmes.

9.1.1. Du point de vue du patient

La relation médecin-malade doit pouvoir être améliorée par le recours à des systèmes d'information de plus en plus intégrés.

Ainsi, dans le cadre de l'informatisation des dossiers médicaux, les informations concernant le patient (antécédents médicaux et familiaux, résultats des examens réalisés, traitements suivis, compte-rendu d'hospitalisation) devraient facilement être disponibles pour le médecin traitant.

En outre, les professionnels de santé devraient pouvoir améliorer la qualité de leur

diagnostic par le recours à des outils d'aide à la décision en ligne et par le développement de la communication entre professionnels (développement de la télémédecine notamment).

Enfin, s'agissant de la continuité des soins au malade, le « Réseau santé social » auquel les médecins accèderont par la carte de professionnel de santé (CPS) devrait permettre la transmission de lettres de sortie de l'hôpital, de résultats d'examens complémentaires ou la prise en charge commune par un réseau de professionnels de santé et la diffusion à tous d'un protocole de soins. De même, l'informatisation des données de santé doit permettre d'améliorer la prise en charge des patients, notamment en situation d'urgence.

9.1.2. Du point de vue des professionnels de santé

L'informatisation du secteur de la santé doit pouvoir améliorer l'exercice de la médecine par les professionnels de santé, en leur apportant des outils utiles à la prise de décision (base de données sur les médicaments, accès à des référentiels de bonne pratique), un accès à des connaissances médicales validées et en développant la possibilité de travail en équipe et en réseaux. En effet, les professionnels de santé doivent pouvoir communiquer entre eux, de manière sécurisée, au sujet d'un patient et de l'organisation des soins.

En outre, le développement de réseaux ville-hôpital et de la communication entre la médecine de ville et le secteur hospitalier est un enjeu crucial de l'informatisation du secteur de la santé.

9.1.3. Du point de vue de la santé publique

L'informatisation du secteur de la santé doit également permettre d'améliorer les politiques collectives de santé publique, par le biais d'une meilleure protection de la santé contre les dangers épidémiques, environnementaux ou liés aux produits de santé, d'une part, d'une meilleure connaissance de l'évolution des maladies transmissibles et de l'état de santé de la population, d'autre part.

De ce point de vue, le bénéfice attendu de l'informatisation du système de santé est le renforcement du dispositif de veille sanitaire grâce une circulation verticale rapide de l'information ainsi qu'une meilleure connaissance épidémiologique de la population.

10. Conclusions

Les systèmes d'informations hospitaliers, développes au cours des 40 dernières années, ont démontré leur efficience et fait preuve d'une maturité suffisante pour envisager leur généralisation. Se pose dans ces conditions la question de la ou des stratégies les plus

adaptées pour choisir, déployer et assurer la maintenance d'un SIH intègre en prenant en compte les dimensions techniques, financières et organisationnelles d'un tel projet.

Dans un contexte économique difficile, une décennie peut représenter la bonne échelle de temps pour mener à bien un tel projet. L'informatisation des plateaux techniques reste considérée comme l'étape préalable à la mise en œuvre d'un dossier patient partage et des outils de prescription. Elle doit être suivie par la mise en œuvre d'un dossier patient électronique partage puis des outils de prescription d'actes et de gestion des rendez-vous.

L'informatisation du dossier médical est possible et certainement utile pour améliorer la continuité des soins. Le dossier médical regroupe plusieurs modules, les communément utilisés sont : L'identification du patient, le dossier médical du patient, le dossier de soins, la prescription, la gestion de la Pharmacie à Usage Interne. Tous ces modules doivent être interconnectés et gérés par un SIH.

SERIE de TD N°2

Exercice :

Un hôpital de 700 lits dispose des applications informatiques suivantes : un système de gestion administrative des patients (identité/mouvements, facturation) développé en interne, deux systèmes de gestion de laboratoires (biologie, d'une part, bactériologie et immunologie de l'autre) déversant leurs résultats sur un serveur de résultats développes tous trois en interne, un logiciel de gestion de la pharmacie permettant la saisie des prescriptions thérapeutiques, un système de gestion de la radiologie avec son outil propre de gestion des rendez-vous, un logiciel spécialise de gestion des urgences. Proposez une stratégie de poursuite de l'informatisation à 5 ans. Quels composants faut-il conserver, supprimer ou envisager de supprimer à terme ?

Réponse :

La situation décrite dans cet exercice est une situation fréquente dans les hôpitaux avec un début d'informatisation du circuit administratif et des principaux plateaux techniques. Le développement en interne d'applications d'informatique hospitalière est progressivement abandonne remplace par l'achat et le paramétrage de progiciels intègres. Les sous-ensembles applicatifs pouvant être amenés à disparaitre à court ou moyen termes sont les suivants : le module de **gestion des identités** remplace par le composant **identité/mouvement du SIH**, **le serveur de résultats et le logiciel des urgences** remplaces par **le dossier patient intégré**, le composant **gestion de rendez-vous de radiologie** remplace par un composant **générique de gestion des ressources de l'hôpital**, la partie prescription du **logiciel de pharmacie** remplacée par un **composant général de gestion des actes**. Le remplacement des deux logiciels internes de gestion des laboratoires par un produit industriel conforme aux normes d'échange internationales **(HL7)** doit être effectue au plus tôt. Une fois une solution retenue pour le système d'information clinique, le déploiement informatique est habituellement planifie en deux ou trois phases. Pendant le déploiement d'une phase, le paramétrage des progiciels pour les phases suivantes peut être effectue en parallèle. Les quatre grandes étapes ci-dessous constituent un exemple de stratégie validée. Le calendrier réel doit bien sur tenir compte du choix exact de la solution retenue et du niveau d'investissement, puis adapte en fonction des retours des utilisateurs dès les premiers déploiements.

- Etape 1 (12-18 mois) : définition de la structure d-e-Gouvernance, mise en place d'une équipe de projet chargée de la réalisation du plan d'urbanisation, de la rédaction du cahier des charges et du dépouillement des offres. Choix d'une stratégie de gestion des infrastructures informatique (en interne ou externalisée sur un site sécurisé et agrée).

- Etape 2 (6-12 mois) : paramétrage des fonctions de base du SIH (identités/mouvements, dossier patient intégrant les données des plateaux techniques). Formation des utilisateurs aux fonctions de bases.
- Etape 3 (12-18 mois) : déploiement des fonctions de base. Paramétrage d'un second ensemble de fonctionnalités (prescription des actes simples et composes, rendez-vous). Formation des utilisateurs aux fonctions avancées. Corrections des bogues sur les fonctions de base.
- Etape 4 (12-18 mois) : déploiement de la seconde phase. Paramétrage de fonctions avancées (par exemple protocoles complexes, outils d'aide à la décision, dossiers de spécialités). Correction des bogues sur les fonctions avancées.

Certains systèmes d'information cliniques intègrent leur propre outil de gestion de laboratoires (approche horizontale décrite dans ce chapitre). Si tel est le cas, paramétrage du système du système de laboratoire sera concomitant de celui du dossier patient (Etape 2). Il en est de même du système de communication et d'archivage des images (PACS). Le déploiement des fonctions du PACS peut être planifie au cours des étapes 3 et 4 du projet.

QCM :

1. Concernant le dossier médical, papier ou électronique, quelle est la (ou quelles sont les) proposition(s) exacte(s) ?

a) Le dossier médical inclut notamment les notes personnelles du médecin. Ces notes peuvent faire référence à la vie privée du patient. **VRAI**

b) Le dossier médical peut être accepté comme élément de preuve par un tribunal. **VRAI**

c) Le dossier médical peut se présenter sous la forme d'un dossier patient unique ou, dans certains établissements, sous la forme de plusieurs dossiers séjour. **VRAI**

d) Sur les prescriptions médicales, lorsque le nom et la date de naissance du médecin prescripteur sont lisibles, sa signature devient facultative. **FAUX**

e) Le dossier médical peut inclure des dossiers spécialisés, comme le dossier d'anesthésie. **VRAI**

2. Concernant le Dossier informatique du patient, quelle est la (ou quelles sont les) proposition(s) exacte(s) ?

a) Il sert en général plusieurs objectifs (partage d'information, stockage d'information, enseignement, traitements statistiques...) **VRAI**

b) Il est constitué plusieurs dossiers par patient partagé par tous les médecins inscrits à l'Ordre **FAUX**

c) Il contient des éléments de natures différentes (images, lettres, compte-rendu, résultats d'analyses...) **VRAI**

d) Il est détruit à la sortie du patient **FAUX**

1. Introduction

La révolution numérique est en marche et investit les hôpitaux. En effet, la Consultation simultanée d'images radiologiques, le diagnostic assisté par ordinateur, le suivi des patients, dossier médical en ligne, tout ça est devenu possible grâce à la technologie de l'information. Le numérique est en train de révolutionner l'univers de la santé et ses possibilités sont immenses. Comme il représente un formidable outil de gestion des coûts financiers.

Le domaine de santé le plus concernée par les progrès technologiques est celui de l'imagerie médicale. Ce dernier a connu les évolutions technologiques les plus fulgurantes par l'avènement de la 3D et la modélisation. Mais ces évolutions créent de nouveaux besoins liés à l'augmentation de la production d'images dont il faut faciliter l'archivage et la circulation, au même titre que la lecture et l'analyse.

Afin de suivre le développement technologique connu dans le domaine d'imagerie médical. Les hôpitaux commencent à s'informatiser, la radiologie numérique se substitue à la radiologie analogique. Pareil les autres services comme, la cancérologie, la cardiologie ou encore la neurologie, sans parler des autres spécialités médicales, ne peuvent s'envisager aujourd'hui sans informatisation. Le gros challenge pour les hôpitaux actuellement est la mise en place d'un système d'information permettant l'échange, l'archivage et de partage de données numérisées, et en particulier des images. Ces systèmes appelés PACS (Picture Archiving and Communication System) pour les images ou RIS (Radiology Information System) pour les autres données.

Beaucoup de chemin reste à parcourir pour généraliser les PACS et les mutualiser au niveau régional et national, mais plus personne ne conteste aujourd'hui l'intérêt de supprimer les vieux clichés d'antan. Ce chapitre vous invite à découvrir les réseaux de partage d'images numériques, leurs avantages pour les établissements de santé et les patients et leurs enjeux.

2. L'imagerie médicale, au cœur de la pratique de santé

L'imagerie médicale est le domaine qui a le plus contribué au progrès médical depuis 20 ans, s'imposant comme un pivot du développement futur de la médecine. D'année en année, la proportion d'images médicales obtenues sous forme numérique croit considérablement et constitue la base du diagnostic clinique. **L'imagerie intervient à tous les niveaux du processus de soin :** dépistage, diagnostic**,** bilan pré-thérapeutique, aide à la décision, planification et orientation des traitements et suivi de l'efficacité de certains traitements**. Son usage optimise la prévention,**

l'accompagnement et le suivi d'un nombre croissant de pathologies. Par exemple :

- **En cancérologie**, l'IRM corps entier et le TEP sont les examens clés du diagnostic, du bilan d'extension pré-thérapeutique et du suivi de la recherche de récidive dans la plupart des cancers.
- Pour les **pathologies vasculaires et cardiovasculaires**, les scanners et l'IRM cardiaque font référence.
- **En neurologie** : l'IRM est nécessaire pour de nombreuses pathologies, notamment pour la **maladie d'Alzheimer**.
- Dans la prise en charge des urgences, un plateau d'urgence ne peut accueillir des patients sans un accès privilégié et dédié au scanner.

Les progrès technologiques en matière d'imagerie, ainsi qu'en communication facilitent et optimisent les échanges des images entre les différents praticiens. Les images sous forme de données numériques ont permis le développement de stations et consoles de visualisation et d'interprétation sur écran. Cela a entraîné une utilisation croissante des techniques de traitement et d'analyse automatiques des images.

L'acquisition des images sous forme numérique s'applique à différents équipements : IRM, scanner, scintigraphie, angiographie, échographie, radiographie conventionnelle (plaques au phosphore et capteurs), mammographie…L'image produite par ces modalités doit être conforme au standard **DICOM**. Dans le cas contraire, des solutions de rehaussement (hardware et/ou software) sont généralement disponibles.

Des équipements réseautiques sont nécessaires, non seulement pour optimiser l'usage des images mais aussi pour permettre leur bonne utilisation.
A cet effet, tout un système de réseau et d'archivage doit être mis en place afin de bien mener la gestion du **dossier d'imagerie** qui un module important dans le **dossier médical du patient**.

3. Les réseaux d'imagerie médicale

Les réseaux d'imagerie ont plusieurs objectifs :

- Interconnecter les différents équipements d'imagerie médicale pour réduire les opérations manuelles et optimiser la circulation des images, de leur production à leur interprétation.
- Transférer rapidement les images à l'intérieur et à l'extérieur des établissements pour accélérer et optimiser les processus diagnostiques et thérapeutiques, améliorer la qualité des soins et assurer un meilleur suivi des patients.

- Partager l'imagerie avec les différents médecins en charge du patient tout au long de sa maladie et dans le cas de maladies chroniques, biologique ou thérapeutique.
- Archiver de façon rationnelle et durable les images réalisées pour en disposer de façon rapide à la demande des équipes en charge du malade.

Deux éléments interviennent pour structurer un réseau d'imagerie : **le RIS et le PACS**.

1. **Le RIS** - Radiology Information System ou Système d'Information en Radiologie - **est un système réseautique de gestion des activités d'un service radiologique.** L'optimisation de ce système nécessite l'utilisation d'un PACS (Picture Archive and Communication System) pour permettre la diffusion des demandes de médecins, des images et des comptes rendus, le RIS ne diffusant que sur les stations d'interprétation dans les services de radiologie.
2. **Le PACS** - Picture Archiving and Communication System - **est un système de gestion électronique des images médicales** avec des fonctions d'archivage, de stockage et de communication rapide. Ses capacités sont très supérieures à tous les équipements existants et offrent des perspectives de développement des réseaux d'imagerie à grande échelle et sur le long terme. **Il optimise le RIS dont il est le complément indispensable pour la gestion des images.**

Le RIS et le PACS ont une relation directe avec les différentes modalités d'imagerie. Les modalités d'imagerie sont des équipements technologiques capables de créer, modifier et traiter des images. Dans le monde médical, les soignants parleront de modalités d'imagerie en faisant référence aux outils d'acquisition des images, tels que les scanners, les IRM, etc. Or, en termes de modalité d'imagerie, il y a aussi les outils de traitement et d'archivage des images, tels que les consoles de post-traitement dédiées, les serveurs d'application, les graveurs de CD/DVD, ou encore les PACS, etc. Sous le terme « modalité d'imagerie », il faut donc considérer l'ensemble des outils de l'imagerie.

4. Le système d'information de radiologie (RIS)

Le système d'information de radiologie ou SIR, communément appelé le RIS (pour Radiology Information System), C'est un logiciel qui est un outil de production du service d'imagerie médicale qui gère et fiabilise l'ensemble des données du dossier du patient, de la prise de rendez-vous jusqu'aux statistiques d'activité. Ces fonctionnalités sont très importantes dans le cas où l'hôpital n'est pas équipé d'un système d'information hospitalier.

Les multifonctionnalités et multi-optionnels composant ce logiciel permettent de définir et de gérer de manière spécifique des profils utilisateurs différents (prescripteurs, radiologues, manipulateurs, secrétaires).Composé d'une partie gestion et d'une partie image, il permet au service du patient et

des praticiens :

- De gérer le dossier du patient et son historique
- De consulter l'historique commun des patients de n'importe quel endroit du réseau
- De conserver sur plusieurs années tous les évènements entrant dans le dossier patient
- Aux médecins de produire des comptes-rendus en utilisant la puissance de la dictée numérique afin de numériser le circuit des comptes rendus
- De produire, d'archiver et de diffuser des comptes-rendus
- L'indexation des images au dossier du patient et la gestion de l'historique complet sur une durée de plusieurs années
- La diffusion des images produites par le service dans l'hôpital
- De stocker les images issues du scanner, IRM et autres modalités d'imageurs au format DICOM

Nous détaillons ici les différents partie de gestion d'un SIR , qui nous pouvons définir par un Système informatique qui permet d'automatiser les workflows et de gérer les informations manipulées par le service de radiologie :les patients, les ordonnances, les examens, les ressources, les consommations (médicaments, produits, …),les comptes-rendus ...

- Gestion du parcours du patient = « Workflow » = Listes de travail

(accueil, en salle, examen fait, examen à interpréter, examen dicté, examen à signer, examen validé, examen envoyé…)

- Gestion des demandes d'examen (et correspondants)
- Gestion des informations spécifiques à la radiologie (Produits injectés, Contre-indications, Dose reçue, Cotation des actes,…)
- Gestion des compte-rendus (base de données) :(Dictée, saisie, frappe, ventilation, stockage)
- Gestion de l'activité

Nous mentionnons ici Les différents acteurs qui participent dans l'organigramme de SIR :

- Réceptionniste
- ATM (Assistant Technico-Médical)
- Médecin radiologue
- Secrétaire
- Gestionnaire
- Service Facturation.

4.1. Les fonctions d'un RIS de la prise de RDV à l'envoi du CR

- Prise de rendez-vous, qui se fait par le poste de réceptionniste avec les fonctions suivantes :
- Planification des examens par la recherche d'un créneau horaire dans l'agenda par salle, par jour / semaine, …
- Proposition automatique de plages horaires
- Accueil et information des patients (Déroulement de l'examen ;Conditions (jeun, …) ; Contre-indications (grossesse, …)
- Prise en compte des indisponibilités : personnel, matériel, jours de garde, jours fériés, …(Gestion des collisions)
- La plage allouée dépend du type d'examen (Unités de soins ou Consultations)
- Impression d'étiquettes, scanner les ordonnances, …
- Communication bidirectionnelle avec le logiciel administratif de l'hôpital (HIS) (Données administratives du patient)
- Gestion du dossier radiologique du patient, qui se fait par poste ATM
- Visualisation des anciens examens et anciens comptes-rendus du patient
- Visualisation des données médicales permanentes (Allergies ; Pace maker ;Événements, ...etc)
- Doses Rx reçues
- Gestion des ressources (personnel, salles, …)
- Gestion des examens radiologiques, qui se fait par poste ATM
- Codification examen
- Information examen (Incidences, côtés, …
- Saisie des consommables (Films, médicaments, produits de contraste, matériels spécifiques (cathéters) ...
- Événements, remarques
- Référentiel métier
- Protocoles réalisation d'un examen
- Consultation des critères de réussite d'un examen
- Visualisation des surveillances à réaliser pour un examen
- Suivi des consommations par poste ATM
- Gestion des comptes-rendus d'examens

Possibilité d'interprétation sur base d'une liste personnelle

• Gestion statut des comptes-rendus (Provisoire, Validé, Á valider, Á corriger)

• Gestion de « templates » de compte-rendu

» Données patient, médecin prestataire

» Date, type d'examen

» Intégration d'images

• Création des comptes rendus (Dictée digitale ; Reconnaissance Vocale)

• Utilisation de thésaurus médicaux

• Impression et envoi au prescripteur et médecins conseillers

» Envoi automatique par email

- Edition et impression de documents de travail (Etiquettes ; Listes de travail) par poste réceptionniste
- Production de statistiques
- Recherche médicale

4.2. Objectif d'un Système d'information en Radiologie :

Le but principale de SIR est de Faciliter la gestion et l'organisation du service de radiologie par :

• Simplification des scénarios de travail (workflows) au niveau du service de radiologie

• Disponibilité des données administratives et médicales

• Vue détaillée des activités du service de radiologie

• Rationalisation de la gestion du service de radiologie

• Décentralisation du traitement des données c.à.d. ' Postes de travail répartis dans les différents services ou l'accès simultanés aux infos par les Cahiers de RDV pour chaque patient et pour chacun des acteurs (agenda électronique des salles)

• Gestion des ressources telles que le personnel et les salles

• Statistiques automatisées par exemple le nombre d'examens par année par salle

5. Définition du PACS

Le PACS ou **P**icture **A**rchiving and **C**ommunication **S**ystem est un système de gestion électronique des images médicales incluant des fonctions de stockage, d'archivage et de communication via un réseau des images reposant sur le standard **DICOM (Voire Chapitre 4)** et donc le traitement à distance ou en réseau local avec des ordinateurs disposant de moniteurs à haute définition pour la visualisation des examens effectués en radiologie. Il rend possible le cycle suivant de gestion des images médicales :

- Acquisition sur les producteurs d'images.
- Archivage électronique d'images et de données médicales élevées.
- Communication via un réseau rapide et consultation.
- Traitement et interprétation sur des stations de consultation.

Ce type de système est une solution permettant d'enregistrer de manière numérique des images radiologiques, et de visualiser sur un moniteur, de les transmettre et de les archiver tout en éliminant les images traditionnelles sur film. Cette technologie a atteint un certain niveau de maturité et connais un essor depuis quelques années dans les hôpitaux à travers le monde.

5.1. Principe, objectifs et avantages de PACS :

5.1.1. Principe de PACS:

Un PACS peut être imbriqué dans le **S**ystème d'**I**nformation **H**ospitalier ou SIH de l'établissement et prétendre à une totale interaction avec le **S**ystème d'**I**nformation en **R**adiologie ou SIR. Ces connexions entre différents systèmes ont pour but l'échange de données primordiales au bon fonctionnement de l'ensemble du réseau. Par exemple, le PACS, réellement dédié à l'image, puise les informations pertinentes du malade (données démographiques) dans le SIR. Cela permet la réconciliation automatique d'une image à une entité patiente. Il y a identification et mise en correspondance de l'image avec le patient. Cependant un PACS peut fonctionner sans SIR ni SIH mais ses avantages sont considérablement amenuisés : il n y a plus de rapprochement entre les images et le dossier patient correspondant.

Ces échanges de données SIH/SIR/PACS ont bien d'autres vertus comme le suivi de l'avancement d'un examen, la planification de rendez-vous, la gestion des comptes rendus, le suivi du **D**ossier **M**édical **P**atient (DMP) **.** Ils doivent être sécurisés au niveau du système et des accès. La clé de voûte de l'ensemble du système est l'identification unique du patient

Le schéma fonctionnel suivant illustre de façon concrète les interactions entre les différents systèmes d'information :

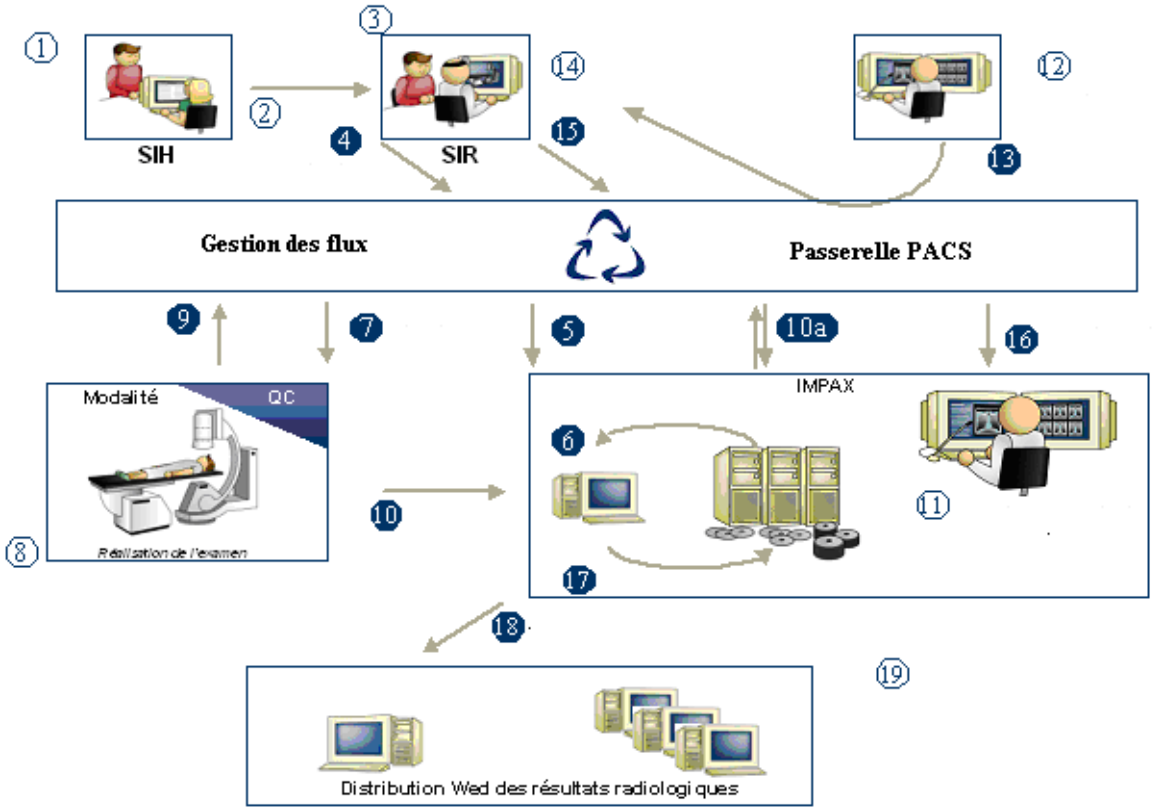


Figure III.1 : Schéma des étapes du cycle examen d'imagerie médicale dans un système SIH/SIR/PACS coordonné. (Source : Agfa)

Les étapes bleu concernent directement le fonctionnalités d'un PACS : 1) Admission du patient, 2) Admission Sortie Facturation Transfert, 3) Examen demandé et planifié, 4) et 5) notification du statut de la demande, 6) pré chargement des images, 7) Liste de travail vers les modalités (Worklist), 8) réalisation de l'examen, 9) notification du statut de la demande, 10) stockage des images, 10a) vérification, 11) réalisation du diagnostic et création du compte-rendu, 12) transcription du compte-rendu, 13) compte-rendu, 14) compte-rendu approuvé, 15) et 16) notification du statut du compte-rendu, 17) archivage des images vers le stockage à long terme, 18) images transmises au serveur WEB, 19) consultation).

5.1.2. Objectifs de PACS :

- Collecter, stocker et archiver des images ou vidéos numériques et des données patient à partir de l'ensemble des modalités productrices (Scanner, IRM, échographes …) connectées au PACS mais aussi par réseau, CD/DVD et numérisation de films.
- Assurer la conservation de ces images digitales sans risque de perte de dossier ou de détérioration des images selon des contraintes réglementaires précises (durée de conservation, taux de compression **(voire chapitre 5)**.
- Fournir un accès rapide, facile et sécurisé à l'ensemble des images et données, uniquement

pour des personnes autorisées et depuis n'importe quelle station PACS reliée au réseau (intranet, point à point …).

- Permettre le post-traitement local des images, la comparaison d'examens, la visualisation multi modalité et le recalage d'images et ainsi améliorer les conditions d'interprétation.
- Permettre l'accès simultané à la même image depuis plusieurs stations PACS.
- Permettre la sélection d'images pertinentes (Key object selection DICOM ou Key Im Note IHE).
- Associer un compte rendu aux images et suivre l'avancement d'un examen grâce aux SIR.
- Permettre la diffusion des images à l'extérieur de la structure hospitalière : aux patients par CD, aux médecins généralistes par télé radiologie, CD ou Internet, aux autres établissements hospitaliers par réseau informatique (VPN) …
- Intégrer les images dans des bases de données nationales (réseau de santé sociale, Wanadoo santé …).
- Suivi de la dosimétrie patient.
- Suivi des flux d'activité par le biais de statistiques.
- Traçabilité du dossier, des examens, des intervenants (support de preuve juridique).
- Accessibilité 24H/24 et 365jours/365 aux images.
- Diminuer le coût de production des images radiologiques, film, produits chimiques, maintenance.
- Diminuer le temps médecin, radiologues et manipulateurs, brancardiers, temps de transport et de recherche de dossier en diminuant les déplacements.

5.1.3. Les avantages du PACS

Pour les patients, le PACS **est** un gage de qualité des soins supplémentaire à tous les niveaux de la prise en charge (du diagnostic au suivi thérapeutique). Le dossier image intégré au dossier médical informatisé du patient est l'assurance d'un meilleur suivi. Rapidité d'accès aux informations, vision d'ensemble, concertation et échanges facilités pour les cliniciens, renforcent la qualité du diagnostic et de la décision médicale. Parallèlement, le risque de perte ou de dégradation des films ou des CD- ROM disparaît. Enfin, il n'a plus besoin de porter ou faire suivre son dossier à chaque consultation.

Pour les radiologues et médecins **cliniciens**, le PACS **facilite l'interprétation** dans la mesure où le dossier radiologique est complet et mis à jour au fur et à mesure des examens et interventions et en ligne 24h/24 et 7j/7. C'est également un outil d'aide à la prise de décision

du fait de la facilité et de la rapidité des échanges entre médecins qu'il induit, en interne ou à l'extérieur. La concertation peut se faire à tout moment, même en consultation, chaque médecin ayant accès directement et simultanément aux images.

Les manipulateurs, quant à eux, **gagnent un temps précieux qu'ils peuvent consacrer aux patients**. De plus, l'accès aux examens antérieurs facilite la reproductibilité des examens successifs pour la surveillance. Les secrétaires n'ont plus de dossier radiologique à gérer et sont donc plus disponibles pour mieux organiser leur travail et les archivistes voient leur carrière évoluer.

D'un point de **vue économique**, le PACS représente une **économie considérable sur le coût des films:** en 2003, les frais de films de l'Institut Curie (en France) s'élevaient à 500 000 euros par an. En 2007, ils n'étaient plus que de 20 000 euros (principalement pour les mammographies). En outre, les frais de maintenance sur les reprographes ont chuté drastiquement. A cela s'ajoutent des avantages écologiques évidents. Ces économies sont néanmoins en partie réduites par l'ensemble des coûts de fonctionnement du PACS (maintenance, renouvellement matériel, coûts d'administration).

Du point de vue de l'organisation du travail, le « sans film » **a fait évoluer les pratiques professionnelles** en facilitant la gestion des images, l'ensemble des données patient étant reliées en ligne, et ouvert de nouvelles perspectives pour les manipulateurs et les archivistes.

5.1.4. Les principales fonctions du PACS sont :

- Le stockage de tous les examens radiologiques.
- La gestion et la mise en réseau de toute la production d'images numérisées avec un accès simultané à la même image à partir de n'importe quel poste de travail.
- L'archivage, en assurant la conservation des images numériques sans risque de perte ou de détérioration de leur contenu.
- La consultation d'examens radiologiques sur des stations ou consoles de visualisation.
- Le diagnostic, en permettant la manipulation et le traitement local des images.
- Le partage et l'envoi d'images dans et en dehors du service ou de l'hôpital pour rendre l'accès facile et rapide à toutes les images pour tous les médecins concernés.
- L'échange d'informations administratives avec les systèmes informatiques radiologiques (RIS) et hospitaliers (SIH).

La fonction d'archivage assurée par le PACS est la condition pour utiliser au mieux les images en garantissant leur bonne conservation et leur accès rapide. Cette fonction permet une meilleure qualité de soins et est particulièrement cruciale pour les programmes de dépistage et la prise en charge des maladies chroniques.

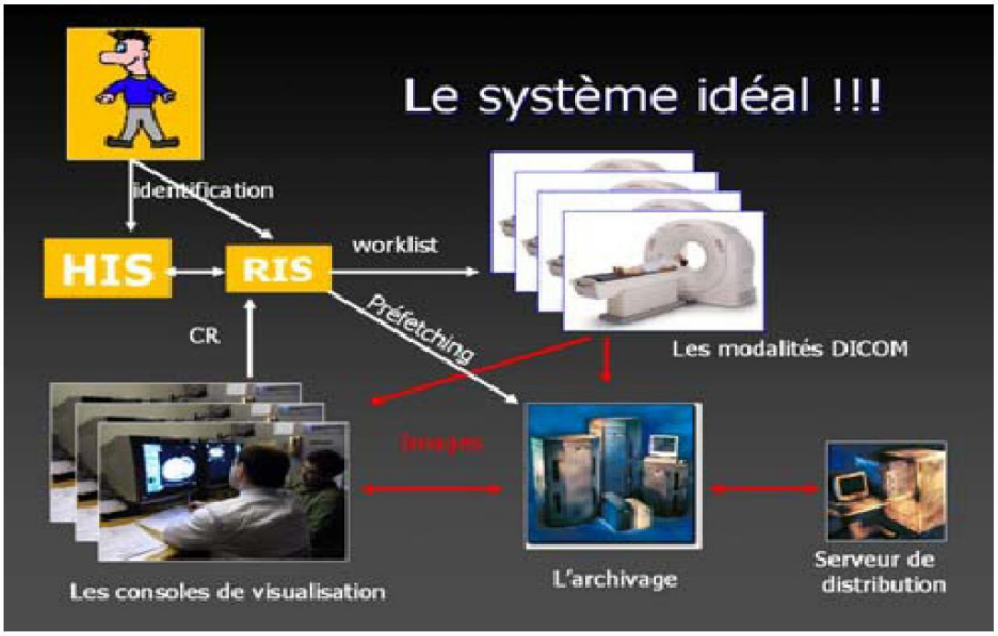


Figure III.2.les principale fonction du PACS

5.2. Le PACS pour archiver les images

D'une manière simplifiée, le PACS est un système informatisé qui centralise et qui gère l'acquisition numérique de tous les examens radiologiques, la consultation de ces images sur des consoles de visualisation, l'impression et l'envoi d'images à l'intérieur et en dehors de l'hôpital ainsi que l'échange d'informations administratives avec les systèmes informatiques radiologiques (RIS) et hospitaliers (SIH).

Le PACS représente l'évolution naturelle des nouvelles technologies numériques vers un environnement global numérique où les activités basées sur le film sont progressivement remplacées par leur équivalent numérique pour aboutir à une pratique sans film. Il est le sous ensemble du système d'information hospitalier (SIH) permettant de collecter, stocker et archiver des images dans une banque d'images accessible de n'importe quel point de l'hôpital par tous les professionnels concernés, permettant ainsi l'échange optimisé de ces informations.

5.2.1. Différence entre le stockage et l'archivage

Le stockage des données est l'enregistrement des données sur un support physique, tel qu'un disque dur (quel que soit son type), une clé USB, une bande magnétique, etc. L'archivage de données consiste à les placer dans un système qui assure leur préservation, mais aussi leur sécurisation. Ainsi, les données conservent leur valeur, notamment légale. La modification des documents est interdite, de même pour leur destruction, sauf sous contrôle strict. Toute action effectuée sur le document est tracée.

5.2.2. Archivage

- **Archivage court terme**

C'est le dispositif qui permet de sauvegarder temporairement les images générées par l'ensemble des modalités. Un accès rapide aux images est rendu possible grâce à l'utilisation de dispositif appelé **RAID** (Redundant Array of Independant Disk).

La capacité d'archivage peut être calculée en fonction du nombre et le type d'examens à archiver ainsi que la durée moyenne d'archivage.

- **Archivage long terme**

Il utilise la technologie du Juke Box qui sauvegarde les images sur quatre types de médium :

- DLT, LTO (ruban magnétique),
- MOD (disque magnéto-optique),
- CD-R (Recordable Compact Disc),
- DVD (Digital Versatil Dics),

Le système est capable d'indiquer le contenu de chaque médium.

- **Calcul des besoins d'archivage**

Le nombre de GB requis dépend des paramètres suivants :

- Le type de modalité,
- Le nombre moyen d'images par étude et par modalité,
- Le nombre de pixels de chaque image,
- Le nombre d'étude par année,
- Le taux de croissance du volume d'examens.

Pour l'archivage des examens en ligne, il faut prendre en considération les éléments suivants :

- Le nombre d'examens à archiver par jour,

- Le pourcentage d'examens courants ayant des antérieurs,

- Le nombre moyen d'examens antérieurs par étude courante,

- La taille (MB) des examens antérieurs par rapport aux examens courants,

- Le pourcentage utilisé pour initier la suppression d'examens du cache (high water mark),

- Le taux de compression s'il y a lieu.

Exemple :

Comme exemple de calcul, considérons les hypothèses suivantes :

- Besoin de 90 jours d'examens en ligne pour une production de 10,7 GB/j,
- Technologie RAID 5 (chaque rangée est composée de 6 disques dont un pour la parité),
- Compression sans perte 2:1 et le high water mark est de 90%,
- 60 % des études courantes ont des examens antérieurs,
- 1,5 des études antérieures exige la même capacité d'archivage que les études courantes.

Calcul :

RAID = (10,7 GB/jour x 90 jours) +(10,7 x 0,6 x1,5) x 7 jours= 1030 GB.

En tenant compte du 6 ième disque de parité (1/6=16,7% d 'espace non utilisé pour le data) on obtient alors: (100-16,7)x0,9x1030 GB = 1367 GB.

Si on rajoute la compression (2:1), on aura 684 GB

5.3. Les normes, les standards, la règlementation et leurs contraintes

L'écueil de la mise en place d'un PACS est en particulier dû aux difficultés d'intégration et de communication dans le SIR ou le SIH, l'intégration et la compatibilité DICOM des modalités à connecter.

5.3.1. Les normes et les standards concernés :

La communauté scientifique et les sociétés savantes concernées se sont penchées sur le problème d'intégration et de communication entre divers systèmes d'information donnant naissance aux standards suivants sensés facilité ces associations :

- Standardisation du format des messages de communication selon ACR/NEMA.
- Standardisation des réseaux ouverts selon le modèle OSI de l'**I**nternational **S**tandard **O**rganism ou ISO.
- Standardisation de communication **H**ealth **L**evel **7** ou HL7 pour la gestion du compte

rendu et DICOM 3.0 pour l'imagerie médicale. Ces deux standards assurent aussi la gestion des listes d'examen (worklist) et la réconciliation image/patient.

Le principe d'IHE ou **I**ntegrating the **H**ealthcare **E**ntreprise (qui s'appuie sur les standards DICOM et HL7) vise à réunir les utilisateurs et industriels du monde médical afin d'identifier et de résoudre les problèmes liés à la communication des systèmes d'information particulièrement en imagerie. Il se base sur des séances de test de connectivité lors de rassemblements du type "Connectathon" et rédige des « Profils d'intégration » types à un appareil.

5.3.2. La réglementation concernée :

La réglementation est majoritairement dédiée au **D**ossier **M**édical **P**atient DMP, à la confidentialité des données médicales et à l'archivage des documents d'imagerie. Pour les raisons et les objectifs suivants :

- confidentialité des données patient,
- Suivi des soins,
- Droit d'accès du patient à son dossier médical,
- Défense des intérêts de l'établissement en santé et des patients lors de recours en justice grâce à l'apport de preuves,
- Base de données pour la recherche.

Les documents et textes impliqués sont :

- le Code de la Santé Publique : Art R1112-2 relatif à la conservation des images médicales dans le dossier médical.
- l'arrêté du 11 Mars 1968 relatif au délai de conservation des dossiers médicaux.
- la circulaire du 2 août 1960 relatif à la conservation minimale de 5 ans des clichés radiographiques.

La difficulté d'interprétation de la réglementation réside dans le fait que l'on distingue les supports d'archivage : clichés radiographiques, papier, supports informatiques, CD/DVD/DD … En outre, la loi du 13 Mars 2000 précise que le format électronique est admis en preuve au même titre que l'écrit.

Aujourd'hui, il n'existe pas de texte législatif concernant l'archivage sur supports informatiques. Cependant, considérant l'association des images au DMP on devrait s'acheminer vers une durée minimale de 20 ans de conservation. Un décret est en cours de

rédaction concernant le sujet.

Il est primordial de mesurer l'ampleur des conséquences de la définition de ces durées d'archivages dont vont dépendre les capacités de stockage à prévoir lors du déploiement du PACS. Cette décision aura un impact non négligeable sur la définition du besoin dans le cahier des charges au niveau du matériel dédié au stockage et à l'archivage.

5.3.3. Sécurité informatique

Compte tenu du transfert de données patient confidentielles, la sécurisation est un aspect primordial de la mise en place d'un réseau informatique comme le PACS. Une réflexion est nécessaire au niveau de **:**

- L'infrastructure réseau et la sécurité réseau informatique.
- La sécurisation des accès au réseau PACS : Firewall, antivirus, cryptage **(voir chapitre 6)** , Virtual Private Network, HTTPS (sécurisé), Cartes I.D et C.P.S …
- La sécurisation des accès aux consoles : login, mot de passe, biométrie.
- La possibilité ou non d'accès depuis le SIR au PACS et inversement.

5.3.4. Limites et difficultés

Le déploiement d'un PACS dans un établissement de santé est une révolution qui induit des bénéfices évidents. Malgré cela, il existe bel et bien des limites pour une telle installation.

La principale est le coût de la mise en œuvre (matériel, logiciels, câblage réseau, maintenance, sécurisation, upgrades, formations …) et du stockage (≈ 0,16 euros le Mo ou 3€ le CD)

Un tel projet engendre aussi des inconvénients d'ordre organisationnel :

1. Changer les habitudes de travail du personnel hospitalier,
2. Délimiter les capacités de stockage des données qui dépendent des objectifs médicaux, de la durée à couvrir (une hospitalisation, plusieurs consultations, un suivi sur 10 ans ?) et des obligations règlementaires (DMP : archivage sur 20 ans).
3. Déterminer judicieusement le périmètre du PACS : modalités à connecter, le nombre, le type et la localisation des stations PACS, les personnes autorisées et les droits d'accès à l'image …

6. Composants d'un PACS

- **Les stations informatiques intégrées au PACS :** stations d'acquisition de l'image (station IRM, Scanner..), stations de post-traitement de l'image, stations de lecture et de

diagnostic (PC médecins ou Internet), stations d'administrateur réseau et de serveur (2 technologies réseau ; 2 technologies logicielles).

Classiquement 2 ou 3 écrans

- 1 écran pour afficher le RIS (accès antériorité, dossier patient, dictée du CR)
- 1 ou 2 écrans pour afficher le ou les examen(s)

Figure III.3 Station PACS de post-traitement

- **Les modalités créatrices d'images :** IRMs, scanners, échographes, salles de radiologie, numériseurs, lecteurs CD…
- **Les modalités de duplication de l'image** : imprimantes, graveurs de CD/DVD, reprographes laser …
- **Les dispositifs de stockage et d'archivage de l'image:** baies de disques durs, armoires de disques optiques ou magnétiques …

Figure III.4 .A) robot de gravure CD/DVD ;B) Librairie de bandes magnétiques

- **Le câblage et les composants actifs du réseau informatique physique :** serveurs, routeurs, répétiteurs, interfaces DICOM …

7. Facteurs clés de réussite de mise en œuvre

- Prévoir un système évolutif et modulable : extension des modalités connectables, des capacités de stockage et du réseau physique.
- Uniformiser la solution sur l'ensemble des services et sites (Interfaces graphiques, types de consoles …)
- Former et assister les futurs utilisateurs (peur du changement de leur part et habitudes à modifier.
- S'assurer de la pérennité du fournisseur afin d'assurer la maintenance, les extensions du réseau, la connexion de nouvelles modalités ; le tout à long terme.
- Respecter les normes en vigueur.

8. Le marché existant

Les sociétés capables de fournir une solution PACS sont réparties selon quatre familles : les fournisseurs de modalités d'imagerie, les fournisseurs en télé radiologie, les fournisseurs de surfaces sensibles et les fournisseurs de solutions informatiques. Voici quelques exemples : Agfa (Système Impax), Etiam, GEMS (Système Centricity), Mc Kesson (Système Horizon Medical Imaging), Philips (Système iSite de STENTOR par rachat) , Fuji (Système Synapse), Global Imaging Online (Système DIAM 4), Kodak (System 5), Ferrania (Système Lifeweb One), Telemis, Cerner, Vepro, Siemens (Système Syngo Suite) …

9. Exemple de PACS

L'exemple du PACS suivant retranscrit le cycle de gestion des images dans un réseau de communication et de stockage et les applications possibles.

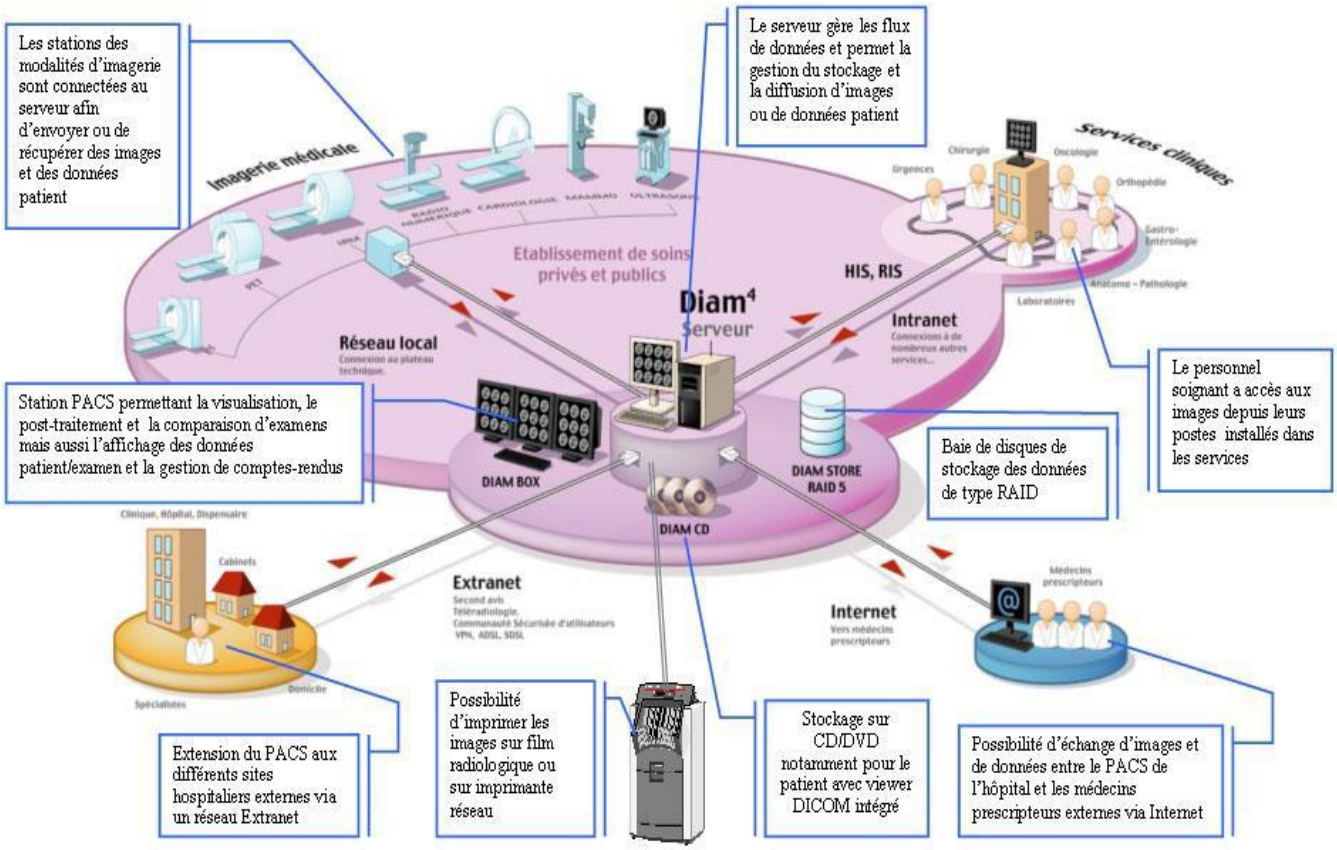


Figure III.5.Schéma d'organisation d'un PACS au sein d'une structure hospitalière

10. Le PACS : infrastructure et fonctionnement

10.1. Simplicité et facilité de mise en œuvre caractérisent l'infrastructure développée. Elle s'appuie sur un serveur principal de grosse capacité qui assure toutes les fonctions d'acquisition, d'indexation sur une base de données, de stockage et de diffusion des images vers les consoles d'interprétation et les cliniciens.

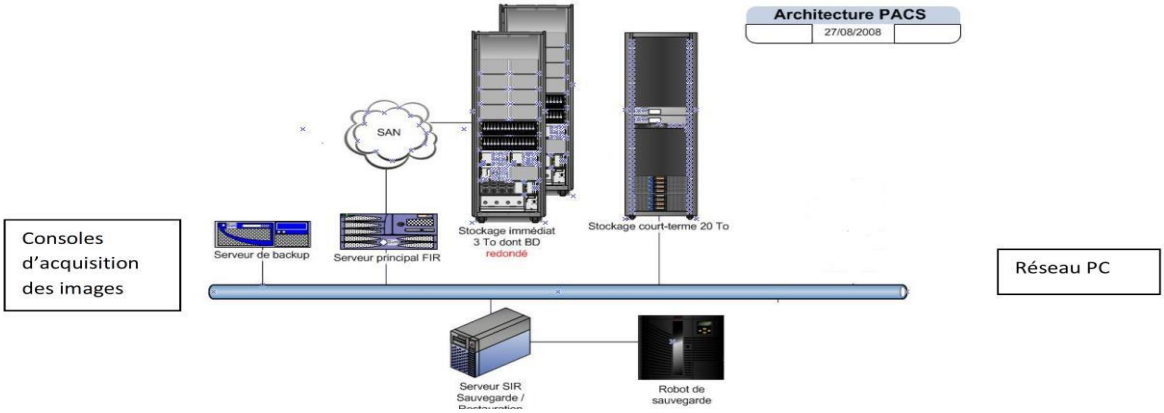


Figure III.6. Architecture PACS

10.2. Mode de fonctionnement :

- Envoi automatisé des images sur un premier serveur au moment où elles arrivent. Ce serveur principal reçoit les données saisies et diffuse les images.
- Indexation dans une base de données Oracle.
- Premier stockage sur un espace court terme d'accès très rapide qui contient 2 années d'examens en ligne.
- Archivage sur un second dispositif de plus grosse capacité qui sert également de stockage secondaire et permet d'avoir l'intégralité des examens en ligne avec des temps d'accès légèrement moins performants.
- Envoi des images vers un second serveur qui va piloter un robot de sauvegarde sur bandes pour une sauvegarde externalisée en cas d'incident technique majeur.

10.3. Des procédures spécifiques de crise en « mode dégradé » : ont été mises en place en cas de dysfonctionnement ou de panne majeure : utilisation du serveur back up éteint en temps normal, validation par les radiologues et conservation de tous les examens sur les consoles d'acquisition, impression des clichés sur films ou CD-ROM et archivage de la liste des examens du jour pour une vérification ultérieure.

10.4. Conditions du développement de ces réseaux

La transmission des images au travers d'un réseau nécessite une standardisation du format des messages et le respect des normes et protocoles établis par l'industrie pour assurer la cohérence et l'inter compatibilité des systèmes.

Ces normes sont :

- Le DICOM (Digital Imaging Communication in Medicine ; transmission d'imagerie médicale numérique).
- Le HL7 (Health Level 7) pour l'échange d'informations textuelles qui assure l'uniformité et la compatibilité entre les RIS et les SIH.
- Le IHE (Integrating the Healthcare Enterprise) défini pour assurer le partage d'informations entre professionnels de santé.

Le système RIS/PACS, intégré au SIH est un outil d'avenir pour constituer le dossier d'imagerie du patient. Il améliore la qualité des soins en favorisant la communication entre les praticiens autour de l'imagerie et plus généralement du dossier patient auquel l'image

doit être intégrée.

En améliorant la circulation des images dans la structure hospitalière, les réseaux d'imagerie intra hospitaliers permettront à terme une communication inter établissements et la réalisation d'un dossier patient.

Ces équipements sont fondamentaux. En Europe et dans le Monde, de nombreux pays l'ont compris et ont investi dans les réseaux d'imagerie RIS et PACS pour entrer en cohérence avec le développement des installations d'appareils d'imagerie multi-coupes (scanners, IRM..) dont ils optimisent les fonctionnalités, pour améliorer la qualité des soins et pour réduire les coûts de santé.

11. Conclusion :

Dans ce chapitre nous avons présenté le système le plus courant couramment utilisé dans la gestion des images médicales (PACS).Toutes ces applications ont pour objectifs de faire circuler et stocker plus vite, en plus grand nombre les flux d'information médicale. Le PACS permet d'arriver à faire de diagnostics moins, autant ou plus précis que dans le modèle de film traditionnel. Nous pouvons citer les bénéfices potentiels de l'implémentation d'un PACS dans le CHU de Tlemcen (par exemple) :

- Diminution du temps passé à chercher des images
- Augmentation de la productivité des technologues
- Délai d'initiation clinique réduit.
- Assurer un meilleur suivi des patients.
- Elimination de reprise d'examens (diminution du ratio de rejet d'image)
- Rapidité de service au patient accrue
- Plus grande qualité de soin
- Accès aux images plus facile
- Elimination des pertes de films
- Réduction des couts de gestion d'image, d'entreposage et de personnel
- Améliorer la qualité de vie au travail des employés d'un département de radiologie.
- Assurer la sécurité, de contrôlé les copies et de protéger l'intégrité des données.

SERIE DE TD N°3

Exercice 1 :

1. Calculer l'espace d'archivage dans un PACS pour une durée de 30 jours, pour des examens en ligne pour une production des images médicales de 12 GB/J.

Notons que la technologie Utilisé est RAID3 (chaque rangée est composée de 4 disques ou un pour la parité)

2. Calculer l'espace d'archivage dans ce système sachant que 50% des études courantes ont des examens antérieurs et que 2% des études antérieures exige la même capacité d'archivage que les études courantes.
3. Si nous utilise pour archiver ces images médicales une compression sans perte 2:1, quel est la valeur de l'espace d'archivage.
4. Le pourcentage utilisé pour initier la suppression d'examens du cache (high water mark) est de 80% ; calculer le RAID final pour cette structure d'archivage ?
5. Calculer le nombre de GB requit pour les mêmes hypothèses données précédemment, mais avec la technologie RAID 5. commentez les résultats obtenus ?

Solution

1. RAID = (12 GB/jour x 30 jours)*7jours=360*7=2520GB
2. Raid 3, en tenant de compte du 4 ieme disque de parité (¼=25% d'espace non utilisé pour le data) ,on obtient alors (100-25) x2520 GB = 189000 GB.
3. RAID avec compression = 189000/2=94500GB
4. RAID avec HWater mark de 80% ,on aura :94500*0.8=75600GB
5. RAID = (12 GB/jour x 30 jours) +(12 x 0,5 x2) x 7 jours= 30240 GB.

RAID 5, donc en tenant compte du 6 ième disque de parité (1/6=16,7% d'espace non utilisé pour le data) on obtient alors: (100-16,7) x0,8x 30240 GB = 2015193.6 GB.

Si on rajoute la compression (2:1), on aura 100756.8 GB

QCM :

Le système d'information en radiologie (SIR) permet :

A- D'automatiser les workflows et gérer les informations manipulées par le service de cardiologie **(FAUX)**
B- Gérer des informations des patients manipulés par le service de radiologie **(VRAI)**
C- D'envoyer et manipuler des images JPEG et TIFF **(FAUX)**
D- D'améliorer la qualité de soin par l'archivage des images DICOM sur une durée de 3 ans. **(FAUX).**

1. Introduction

Le domaine de l'imagerie médicale a beaucoup évolué depuis ses débuts au courant des années 1970**.** On a vu au cours des années l'émergence de plusieurs modalités (rayons X, ultrasons, résonnance magnétique...) utilisées dans divers services de la médecine. Cette évolution a inévitablement attiré les manufacturiers d'équipements électriques et électroniques à s'intéresser aux équipements médicaux car ils voyaient là un marché prometteur pour l'avenir. Chaque constructeur offrait donc une large gamme d'équipements.

Un problème est malheureusement survenu avec la vulgarisation des équipements : la communication entre équipements de différentes marques était impossible. Ceci entrainait donc une complexité des systèmes d'information des établissements médicaux. C'est là que l'urgence d'une normalisation des équipements et des données médicales est apparue.

Différents comités au sein des organisations de normalisation ont donc vu le jour dans le but de simplifier les systèmes d'information de la santé. Parmi ces comités, on citera **:**

- Le Comité Technique 251 (appelé Health Informatics) au sein du CEN (Comité Européen de Normalisation) en 1991.
- Le Comité Technique 215 (appelé également Health Informatics) au sein de l'ISO en 98.
- Le Comité ACR-NEMA en 1983 devenu DICOM en 1991.

Avec le développement des technologies numériques en général et en imagerie médicale particulier à partir des années 1970, l'American College of Radiology (ACR) et la National Electrical Manufacturers Association (NEMA) ont remarqué la nécessité grandissante de créer une méthode standard facilitant le transfert des images médicales et leurs informations entre machines de différents constructeurs qui, jusque-là, possédait des formats propriétaires

- Le Comité HL7 (Health Level seven) au sein de l'ANSI (American National Standards Institute) en 1987.

Parmi les différentes normes créées par ces différents organismes, la plus aboutie et la plus prépondérante est la norme DICOM.

Avant l'apparition du standard DICOM, il existait plusieurs problèmes liés à l'archivage des images et à la communication entre les machines des différents constructeurs. En effet, chaque constructeur possédait ses formats propriétaire, qui n'était

donc lisible que par les machines de ce même constructeur, il se posait donc le problème **d'interopérabilité** entre les machines, cela rendait impossible la communication entre les médecins, les hôpitaux et même les services d'un même hôpital si les équipements étaient de marques différentes.

L'autre problème qui se posait était que les différentes informations liées à l'image médicale telles les informations relatives au patient (nom, age, sexe, antécédents...), le nom du médecin traitant, les rapports d'examen... étaient stockées séparément de l'image. Cette manière hétérogène de stocker les informations menait inévitablement à **des erreurs d'archivage**, d'où la perte d'information utile. La probabilité qu'une erreur pareille ne se produise est assez importante vu le nombre important d'images présentes dans chaque hôpital.

Dans plusieurs cas, le médecin traitant consulte ses collègues pour émettre son diagnostic, or il n'y a que son nom qui figure dans le rapport qu'il fait, pourtant il prend en considération l'avis des autres médecins. En cas de mauvais diagnostic, le médecin traitant est tenu comme le seul responsable alors qu'il a pu être, accidentellement, induit en erreur par un autre collègue.

2. Les standards et normes de l'imagerie médicale

Les standards et les normes en informatique permettent de simplifier et d'uniformiser la communication entre les applications, et ainsi de faciliter le développement d'interfaces.

2.1.Un format de message commun : le standard HL7

2.1.1. Définition

Tout comme la langue de Shakespeare est le « standard » de la communication orale et écrite entre les individus de notre planète, HL7 (Health Level 7) est le « standard » de communication « qui définit un format de message pour les échanges informatisés de données cliniques, financières et administratives entre différents systèmes d'information hospitaliers (imagerie, laboratoires, soins infirmiers, dossier administratif patient…) ».

2.1.2. Valeur ajoutée de la standardisation de la communication entre les applications

Considérons un système d'information de santé composé de six logiciels différents : un d'admission (L1), un de prescription de médicaments (L2), un de planification des rendez-vous (L3), un de biologie (L4), un d'imagerie (L5) et un logiciel de facturation (L6). Lorsqu'un patient se rend dans un établissement de santé, il est possible, dans le cadre de son parcours de soins, de décliner dans chacune de ces six applications ses informations

d'identité, à savoir ses nom, prénom, date de naissance, sexe, adresse et identifiant. Dans le cas où il n'y aurait pas de norme de communication entre les différents logiciels, pour échanger ces informations, il faudrait développer deux interfaces entre chaque logiciel. Une de L1 vers L2, une L2 vers L1, puis une de L1 vers L3 et une L3 vers L1, etc. Ce qui représente un total de 30 interfaces d'échange à développer, à maintenir et à faire évoluer !

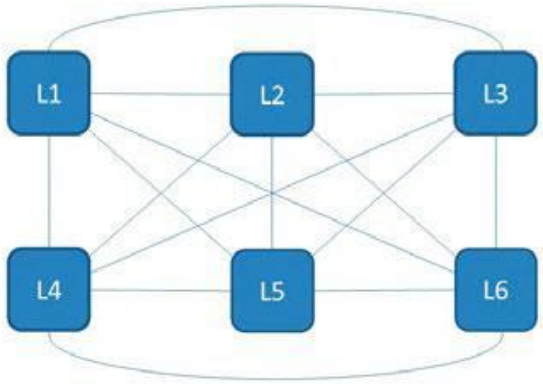


Figure IV.1. Illustration de 30 interfaces

Pour un SI composé de n éléments, cette règle se généralise au développement et à la maintenance de n*(n-1) interfaces : c'est absolument ingérable ! Pour l'exemple précédent, avec le standard HL7, il n'y a plus qu'une seule interface d'échange car les six logiciels parlent un langage commun.

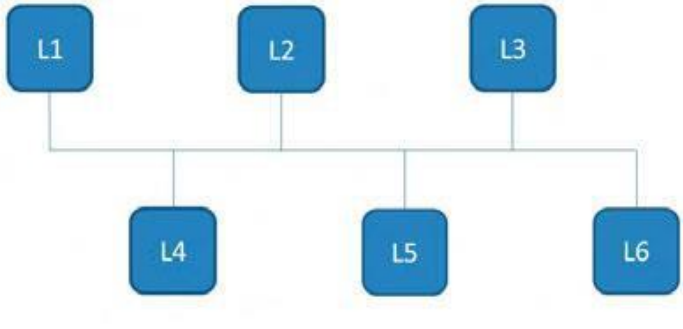


Figure IV.2.Illustration d'une interface

2.1.3. Historique

HL7 est une organisation née en 1987 aux États-Unis et dont l'objectif est de créer un standard de communication pour les systèmes informatiques hospitaliers. En 1994, HL7 obtient une accréditation de l'American National Standard Institute (ANSI) pour le standard de communication HL7.

2.1.4. Principe de HL7.

Chaque application stocke ses informations dans sa base de données et dans son propre langage. Puis, pour chaque patient, les informations « à diffuser » aux autres applications sont regroupées dans un fichier. Elles sont positionnées dans des « cases », que l'on appelle « des segments ». Ce fichier est ensuite diffusé et décodé par les autres applications qui le reçoivent. Voici l'exemple d'un fichier HL7 pour le patient « Paul Durand ».

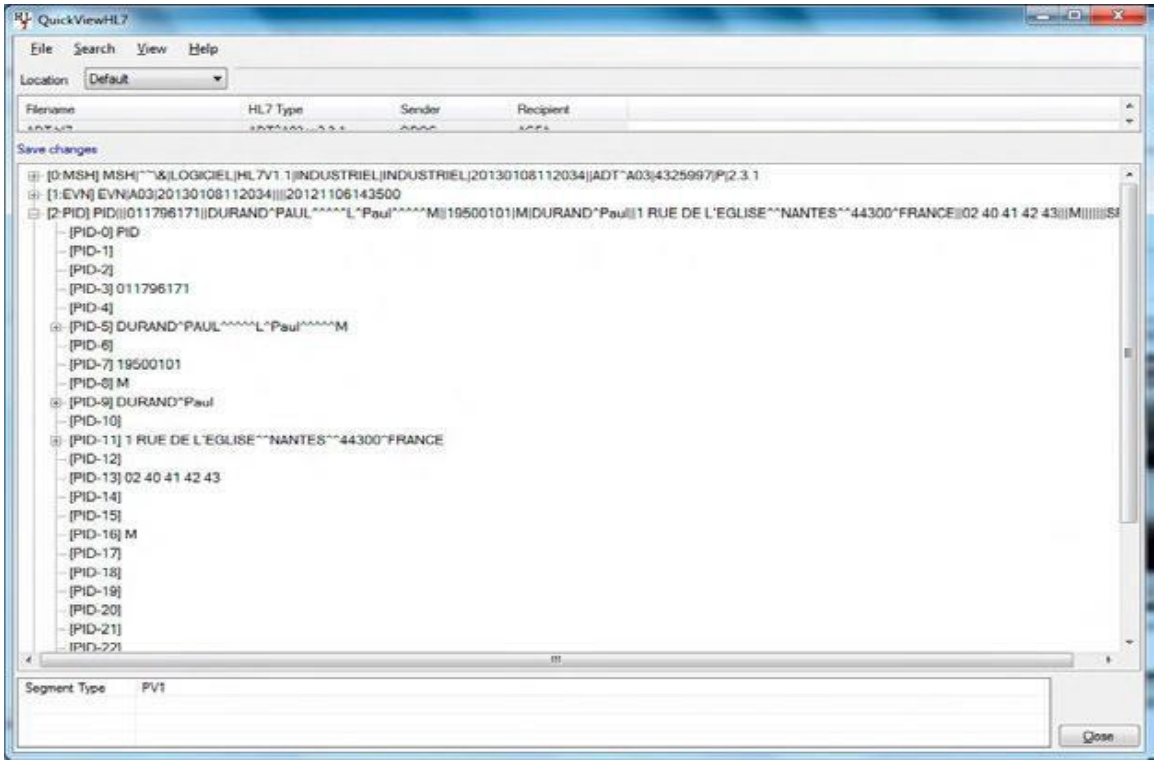


Figure IV.3. Exemple d'un fichier HL7 avec un éditeur HL7

Sur la ligne PID (Patient IDentification), l'IPP du patient figurera toujours dans le segment n°3 (ici la valeur 011796171). Sur cette même ligne PID, la cinquième « case » contiendra toujours les valeurs NOM^PRENOM (valeur « DURAND^PAUL » dans notre exemple). Puis le septième segment contiendra invariablement la valeur « date de naissance » si elle est connue. Il existe des variantes du standard HL7 en fonction des pays, notamment pour la prise en compte des différences de construction des noms de famille ou pour la gestion d'informations complémentaires.

3. DICOM pour les images médicales

3.1.Définition

DICOM est l'acronyme de **D**igital **I**maging and **CO**mmunications in **M**edecine. Il s'agit d'une norme, d'un standard, ou encore d'une structure commune pour la gestion

informatique de l'imagerie médicale. Ce standard évolue en permanence en étendant son domaine d'application. Certains nouveaux chapitres sont en cours de réflexion et de rédaction alors que d'autres ont été annulés. À titre d'exemple, la version 2014 s'est vue enrichie d'un package comportant 14 nouveaux éléments !

DICOM s'applique maintenant aux signaux (ECG, EEG), à la thermographie, à l'ophtalmologie, à la radiothérapie,….. etc.

3.2.Historique

C'est en 1985 qu'une société savante américaine de radiologues, l'American Collège of Radiology (ACR), et un groupement d'industriels, le National Electrical Manufacturers Association (NEMA), se rassemblent et établissent la première version du standard lié à l'imagerie médicale : la norme ACR/NEMA. Une seconde version vit le jour en 1988, mais c'est réellement en 1990, avec la version 3 que naît le standard DICOM qui prend alors le numéro de version 3.0. Cette version existe toujours, cependant, elle est en constante évolution et adaptation. Nous parlerons donc de Version DICOM 3.0 2011 ou encore DICOM 3.0 de mars 2014.

3.3.Vue générale de la norme DICOM

Aujourd'hui DICOM adoptée par la plupart des constructeurs. Avec chaque machine respectant cette norme est émise une déclaration de conformité (Conformance Statement) facilitant ***l'interopérabilité*** avec d'autres dispositifs. Ce standard utilisé dans le milieu médical. Il permet grâce à sa structure de communiquer les images numériques médicales à travers un réseau. Ce format fournit d'une part l'image numérique et d'autre part une information texte relative à l'examen effectué. L'image est alors codée sur plus de 4000 niveaux de gris par pixel. Il est possible de mettre en évidence les zones que le médecin spécialiste désire analyser en gardant qu'une partie de l'information haute résolution. Il permet l'archivage aisé des images et des informations qui y sont associés et facilite leur transmission.

Le recours au processus de numérisation des films radiographiques permet aux radiologues de consulter les images des examens antérieurs .Les numériseurs sont considérés comme des modalités d'imagerie et doivent être conformes à la norme DICOM afin d'assurer la communication des données au PACS.

Figure VI.4. Le numérisateur

Actuellement, la norme DICOM contient 16 parties :

- **Introduction et vision globale** (Introduction and overview) : Donne les grandes lignes du standard en expliquant les raisons qui ont mené à sa création et les buts qu'il a permis d'atteindre.

- **Conformité** (Conformance) : Définit les principes d'une implémentation conforme du standard. C'est suivant cette partie que les déclarations de conformité sont rédigées.

- **Définition des objets d'informations** (Information Object Definitions : IODs) : Spécifie l'ensemble des IODs permettant de donner une représentation des éléments du monde réel et applicables pour la communication numérique d'informations médicales.

- **Définition des services** (Service Class Specifications) : Spécifie l'ensemble des services permettant de donner une représentation des activités du monde réel et applicables pour la communication numérique d'informations médicales.

- **Encodage** (Data Structured and Encoding) : Facilite l'échange des données en définissant une syntaxe de codage précise pour la représentation de l'information.

- **Dictionnaire des données** (Data Dictionary) : Contient tous les codes des balises définissant les éléments DICOM ainsi que les identifiants uniques (Unique IDentifiers : UIDs)

- **Echange des messages** (Message Exchange) : Définit la structure des messages DICOM (DICOM Message Service Element : DIMSE) échangés entre les services communicants DICOM (point-a-point ou a travers un réseau). Un DIMSE définit un élément de communication incluant un service et un protocole, il est utilisé par les entités

DICOM (Application Entity : AE) pour le transfert des informations médicales. Le protocole DIMSE définit les règles nécessaires pour la construction de messages conformes.

- **Support réseau pour l'échange des messages** (Network Communication Support for Message Exchange) : Le modèle de communication DICOM à travers un réseau est basé sur le modèle OSI (Open Systems Interconnected), de l'ISO. Cette partie définit les règles de communication au niveau applicatif entre les entités DICOM à travers un réseau. Les aspects de la communication à de plus bas niveaux mentionnés et explicités dans cette partie ne sont pas propres au standard. DICOM ne définit que la communication au niveau applicatif

- **Support de stockage et format des fichiers pour l'échange de donnée** (Media Storage and File Format for Data Interchange) : Spécifie un modèle général pour le stockage des informations médicales sur une large gamme de supports amovibles pour permettre l'échange des données à travers ces derniers.

- **Profiles des applications spécifiques aux supports de stockage** (Media Storage Application Profiles) : Spécifie un sous-ensemble d'applications conformes DICOM utilisables pour le stockage sur les supports amovibles.

- **Formats de médias et supports physiques pour l'échange de données** (Media Formats and Physical Media for Data Interchange) : Spécifie une structure décrivant les relations entre le modèle de la partie 10 et des supports physiques spécifiques et des formats spécifiques. Elle définit aussi les caractéristiques des supports physiques et des formats associés.

- **Visualisation en niveaux de gris** (Grayscale Standard Display Function) : Définit une fonction normalisée pour l'affichage des images en niveaux de gris.

- **Profiles de Sécurité** (Security and System Management Profiles) : Spécifie la manière dont doit être implémenté et géré un protocole de sécurité, déjà existant (Transport Layer Security (TLS) par exemple) pour être conforme à la norme. DICOM ne définit pas de procédés de sécurisation spécifiques à la norme.

- **Ressources terminologiques** (Content Mapping Resource) : Définit l'ensemble des abréviations utilisées tout au long du document.

- **Informations explicatives** (Explanatory Information) : Permet de mieux comprendre la signification des termes utilisés dans le document.

- **Accès web** (Web Access to DICOM Persistent Objects (WADO)) : Définit un service basé sur le web facilitant la distribution et la consultation d'informations médicales en utilisant les protocoles web (à partir d'une page HTML par exemple).

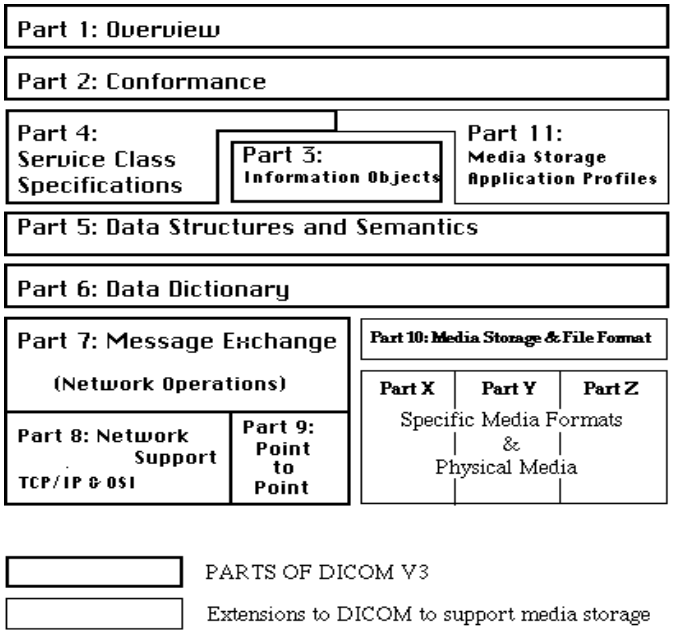


Figure IV.5 ; Architecture de DICOM

4. Buts de la norme DICOM

La norme DICOM facilite ***l'interopérabilité*** entre différents dispositifs revendiquant une conformité en :

- Définissant la sémantique des commandes de communications et des données associées, de sorte à fournir un certain nombre de règles à suivre par les constructeurs. En fait, pour que deux ou plusieurs dispositifs puissent communiquer en liaison point-à-point ou à travers un réseau, il doit y avoir des normes sur la manière dont ils sont censés réagir aux différentes commandes et aux données qui y sont associées, et non seulement aux informations qui sont simplement transférées de l'un à l'autre.

- Définissant la sémantique des fichiers et des services qui y sont associés pour permettre une communication à travers les différents supports amovibles (systèmes non connectés : off-line).

- Définissant de manière très explicite les conditions de conformité pour son implémentation. De plus, une déclaration de conformité doit obligatoirement être émise avec chaque nouveau dispositif respectant la norme, document qui doit contenir assez d'informations permettant de définir les fonctions d'interopérabilité avec d'autres dispositifs.

- Facilitant les opérations dans un environnement connecté en réseau.

- Etant structurée de manière à faciliter l'introduction de nouveaux services, ainsi il lui est facile de s'adapter aux futures applications d'imagerie médicale.

- En se basant sur des normes internationales déjà existantes (le modèle OSI)

5. Le standard DICOM

Ce standard, aussi développé initialement par le comité ACR-NEMA et sorti en 1991, englobe un certain nombre d'améliorations considérables par rapport aux versions antérieures. Ces améliorations notables sont :

- Il est applicable dans un environnement connecté en réseau. Les standards ACRNEMA n'étaient applicables que lors de connexions point-a-point. Pour pouvoir les utiliser en réseau, il fallait une unité d'interface réseau (Network Interface Unit. **NIU**). Le standard DICOM quant à lui est capable d'opérer dans un réseau en utilisant, par exemple, le standard TCP/IP.

- Il est applicable utilisant différents supports amovibles (CDs , DVDs . . .) . Les standards ACR-NEMA ne définissaient pas de format de fichier, de choix de support physique ou de système de fichiers logique. DICOM supporte quant à lui l'utilisation des standards de l'industrie, physiques tels les CD-R, ou bien les systèmes de fichiers logiques, tel le PC File System FAT 32.

- Il spécifie comment les dispositifs revendiquant la conformité à la norme réagissent aux commandes et aux données échangées. Les standards ACR-NEMA étaient limités au transfert des données, mais DICOM spécifie, par le concept des classes de service (Service Classes), la sémantique des commandes et des données associées.

- Il spécifie des niveaux de conformité. Les standards ACR -NEMA avaient spécifié

un niveau minimum de conformité. DICOM décrit explicitement comment un constructeur doit structurer une déclaration de conformité (Conformance Statement) pour choisir des options spécifiques.

- Il est structuré en plusieurs parties sur un document. Ceci facilite l'évolution du standard dans un environnement en pleine évolution en simplifiant l'ajout de nouvelles fonctionnalités. Les directives de l'ISO définissant la manière dont doit être structuré un document en plusieurs parties ont été suivies lors de la construction de la norme DICOM.

- Il introduit des informations explicites pour les images, graphes, formes d'ondes, rapports, impressions...

- Il spécifie une technique établie pour l'identification unique de chaque information. Ceci facilite la définition sans ambigüité des relations entre les différentes informations.

C'est cette dernière version du Standard qui a été maintenue, avec quelques modifications au fil des années pour s'adapter aux nouvelles fonctionnalités et capacités des dispositifs.

6. Propriétés des fichiers DICOM

6.1.L'orientation Objet

En premier lieu, précisons que DICOM est orientée objet, pour cela on désigne par « objet information » (Information Object) une information dans le fichier (image, nom du patient...) et par classe de service (Service Class) appliqué à l'objet toute opération sur cette information.

6.2.Les UIDs

Avant d'aller plus loin, il est important de définir un paramètre primordial utilisé dans DICOM : l'identifiant unique (Unique Identifier UID). C'est un identifiant généré automatiquement par chaque machine conforme DICOM à l'aide d'une technique qui garantit son unicité. L ' UID identifie une information et, du fait de son unicité, permet de la préserver d'éventuelles erreurs. Les identifiants sont obligatoirement présents dans chaque fichier DICOM. Il ne peut exister deux UIDs identiques pour désigner deux informations différentes quelque que soit la machine ou sa localisation. Ainsi l'identifiant d'une série d'images est spécifique à un patient, un examen, une date, un hôpital et une machine. En résumé, l'UID est nécessaire pour des raisons médicales et médico-légales, et

permet aussi la création et la gestion de bases de données.

Il existe quatre UIDs obligatoires dans chaque fichier DICOM :

- SOP Class UID : Identifiant du service auquel est destinée l'image.
- Study instance UID : Identifie un examen entier en temps et en lieu.
- Series Instance UID : Identifie une série d'images dans l'examen.
- SOP Instance UID ou Image UID : Identifie l'image associée au ficher.

6.3.Les Objets de définition des informations (IOD)

Le principe des IODs (Information Object Definition) est un modèle de données abstrait orienté objet utilisé pour spécifier des informations sur des éléments du monde réel. Un IOD fournit aux entités applicatives (AE) communicantes une vue d'ensemble sur les informations échangées.

Un IOD ne représente pas une information spécifique d'un élément du monde réel mais plutôt une classe d'éléments possédant les mêmes propriétés. Un IOD utilisé pour représenter une seule classe d'éléments réels est appelé Objet Information Normalisé (Normalized Information Object). Un IOD incluant plusieurs éléments du monde réel en relation entre eux est appelé Objet Information Composé (Composite Information Object).

Un IOD contient plusieurs attributs (attributs). Ces attributs décrivent les propriétés de l'information sur l'élément du monde-réel représenté. ***(voir plus de détail sur IOD objet DICOM dans la section 10.1)***

6.4.Codage des attributs :

Les attributs sont encodés, comme toutes les données textuelles dans DICOM, de deux manières :

6.4.1. Codage implicite

Dans le codage implicite, l'information est codée sur 3 champs comme suit :

- Champ 1 : Balise contenant un code de 32 bits (16 bits (groupe), par exemple le groupe 0010(h) est le groupe d'identification du patient + 16 bits (élément)) définissant le type d'information contenue dans le troisième champ.

- Champ 2 : Code de 16 ou 32 bits donnant la longueur en octets du troisième champ.

- Champ 3 : L'information utile codée en ASCII dans le cas d'une chaine de caractères, sa longueur est bien sur variable.

Exemple :

Information relative au nom du patient : Salim EL BECHIR On va représenter les valeurs en hexadécimal :

(0010,0010) | 0000000F | 53 61 6C 69 6D 20 45 4C 20 42 45 43 48 49 52

6.4.2 Codage explicite

Dans le codage explicite, l'information est codée sur 4 champs comme suit :

- Champ 1 : Balise contenant un code de 32 bits (16 bits (groupe) + 16 bits (élément)) définissant le type d'information contenue dans le troisième champ.

- Champ 2 : Code sur 16 ou 32 bits contenant une étiquette de 2 lettres représentant le type d'information (PN pour Patient's Name, DA pour patient's birth date~etc), ces codes sont aussi définis par le standard.

- Champ 3 : Code de 16 ou 32 bits donnant la longueur en octets du quatrième champ.

- Champ 4 : L'information utile codée en ASCII dans le cas d'une chaine de caractères, sa longueur est bien sur variable.

Exemple :

On va utiliser le même exemple qu'avant, information relative au nom du patient : Salim EL BECHIR

On va représenter les valeurs en hexadécimal :

(0010,0010) | 50 4E | 0000000F | 53 61 6C 69 6D 20 45 4C 20 42 45 43 48 49 52.

N.B : Lors du transfert d'un fichier DICOM, il doit impérativement être précisé si le codage utilisé est implicite ou explicite pour éviter une interprétation erronée des informations.

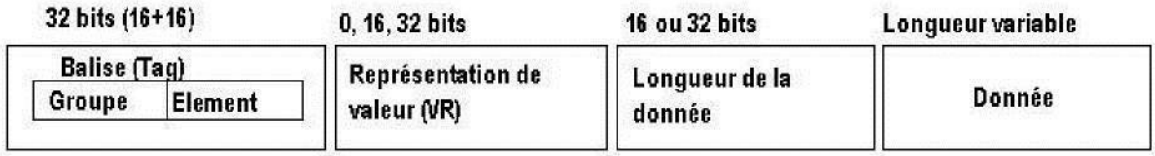


Figure IV.6 : Codage des attributs dans DICOM

6.5.Les SOP Class :

Le traitement d'une information DICOM s'effectue en appariant un objet avec une classe de service en créant ainsi une paire objet/service (Service/Object Pair SOP). Par exemple : le service « imprimer » + l'objet « image « donne la SOP « imprimer l'image ».

L'application d'un service donnée à un objet donné constitue une SOP Class. Par exemple le service « stocker » + l'objet « une image MR (Magnetic Resonance) » donne la SOP Class « Stocker une image MR ».Chaque SOP Class est définie par son propre UID.

En faisant appel à une SOP Class sur une machine avec un patient « réel », il y a génération d'une SOP Instance (information) qui reçoit son propre UID.

Toute machine voulant se conformer à DICOM (ou toute autre AE DICOM) doit impérativement pouvoir traiter au moins un type spécifique d'images et effectuer au moins un service pour ainsi pouvoir gérer une SOP Class. DICOM définit toutes les paires **« objet/classe de service »** possibles.

Le processus de communication DICOM comporte l'échange de SOP Instances en utilisant des messages DICOM. Ce dernier est la « version communication » des SOP Class, il contient les commandes qui utilisent ou fournissent le service spécifié et le code de l'objet information à traiter.

Par ailleurs, la SOP Class doit spécifier si le service DICOM est employé en tant qu'utilisateur (Service Class User : SCU) ou comme fournisseur (Service Class Provider . SCP). Par exemple un scanner utilise le service d'impression fourni par un reprographe, le scanner est alors doté d'une SCU pour le reprographe, de son côté le reprographe est doté d'une SCP pour le scanner.

Cette SOPClass permet de spécifier les paramètres suivants :

- L'espace de sortie des niveaux de gris.

- L'espace de sortie des couleurs.
- La zone de l'image à afficher, à inverser ou à tourner.
- Les données textuelles à afficher avec l'image.
- Afficher deux ensembles d'images sur une seule fenêtre.

6.6.Les services (Service Class) :

Les services sont les opérations qu'il est possible d'effectuer sur les objets information. DICOM utilise les services suivants :

- Vérification (Verification) : Permet de vérifier si deux machines communiquent correctement.
- Stockage (Storage) : Facilite le transfert et la sauvegarde d'informations entre deux dispositifs. Permet aussi à une entité DICOM d'envoyer et/ou de recevoir des images, formes d'ondes, rapports...
- Stockage sur Support amovible (Media Storage) : Spécifie l'échange entre deux dispositifs par l'intermédiaire de supports amovibles.
- InterrogerLRetrouver (Query/Retrieve) : Implémente des commandes de type : FIND, GET et MOVE. FIND permet de demander une liste d'images alors que GET et MOVE permettent d'entamer un transfert qui sera effectué via la classe Storage Service Class citée ci- dessus.
- Notification du contenu d'un examen (Study Contents Notifications) : Utilisée pour notifier l'arrivée d'une nouvelle image ou série d'images. Elle peut être utilisée pour initier un transfert ou vérifier si le transfert d'une image ou d'une série d'images est complet.
- Gestion d'impression (Print Management) : Permet la connexion avec un reprographe, elle sert aussi à donner les spécifications de l'image (couleur, niveaux de gris, taille...)
- Gestion des examens (Study Management) : Permet la gestion des examens (création des rendez-vous, suivi des patients...)
- Gestion des résultats (Result Management) : Permet la gestion des résultats des examens (rapports des médecins, commentaires...).
- Engagement de stockage (Storage Commitment) : Lors de l'utilisation de la Storage SOP Class pour un transfert, il n'y aucun engagement entre les deux entités utilisant ce transfert pour garder la SOP Instance transmise (elle peut être supprimée après

l'envoi ou à la réception après son utilisation une seule fois). La Storage Commitment SOP Class permet a l'émetteur de demander au récepteur de s'engager à sauvegarder la SOP Instance transmise pour un certain laps de temps ou de manière permanente, comme pour un système d'archivage par exemple.

- Gestion des listes de travail (Basic Worklist Management) : Fac il ite l 'accès a ux listes de travail (worklists) et permet leur gestion. Une liste de travail contient les informations relatives a un ensemble de tâches a accomplir, spécifiant les détails de chaque tâche ainsi que son ordre de priorité d'exécution. Un exemple simple d'une liste de travail est celle présente dans un service d'imagerie et contenant les examens programmés.
- Stockage d'une copie logicielle de l'état d'affichage (Softcopy Presentation State Storage) : Ajoute une fonctionnalité supplémentaire a la Storage SOP Class consistant en la capacité de transporter un état d'affichage (Presentation State) souhaité ou d'enregistrer un état existant. Un état d'affichage est défini par différents paramètres tels niveaux de gris/couleurs, fenêtrage.

- Stockage des rapports structures (Structured Reporting Storage) : Extension de la Storage Class, elle donne plus de possibilités au comportement du récepteur.
- Journal d'évènements (Application Event Logging) : Facilite le transfert, sur un réseau, des enregistrements des journaux d'évènements de manière à ce qu'ils soient enregistrés sur le même dispositif central ; un serveur centralisé par exemple.
- Interrogation des informations pertinentes sur le patient (Relevant Patient Information Query) : Facilite l'accès aux informations pertinentes relatives au patient telles qu'elles ont été enregistrées aux différents examens.
- Notification de la disponibilité d'une information (Instance Availibility Notification) : Permet a une AE DICOM de notifier une autre de la présence et de la disponibilité d'une SOP Instance.
- Gestion de la création de supports (Media Creation Management) : Définit un mécanisme qu'un émetteur peut utiliser pour donner une instruction à un dispositif de créer un support d'échange co ntenant un ensemble de SOP Instances qui ont déjà été transférées au dispositif de création du media par le biais de la Storage service Class.
- Stockage du protocole d'attachement (Hanging Protocol Storage) : Permet l'envoi d'une Hanging Protocol SOP Instance d'une AE à une autre. Le protocole

d'attachement est utilisé pour l'attachement des fichiers DICOM en pièce jointes à des e-mails.

- Interrogation/Recherche d'un protocole d'attachement (Hanging Protocol Query/Retrieve) : Facilite l'accès aux Hanging Protocol SOP Intances.

7. **Modèle d'information DICOM :** définit une structure bien précise pour la représentation des informations médicales. Cette structure définit les relations entre les services et les objets, elle est organisée en hiérarchie avec au sommet un service et à la base les informations << brutes >>.

N.B *: Dans cet organigramme et suivant la norme DICOM et les directives ISO, les rectangles désignent les entités et les losanges désignent les relations les reliant.*

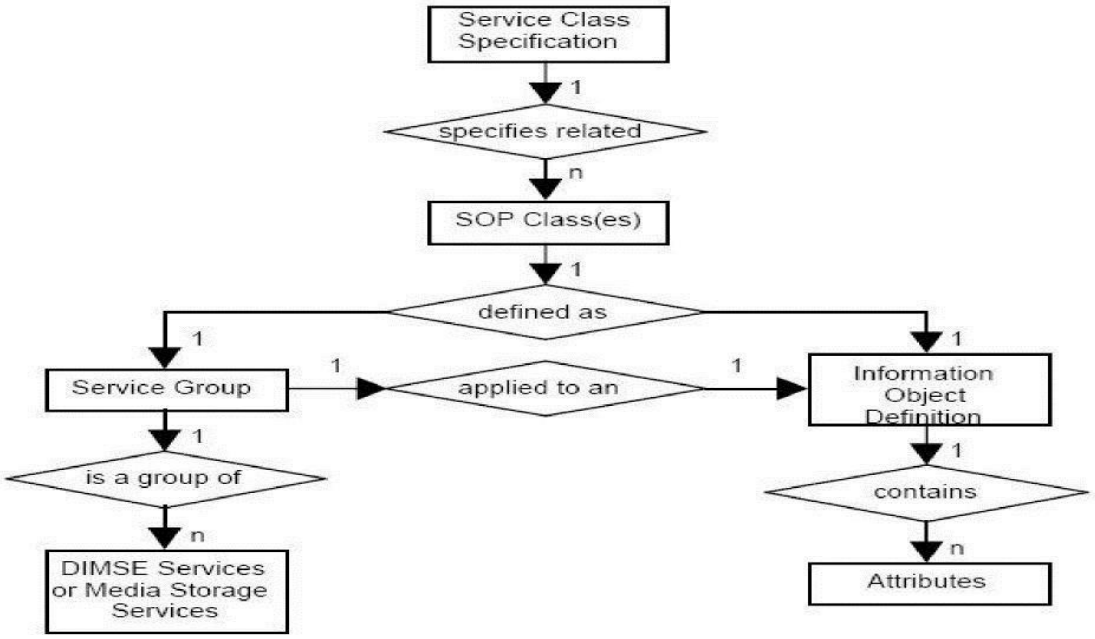


Figure .IV.7 : Modèle d'information DICOM (DICOM Information Model)

A- Explication du modèle.

Au sommet, une classe de services possède ses propres spécifications, elle est en relation avec plusieurs SOP Class du fait de la présence de plusieurs IODs utilisant cette classe. Chaque SOP Class définit un groupe de services appliqués a un IOD. Un IOD contient plusieurs attributs qui représentent l'information exploitable. De son côté, le groupe de services contient des services de gestion des supports de stockage et/ou des services de communication définis via les DIMSEs.

8. Structure des fichiers DICOM :

La structure des fichiers issus de la norme DICOM remédie très efficacement aux problèmes qui existaient avant son apparition.

La première remarque qu'on fera, qui est la plus évidente, est qu'étant donné le fait que DICOM soit une norme adoptée par les constructeurs, il n'y a plus de souci d'interopérabilité entre les machines.

Autre point plus important, un fichier DICOM contient en plus de l'image médicale, plusieurs données textuelles relatives à l'image, le patient, l'examen... Cette manière homogène de stocker toutes les données en un seul fichier facilite grandement leur stockage et accroit de manière très significative la sauvegarde des informations et diminue la probabilité de perte.

On peut donc considérer le fichier DICOM comme un dossier médical complet.

En général, un examen médical s'effectue en une série de plusieurs tests, chaque fichier DICOM contient l'identifiant de la série à laquelle il appartient, il est ainsi aisé de stocker et de rassembler les fichiers d'une même série ensemble. Il est à noter, bien sûr, que l'identifiant de la série est unique. Il existe aussi un autre identifiant unique relatif à chaque fichier DICOM.

De la sorte, chaque image est indépendante, même si elle est transférée ou renommée, les informations qu'elle contient restent intactes.

Le fait que chaque médecin, donnant son diagnostic sur l'image, laisse sa trace dans le fichier implique qu'il a une part de responsabilité dans le diagnostic final établi par le médecin traitant. En cas de mauvais diagnostic, il existe plus d'informations permettant d'éviter une telle erreur à l'avenir.

- ***Infos contenues dans un fichier DICOM :***

1. **Une entête (header) avec données démographiques et techniques**

[0008] Identification de la machine : date d'examen ; type d'examen ;fabricant de la machine ;hôpital ou institution, …

[0010] Infos sur le patient : nom ; date de naissance ; sexe

[0018] Infos sur l'acquisition de l'information : épaisseur de coupe, variable suivant le type d'examen,

2. **Un entête (header) avec données démographiques et techniques**

[0020] Infos sur l'examen :orientation du patient ;nombre d'images dans l'acquisition ; commentaires, …

[0028] Infos sur l'image et le type de codage : Largeur ; hauteur

3. **les données image (pixels) :**

[7FE0] Pixels de l'image

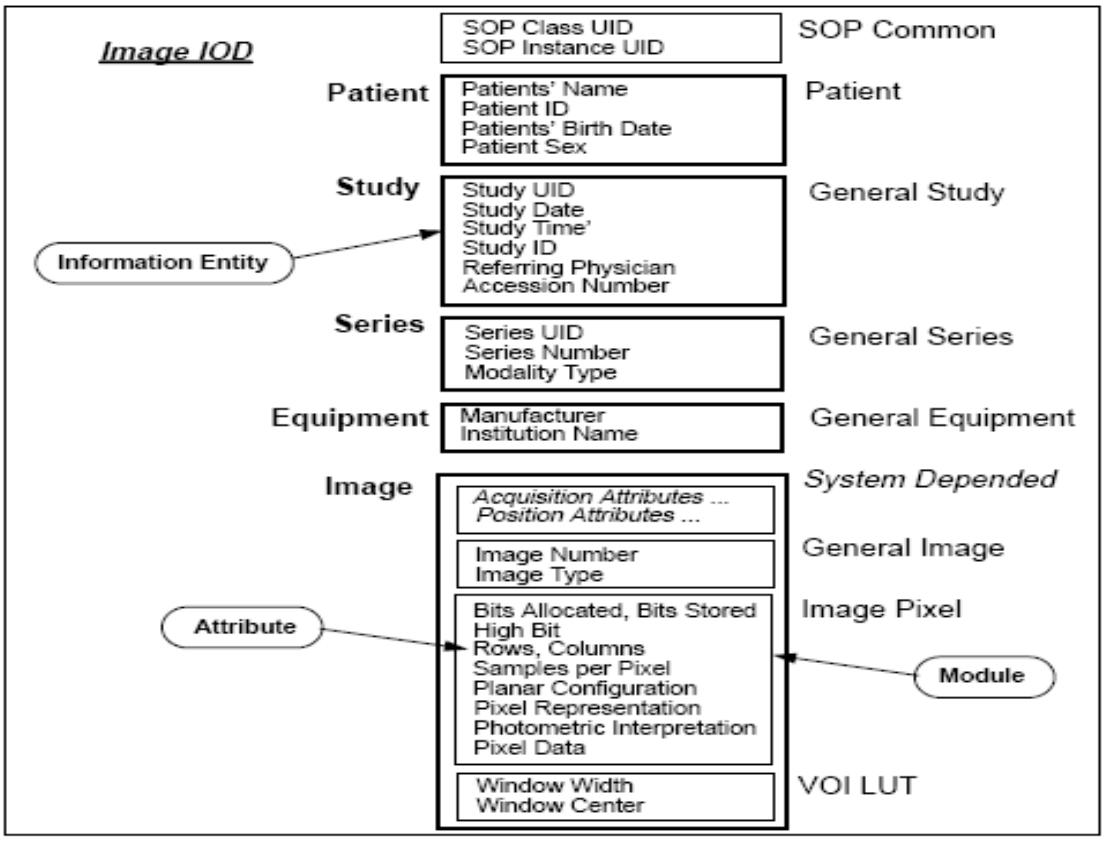


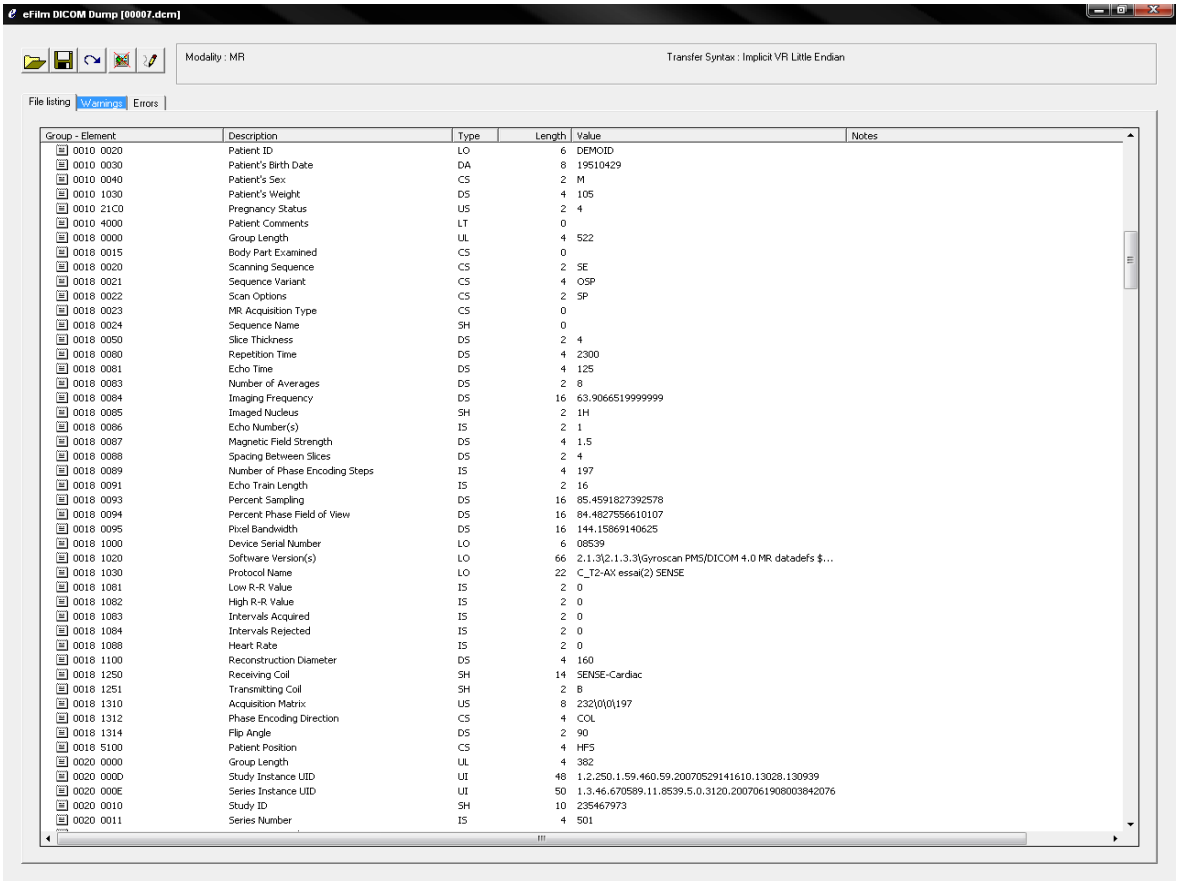
Figure IV.9. Infos contenue dans un fichier DICOM

Un fichier DICOM est composé comme suit, il y a 128 zéros d'abord, ensuite viennent les caractères « DICM » en ASCII. Après viennent les informations textuelles et les pixels de l'image. Parmi les informations textuelles, on trouve :

- ✓ Les coordonnées du patient.
- ✓ La date et le type d'examen.
- ✓ Les références de la machine utilisée.

- ✓ Le nom du médecin ou du technicien qui effectue l'examen.
- ✓ Le nom de l'hôpital.
- ✓ Les données d'acquisition de l'image.
- ✓ L'identifiant de la série à laquelle appartient l'examen.
- ✓ Les rapports des diagnostiques effectués par le/les médecin(s) traitant(s).

Une fausse idée reçue très répandue dit que dans le fichier DICOM, il y a un entête contenant les informations textuelles et qu'ensuite viennent les pixels de l'image. Le fichier DICOM contient des champs d'informations et la matrice représentative de l'image est un de ces champs, le dernier. L'IOD matrice image est identifié par la balise (7FE0, 0010).



Group - Element	Description	Type	Length	Value	Notes
0010 0020	Patient ID	LO	6	DEMOID	
0010 0030	Patient's Birth Date	DA	8	19510429	
0010 0040	Patient's Sex	CS	2	M	
0010 1030	Patient's Weight	DS	4	105	
0010 21C0	Pregnancy Status	US	2	4	
0010 4000	Patient Comments	LT	0		
0018 0000	Group Length	UL	4	522	
0018 0015	Body Part Examined	CS	0		
0018 0020	Scanning Sequence	CS	2	SE	
0018 0021	Sequence Variant	CS	4	OSP	
0018 0022	Scan Options	CS	2	SP	
0018 0023	MR Acquisition Type	CS	0		
0018 0024	Sequence Name	SH	0		
0018 0050	Slice Thickness	DS	2	4	
0018 0080	Repetition Time	DS	4	2300	
0018 0081	Echo Time	DS	4	125	
0018 0083	Number of Averages	DS	2	8	
0018 0084	Imaging Frequency	DS	16	63.9066519999999	
0018 0085	Imaged Nucleus	SH	2	1H	
0018 0086	Echo Number(s)	IS	2	1	
0018 0087	Magnetic Field Strength	DS	4	1.5	
0018 0088	Spacing Between Slices	DS	2	4	
0018 0089	Number of Phase Encoding Steps	IS	4	197	
0018 0091	Echo Train Length	IS	2	16	
0018 0093	Percent Sampling	DS	16	85.4591827392578	
0018 0094	Percent Phase Field of View	DS	16	84.4827556610107	
0018 0095	Pixel Bandwidth	DS	16	144.15869140625	
0018 1000	Device Serial Number	LO	6	08539	
0018 1020	Software Version(s)	LO	66	2.1.3\2.1.3.3\Gyroscan PMS/DICOM 4.0 MR datadefs $...	
0018 1030	Protocol Name	LO	22	C_T2-AX essai(2) SENSE	
0018 1081	Low R-R Value	IS	2	0	
0018 1082	High R-R Value	IS	2	0	
0018 1083	Intervals Acquired	IS	2	0	
0018 1084	Intervals Rejected	IS	2	0	
0018 1088	Heart Rate	IS	2	0	
0018 1100	Reconstruction Diameter	DS	4	160	
0018 1250	Receiving Coil	SH	14	SENSE-Cardiac	
0018 1251	Transmitting Coil	SH	2	B	
0018 1310	Acquisition Matrix	US	8	232\0\0\197	
0018 1312	Phase Encoding Direction	CS	4	COL	
0018 1314	Flip Angle	DS	2	90	
0018 5100	Patient Position	CS	4	HFS	
0020 0000	Group Length	UL	4	382	
0020 000D	Study Instance UID	UI	48	1.2.250.1.59.460.59.2007052914161O.13028.130939	
0020 000E	Series Instance UID	UI	50	1.3.46.670589.11.8539.5.0.3120.2007061908003842076	
0020 0010	Study ID	SH	10	235467973	
0020 0011	Series Number	IS	4	501	

Figure IV.10 : interface DICOM qui représente les infos sur l'acquisition de l'information et l'examen [0018] et [0020]

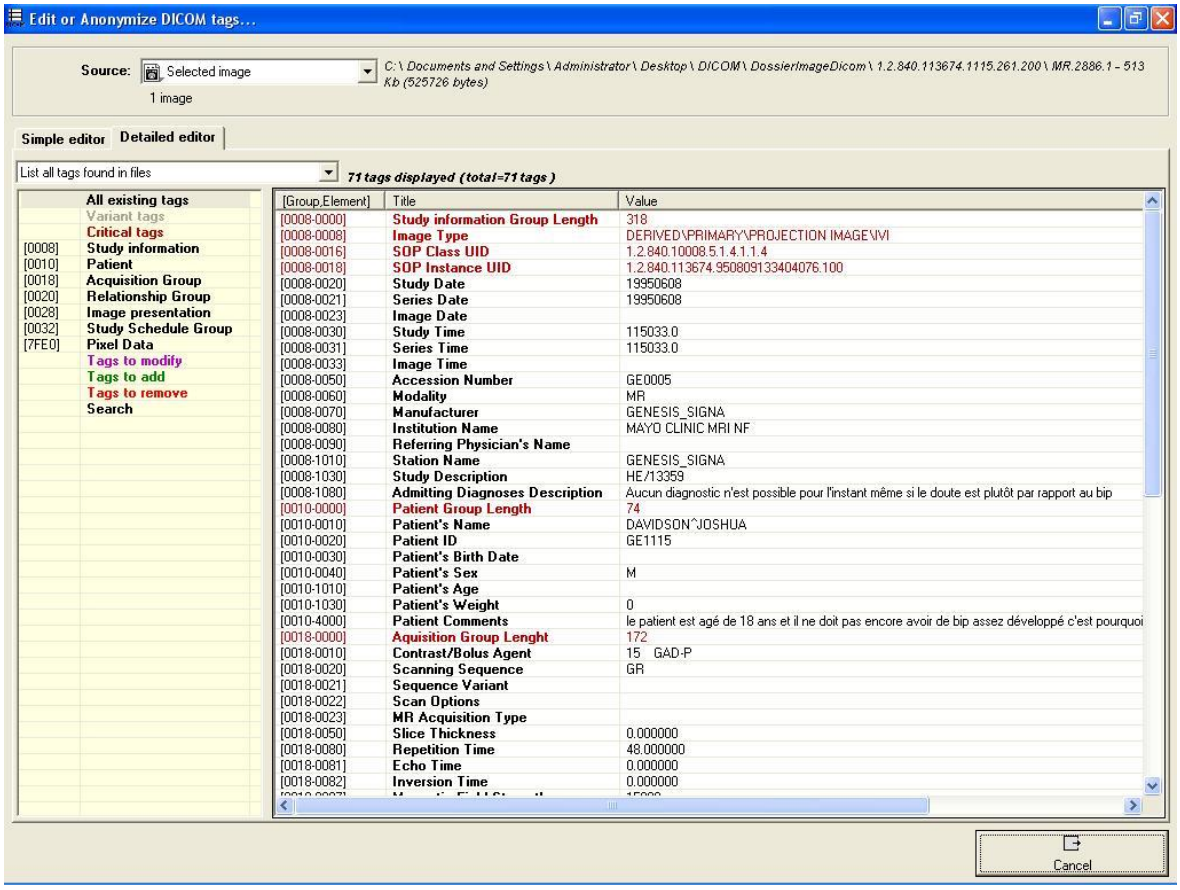


Figure.IV.11 structure de fichier DICOM

9. Particularités d'une image DICOM :

Une image DICOM peut être représentée en niveaux de gris ou en couleurs en utilisant un des systèmes R\TB ou CMJN ou bien en utilisant une palette de couleurs. Un pixel est représenté sur 8 bits, 16 bits ou plus suivant le nombre de nuances à représenter. DICOM permet aussi le réglage du fenêtrage. Le principe du fenêtrage consiste à ne pas lire l'intégralité de la matrice image en ne sélectionnant que certaines informations. Cette particularité est plus qu'appréciable dans le milieu médical ou il est important de considérer le maximum de nuances possibles. Par exemple, l'image d'un organe peut nécessiter un échantillonnage de 0 à 4096 alors qu'il n'est possible de visualiser que 256 niveaux à l'écran. Le fenêtrage nous permet donc d'avoir 16 représentations différentes de cette image.

Les pixels d'une image DICOM peuvent être stockés de manière native (sans compression), avec une compression sans pertes ou avec pertes. DICOM prévoit l'utilisation de plusieurs types de compression. La méthode de compression est spécifiée

dans la syntaxe de transfert. Chaque compression possède son propre UID de la syntaxe de transfert (Transfer Syntaxe UID).

Compression d'image progressive (JPEG2000 Interactive Ptotocol : JPIP) : Cette possibilité répond au besoin de transmettre les images de façon progressive, en permettant l'affichage des données avec une précision croissante au fur et à mesure de la transmission, afin de permettre à l'utilisateur de voir l'image avant la fin du transfert et de lui permettre de l'interrompre si celui- ci n'est plus nécessaire.

Du point de vue décodage et simplicité des applications de lecture et d'affichage, il est souhaitable de garder la matrice représentative sous forme native. Rappelons que pour qu'une AE puisse lire correctement une image compressée à partir d'un fichier DICOM, elle doit être compatible avec la méthode de compression utilisée. Cependant, vu le nombre croissant des images médicales dans les hôpitaux, et donc l'espace important qu'elles utilisent, la compression commence à gagner du terrain et l'intérêt qu'on lui porte commence à grandir.

10. Principe DICOM

Des modalités DICOM bien définies telles qu'un scanner, une IRM ou encore un PACS, vont traiter des objets DICOM (les images) en leur appliquant des services (affichage, copie, impression, etc.).

10.1. Objets DICOM

Qu'est-ce qu'un objet informatique ? Un objet est un conteneur symbolique qui possède sa propre existence et incorpore des informations et des mécanismes en rapport avec le monde réel, et qui sont traités dans un programme.

Derrière cette définition un peu floue, il faut concevoir un « objet » DICOM comme une encapsulation de données DICOM. Des mécanismes pourront ensuite être appliqués à cet objet. Ce dernier peut contenir un ou plusieurs autres objets.

Les données de l'objet sont appelées des champs DICOM ou encore des tags DICOM. Ces données seront par exemple une image au format .jpg, une vidéo au format AVI, une valeur de numéro unique d'examen, une valeur de numéro unique d'image, un IPP patient, une date de naissance, des informations sur les examens, etc.

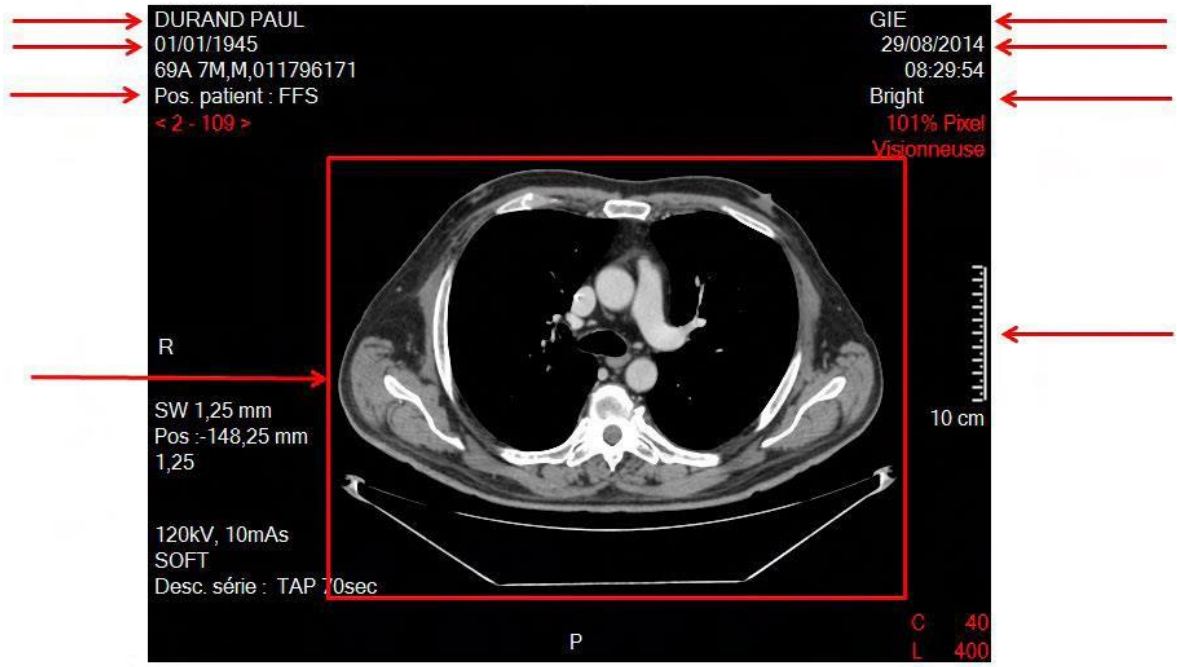


Figure IV.12.Image DICOM et objets associés

Pour comprendre simplement la notion d'objet DICOM Prenons l'exemple de scanner du patient Paul Durand qui a scanné de 600 images composé de trois séries de 200 images chacune. Il s'agit d'une série par région anatomique scannée, soit une série du thorax, une de l'abdomen et une du pelvis (bassin). Considérons que cet examen est contenu dans une grosse boîte. Le libellé de l'examen « Scanner Thorax Abdomen Pelvis de Paul Durand » y est inscrit. Cette boîte représente un objet DICOM. À l'ouverture, on y découvre d'autres boîtes : une intitulée « données patient », une autre « série Thorax », une « série abdominale », une « série pelvis », une « données de l'examen d'imagerie », etc.

À l'ouverture, la boîte « données patient » contient également d'autres boîtes : celles du nom, du prénom, de la date de naissance, etc. Ces mêmes contenants renfermeront des valeurs, à savoir « Durand » pour la boîte « nom » et « Paul » pour « prénom ».

Dans la boîte « données de l'examen d'imagerie », nous trouverons les boîtes « numéro unique d'identification de l'examen », « date de l'examen », « libellé de l'examen », « lieu de réalisation de l'examen », ou encore « modalité d'imagerie utilisée ». Celle intitulée « numéro unique d'identification de l'examen » contient une valeur qui n'est autre que le numéro unique de l'examen (l'accession number).

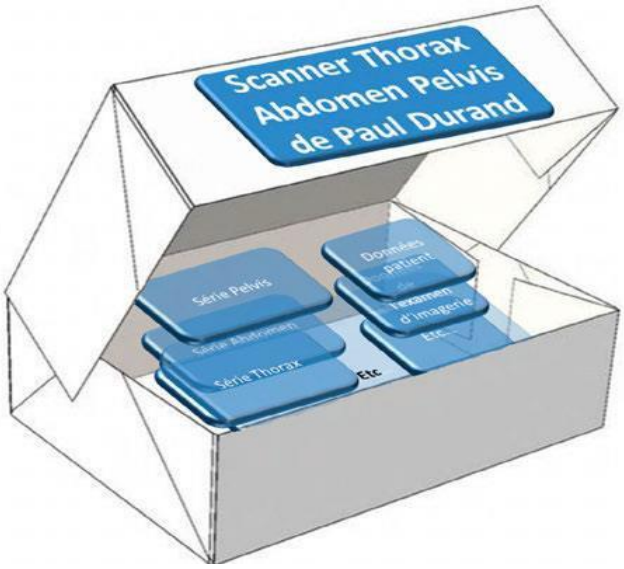


Figure IV.13. Boîte « Scanner Thorax Abdomen Pelvis de Paul Durand »

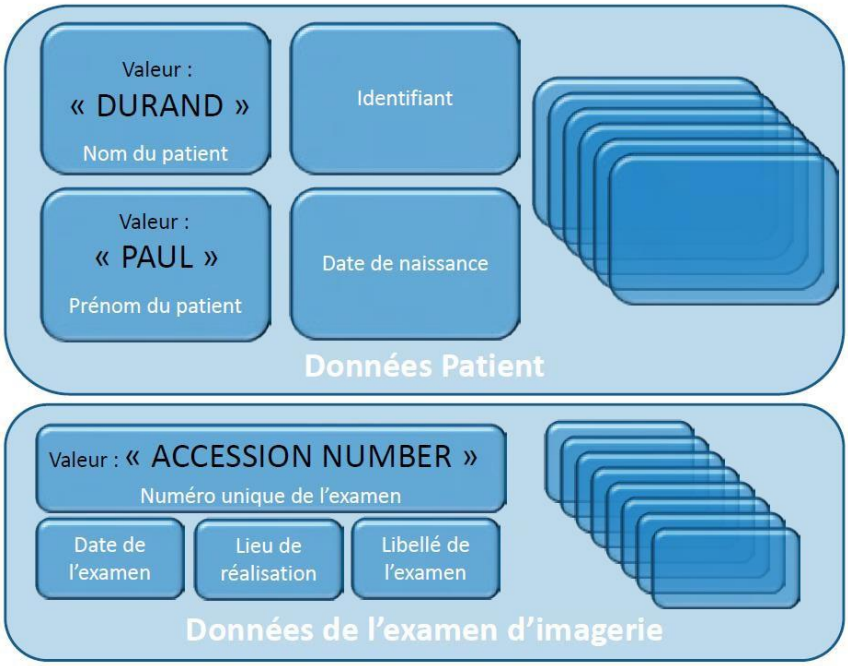


Figure IV.14 :.Boîtes « données patient » et « données de l'examen d'imagerie »

Enfin, la boîte « série Thorax », se décompose en une boîte « libellé de la série » contenant la valeur « Thorax », puis 200 boîtes libellées « image 001 », « image 002 », jusqu'à « image 200 ». Chacune des boîtes « images n » contient deux objets DICOM : une valeur « image » et un objet « données associées à l'image ». La valeur « image » est l'image réalisée en tant que telle. Il s'agit par exemple d'une image au format .jpg, compressée avec ou sans perte : le format « jpeg lossy » pour les images compressées avec pertes et le format « jpeg

lossless » pour celles compressées sans perte. L'objet « données associées à l'image » contient entre autres la valeur « numéro unique de l'image ».

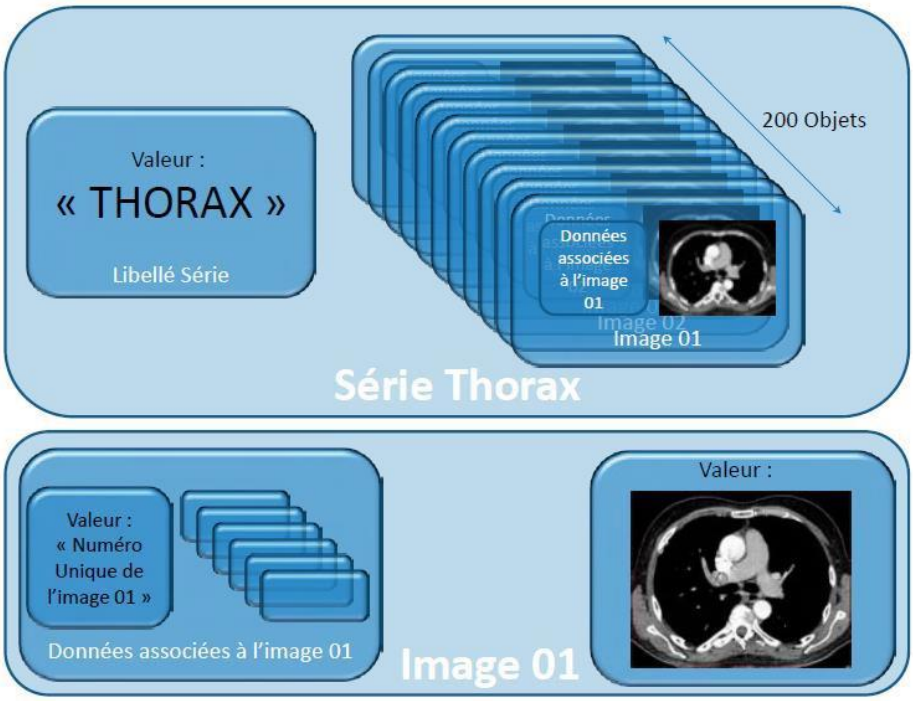


Figure IV.15.Boîtes « série Thorax » et « image 01 »

10.2. Services DICOM

Le traitement des objets DICOM se fait par l'application de mécanismes qu'on appelle des services. Nous présentons ici une série d'exemples de services DICOM nécessaires au transfert d'informations entre les modalités d'imagerie et les outils informatiques.

- Storage DICOM : copie d'images d'une modalité DICOM vers une autre, l'exemple le plus fréquent étant le transfert des images de la modalité d'acquisition vers le système d'archivage.
- Print DICOM : impression de films/images ; il s'agit du transfert d'informations d'une modalité DICOM vers une imprimante DICOM, comme un reprographe.
- Query/Retrieve DICOM : interrogation d'objets DICOM, à savoir un ou plusieurs examens, ou encore des séries d'examens pour afficher des images sur l'écran de l'ordinateur.
- C_Find DICOM : acquisition de la worklist, etc.

10.3. Comprendre les services DICOM

Reprenons l'exemple de l'objet DICOM Scanner Thorax Abdomen Pelvis de Paul Durand du paragraphe précédent et appliquons-lui différents services.

- Service Storage (par exemple rangement/copie) : nous demandons au scanner d'envoyer, au format DICOM, une copie de l'objet DICOM « Scanner Thorax Abdomen Pelvis de Paul Durand » qu'il vient de créer, à la destination système PACS de gestion des archives.
- Service Query/Retrieve : puis à partir d'un visualiseur d'images DICOM quelconque, installé sur un PC du réseau, nous appliquons le service de Query/Retrieve sur l'objet DICOM « Scanner Thorax Abdomen et Pelvis de Paul Durand » archivé sur le PACS.

Pour cela, nous interrogeons, en langage DICOM, le PACS pour qu'il nous liste les examens disponibles en visualisation pour le patient Paul Durand : c'est le service « Query » (Questionnement). Le PACS répond en présentant à l'utilisateur la liste des examens d'imagerie archivés pour le patient sélectionné. Ensuite, nous choisissons dans la liste l'examen (l'objet DICOM) « Scanner Thorax Abdomen et Pelvis de Paul Durand » pour l'afficher sur notre écran : c'est le service « Retrieve ».

- Service Print : enfin, si nous souhaitons imprimer sur film une image du « Scanner Thorax Abdomen Pelvis de Paul Durand », nous appliquons un service « Print » à l'image affichée. Le reprographe destinataire comprendra le message et réalisera l'opération d'impression.

10.4. Identification DICOM

Pour traiter et échanger des objets, les modalités d'imagerie doivent impérativement discuter entre elles et se comprendre (standard DICOM). Elles doivent aussi se localiser logiquement sur le réseau. Par conséquent, chaque modalité possède trois informations de paramétrage indispensables à la communication. Nous pouvons comparer cette « localisation » aux informations nécessaires pour le courrier postal. Tout comme une boîte aux lettres est dotée d'un nom, la modalité d'imagerie doit posséder un nom propre qu'on appelle un AET, soit Application Entity Title. Cette boîte aux lettres est située à une adresse précise ; de même pour la modalité qui est aussi localisée à une adresse précise et fixé du réseau informatique de l'établissement : il s'agit de l'adresse IP

(Internet Protocol). Enfin, la trappe de la boîte aux lettres doit être accessible et ouverte pour y glisser le courrier. Cela revient à dire ici qu'elle « autorise » le courrier à y être déposé par le facteur. De manière identique la modalité d'imagerie doit autoriser la communication des informations d'imagerie médicale. Pour cela, il faut que son port d'écoute soit ouvert. Un port d'écoute est un numéro logique qui permet de différencier les services auxquels on peut accéder.

11. Une norme orientée réseau

L'évolution de l'imagerie médicale a vu évoluer, en parallèle, le monde de l'informatique en général et des réseaux en particulier, surtout avec le concept client/serveur qui a mené à l'avènement de réseaux de plus en plus étendus tel Internet. Au sein des institutions médicales, les systèmes d'information se sont aussi développé et ont vu l'installation de réseaux étendus et performants. C'est ainsi que DICOM s'est orientée vers le domaine du réseau. Il a fallu alors standardiser la norme suivant le modèle OSI « Open Systems Interconnection » de l'ISO. Rappelons que le modèle OSI définit 7 couches différentes qui sont :

- La couche « physique » est chargée de la transmission effective des signaux entre les interlocuteurs. Son service est typiquement limité à l'émission et la réception d'un bit ou d'un train de bit continu (notamment pour les supports synchrones).

- La couche « liaison de données » gère les communications entre 2 machines adjacentes, directement reliées entre elles par un support physique.

- La couche « réseau » gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets.

- La couche « transport » gère les communications de bout en bout entre processus (programmes en cours d'exécution).

- La couche « session » gère la synchronisation des échanges et les « transactions », permet l'ouverture et la fermeture de session.

- La couche « présentation » est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaines d'octets effectivement transmises.

- La couche « application » est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

DICOM s'est donc vue enrichie avec des parties définissant des protocoles de communication réseau. Cependant, DICOM ne normalise que la communication, au niveau applicatif, entre machines physiquement connectées. Le protocole ne décrit pas les communications à un niveau physique (connecteurs, cables...), ni au niveau des protocoles réseau (TCP/IP) (Transmission Control Protocol / Internet Protocol). La norme DICOM permet donc la communication d'une application à une autre.

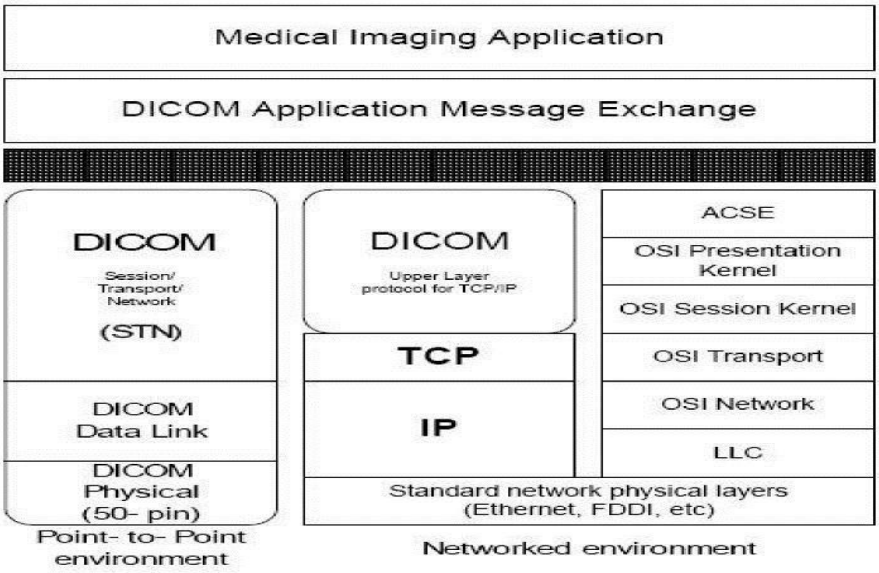


Figure .IV.16 : Couches réseau gérées par DICOM

11.1. La communication entre les machines :

La communication entre machines conformes DICOM s'effectue avec l'échange de messages DICOM (DIMSEs). Il existe deux types de DIMSEs :

- Les opérations (store, print ...) .
- Les notifications (rapports d'évènement...).

La communication entre deux dispositifs passe par plusieurs étapes, il y a d'abord établissement de la connexion, ensuite échange des SOP Class disponibles et supportées par chaque dispositifs. Ensuite le SCU envoie une requête que le SCP exécute. Après la fin de l'opération, la connexion est clôturée.

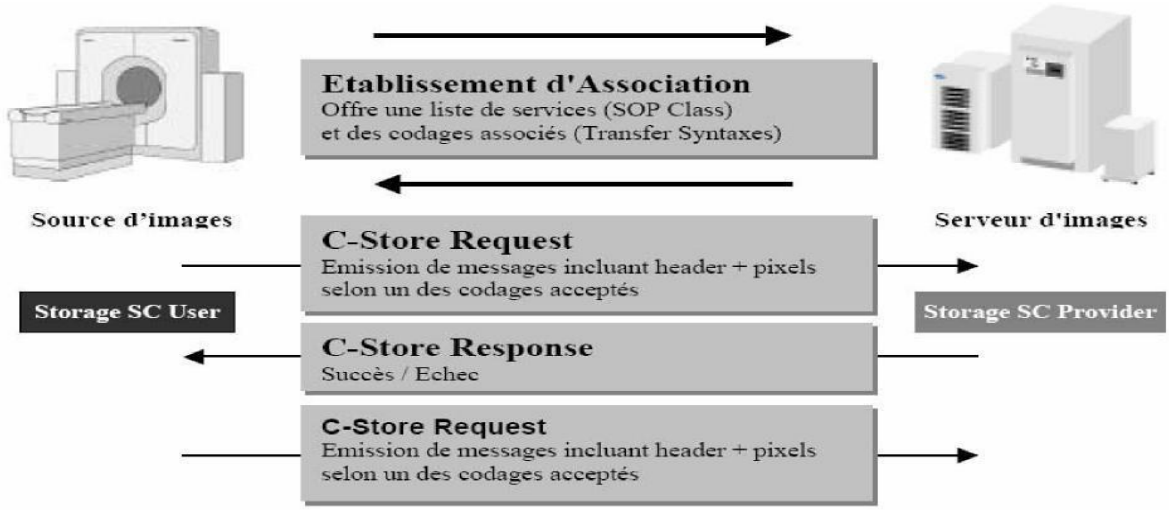


Figure .IV.17: Exemple d'une communication entre deux dispositifs (Opération exécutée : stockage d'images)

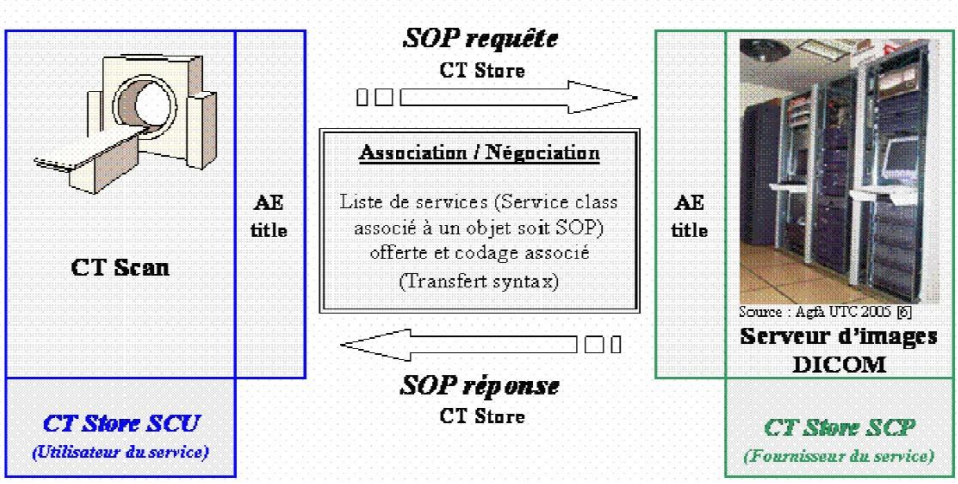


Figure IV.18 : Transmission d'images par DICOM

Exemple négociation SCU-SCP : Je veux transmettre mon image IRM au Serveur a partir de MR Storage SCU avec (Adresse IP: x.x.x.x et AETitle: Dem)

Pour commencer il faut contacter le serveur avec les Coordonnées Storage SCP:

Adresse IP: x.y.y.y ; AETitle: Serv et n° de port: 104

Dem : Hello Serv, Je suis Dem.Je veux travailler avec toi.

Serv :OK Dem. Que puis-je faire pour toi?

Dem : Peux-tu me fournir le service «avec la SOP Class UID suivante : 1.2.840.10008.5.1.4.1.1.4 ?

Serv : Pas de problème, je gère le service Storage pour les images IRM.

Dem : OK pour le DICOM VR Implicit Little Endian ! UID: 1.2.840.10008.1.2

Serv : Pour la syntaxe de transfert, j'accepte le Dicom VR Implicit Little Endian et le Dicom VR Explicit Big Endian.

Dem : Prends-tu en charge la compression JPEG LossLess Ou Lossy

Serv : Non !

Dem : Je vais donc te transmettre mon image avec toutes les données associées pour la SOP Class MR Storage en Dicom VR Implicit Little Endian.

Serv :marché conclu…ok bien reçu

11.2. MODE DE FONCTIONNEMENT

Le réseau doit être constitué de trois types de serveurs fonctionnant sous le système d'exploitation Windows 2003 Serveur. Le serveur Web héberge l'applet Java qui assure l'interrogation de la base de données et la mise à disposition en réseau interne des images médicales. Le serveur DICOM assure le stockage des images en s'appuyant sur une base de données SQLServer.

La confidentialité est obtenue grâce à la structure hiérarchique du format DICOM. Celle-ci se retrouve en pratique, au sein d'une base de données identifiant séparément et dans l'ordre : le patient, les propriétés de l'examen, les séries de l'examen, les paramètres des images et enfin le chemin exact vers ces images [FigIV.19].

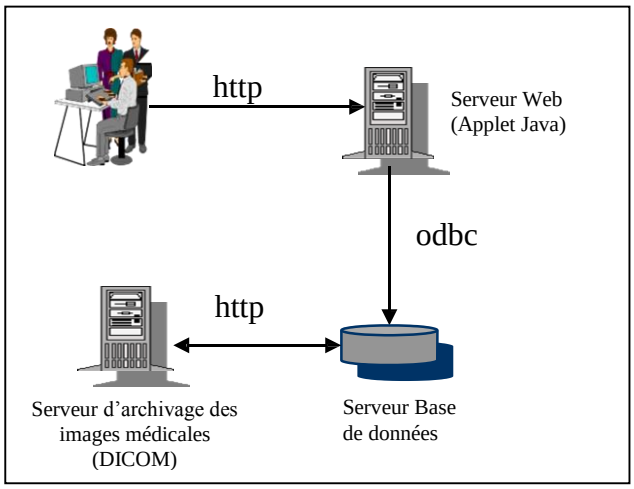


Figure. IV.19 : Mode fonctionnement

Le scénario d'accès à la plateforme se déroule comme suit; le client formule sa requête HTTP pour lancer l'exécution de l'applet Java qui se trouve dans le Serveur Web, cette

dernière sera téléchargée à son niveau, où elle va être exécutée. Cette applet permet selon la demande permettent soit d'accéder à la base de données SQL Server via la passerelle ODBC (Open DataBase Connectivity), cette base contient des liens vers les images médicales Dicom qui se trouvent au niveau du Serveur d'Archivage DICOM. L'applet permet de visualiser les images Dicom et de les traiter.

12. Conclusion :

La norme DICOM a apporté beaucoup d'améliorations au domaine de l'imagerie médicale. Elle a d'un côté simplifié les échanges en supprimant les formats propriétaires, et de l'autre facilité le stockage et l'accès aux différentes informations relatives aux images médicales.

Grace à son procédé d'identification unique robuste, DICOM s'est imposée comme une norme fiable et efficace. De plus, elle a facilité la création de bases de données consultables par les spécialistes de la médecine et a paré à quelques failles médico-légales existantes dans les systèmes qui l'ont précédé.

Autre avantage de cette norme, sa modification est aisée ce qui lui a permis d'être toujours à la page et de suivre l'évolution des technologies de l'information et de l'imagerie médicale.

Malgré le fait que DICOM ait été destiné initialement à la radiologie, son champ d'application s'est largement étendu aux autres applications de la médecine grâce à l'intégration d'autres représentants au sein du comité DICOM.

Le problème majeur de DICOM aujourd'hui est sa complexité, et l'absence du document en d'autres langues que l'Anglais.

Il existe une autre extension de DICOM spécifique à la radiothérapie s'appelle DICOM-RT qui propose un ensemble d'objets correspondant aux données requises à toutes les étapes de préparation et de suivi d'un traitement en radiothérapie.

Série de TD N°4 :

Exercice :

Le fichier DICOM c'est un dossier médical complet. En général, un examen médical s'effectue en une série de plusieurs tests, chaque fichier DICOM contenant toutes les métadonnées indispensables à l'identification du patient, de l'origine du cliché (modalité initiale, date et heure de l'examen, injection de contraste ou non, orientation particulière, et de sa technique de numérisation (type de numériseur utilisé, méthode de compression des données, nouvelle matrice, dynamique d'image, nom de la personne ayant numérisé les images, date et heure de numérisation, etc..).

1. Écrire un programme Matlab qui permet de :
   a) Lire l'image suivante `CT-MONO2-16-ankle` en DICOM

```
- I = dicomread('CT-MONO2-16-ankle.dcm');
b) Donner les propriétés  de cette image ?
- info = dicominfo('CT-MONO2-16-ankle.dcm');
- I = dicomread(info);
```

```
info =
                              Filename: [1x89 char]
                         FileModDate: '18-Dec-2020 11:06:43'
                              FileSize: 525436
                                Format: 'DICOM'
                         FormatVersion: 3
                                 Width: 512
                                Height: 512
                              BitDepth: 16
                             ColorType: 'grayscale'
      FileMetaInformationGroupLength: 192
          FileMetaInformationVersion: [2x1 uint8]
             MediaStorageSOPClassUID: '1.2.840.10008.5.1.4.1.1.7'
          MediaStorageSOPInstanceUID: [1x50 char]
                    TransferSyntaxUID: '1.2.840.10008.1.2'
               ImplementationClassUID: '1.2.840.113619.6.5'
```

   c) Quels sont les infos contenues dans ce fichier image ? cité les avec leurs étiquettes ?

- Cette commande en Matlab, nous donne des informations générale sur le fichier image DICOM et elle nous donne pas des informations détailler tel que l'identification du patient et autre…
- [0008] Identification de la machine : date d'examen (18-12-2020) ; et la version de DICOM N°3 , l'heurs de l'examen est 11 :06 et le fabricant de la machine ou le constructeur est définie par le code « ImplementationClassUID: '1.2.840.113619.6.5' »
- Certains constructeurs de matériel médical ont défini leur propre SOP Class UID, pour désigner un type d'image particulier. Donc, le constructeur est GE 'général Electric' ;avec le nom de SOP' GE Dicom Display Image Info Object'

- [0028] Infos sur l'image et le type de codage : image 3 D , Largeur 192; de taille 512 *512, codé sur 16bits.
- [7FE0] Pixels de l'image.
- UID '1.2.840.10008.1.2' avec la syntaxe de Transfer : Implicit VR Little Endian: Default Transfer Syntax for DICOM
- Pas d'info sur : l'identification de patient, le type d'examen ; hôpital ou institution,

d) Cette image est codée sur 8 ou 16 bits ? Affichez l'image ou on met automatiquement à l'échelle la plage d'affichage de sorte que la valeur minimale de pixel soit noire et la valeur maximale de pixel soit blanche.

- imshow(I,'DisplayRange',[])

e) Lisez les métadonnées du fichier DICOM.

- info = dicominfo(dicomFile);

f) Je veux transférer cette image au serveur avec les Coordonnées Storage SCP:

Adresse IP: x.y.y.y ; AETitle: **Ismail** et n° de port: 80. Quels sont les informations ou données envoyer a **ismail** pour que vous transmettre cette image avec toutes les données associées ?

- Pour transmettre cette image ; ismail a besoin : SOP class UID : '1.2.840.10008.5.1.4.1.1.7' et syntaxe de Transfer UID '1.2.840.10008.1.2'

g) Définissez le PatientName avec une valeur artificielle à l'aide de la représentation de valeur Nom de personne (PN).

- info.PatientName = 'BOUKLI_HACENE^ISMAIL';

h) Écrivez l'image avec les métadonnées modifiées dans un nouveau fichier DICOM.

- dicomFileNotAnon = 'ankle_notAnon.dcm';
- dicomwrite(I,dicomFileNotAnon,info);

i) Lisez les métadonnées du fichier DICOM non anonyme, puis confirmez que le nom du patient dans le nouveau fichier n'est pas anonyme.

- infoNotAnon = dicominfo(dicomFileNotAnon);
- infoNotAnon.PatientName
- ans = *struct with fields:*
- FamilyName: 'BOUKLI_HACENE'
- GivenName: 'ISMAIL'

j) Pour identifier la série à laquelle appartient l'image non anonyme, affichez la valeur de la propriété SeriesInstanceUID.

- infoNotAnon.SeriesInstanceUID

ans =
'1.2.840.113619.2.1.2411.1031152382.365.736169244'

k) Anonymisez le fichier à l'aide de la fonction dicomanon. La fonction crée une nouvelle série avec de nouvelles valeurs d'étude, modifie certaines des métadonnées, puis écrit l'image dans un nouveau fichier.

- dicomFileAnon = 'ankle_anon.dcm'
- dicomFileAnon = 'ankle_anon.dcm'
- dicomanon(dicomFileNotAnon,dicomFileAnon);

Lisez les métadonnées du fichier DICOM anonyme.

- infoAnon = dicominfo(dicomFileAnon);

l) Confirmez que les informations sur le nom du patient ont été supprimées.

- infoAnon.PatientName

ans = *struct with fields:*
FamilyName: '' GivenName: '' MiddleName: '' NamePrefix: '' NameSuffix: ''

m) Confirmez que l'image anonyme appartient à une nouvelle étude en affichant la valeur de la propriété SeriesInstanceUID.

- infoAnon.SeriesInstanceUID

ans = '1.3.6.1.4.1.9590.100.1.2.332976487717284553325912857110685666132'

1. INTRODUCTION

C'est avec l'apparition des ordinateurs, et surtout avec Internet, que les images sont devenues omniprésentes et prépondérantes. Voilà pourquoi depuis quelques années, les centres de recherche en informatique dépensent de nombreuses heures sur des algorithmes de compression. Afin de limiter la taille, ou le poids, d'une image, nous devons la compresser, c'est-à-dire éliminer les informations inintéressantes ou redondantes. Il existe de nos jours plus d'une vingtaine de formats de compression, spécifiquement dans la compression d'image (.gif, .jpeg, .bmp…), ayant chacun leur propre méthode de codage, ou cumulant plusieurs algorithmes, mais tous sont complémentaires.

Une image numérique est une matrice composée d'échantillons élémentaires appelés pixels. Nous appellerons M le nombre de lignes de l'image et N le nombre de colonnes. A chaque pixel d'une image monochrome est associée une valeur numérique à laquelle correspond un niveau de gris, par contre dans l'image couleur le pixel sera un vecteur de trois composants (RGB). En général, le nombre des niveaux de gris est une puissance de deux. Nous considérons, à titre d'exemple, pour une image avec des pixels ayant des niveaux de gris représentés avec des nombre allant de 0 à 255, nous aurons 256 valeurs possibles codées sur 8 bits par pixel (bpp). Notons que par convention le niveau de gris '0' correspond à du noir et le niveau de gris '255' à du blanc. Le nombre de bits par pixels R est appelé « débit ». Nous notons R_0 le débit de l'image originale avant compression et Rc son débit après compression.

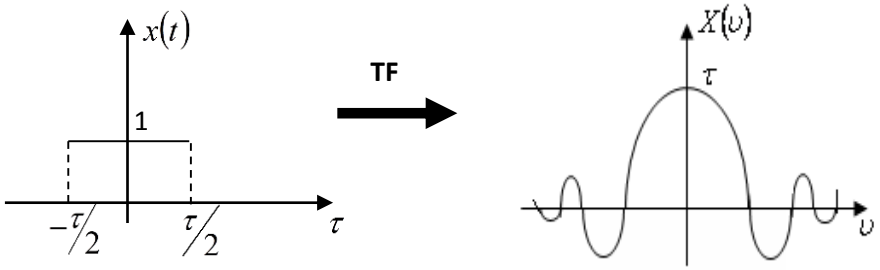
L'image originale est une matrice de pixels qui occupe un total : $Bo=M.N.Ro$ bits. L'image compressée est une suite de bits qui occupe Rc bits. Nous voyons que $Rc=Bc/M.N$ correspond au nombre des bits moyens ramené au nombre de pixels. Cependant l'image compressée n'est généralement pas physiquement composée de pixels. La décomposition est nécessaire pour représenter l'image décomprimée sous forme de pixels visibles. L'image décompressée occupe alors la même place que l'image originale soit Bo bits, en subissant éventuellement une distorsion dûe à la compression. Par abus de langage, nous appellerons souvent par la suite « image compressée » une image qui aura en réalité subi successivement l'opération de compression et l'opération inverse de décompression.

2. CLASSIFICATION DES METHODES DE COMPRESSION

La quantité en intense d'images médicales nécessité des moyens de stockage de plus en plus important, a cette allure le seuil de saturation est très vite atteint. Donnons un exemple simple pour étayer ce que nous avançons : un hôpital classique de 200 lits produit en moyenne, chaque année 875 To de données images. De surcroît si l'on devrait transmettre ces images alors la durée de transmission se pose également.

La solution de ces problèmes consiste à opter pour la compression des données. Il est instructif de présenter la compression de donnés sous sa forme la plus simple. Considérons un signal : $x(t)=\Pi_{\tau}(t)$ pour $t \in \Re$. τ : Étant la durée de l'information.

Sa transformée de Fourier s'écrit sous forme : $X(\upsilon)=\tau \sin c(\tau\upsilon)$



D'après les deux représentations ; il est clair que l'information temporelle est compressée, le signal est bornée entre $-\tau/2$ et $\tau/2$ tandis que l'information spectrale est étalée.

Il apparaît clairement que l'objectif de la compression d'images est de condenser l'information « image » sans toutefois altérer son contenue informationnelle. Aussi, il est à noter que cette technique implique une opération de codage de plus, elle exploite les différentes corrélations spatiales et temporelles.

Enfin la qualité de la compression des images médicales doit tenir compte des éventuelles distorsions pouvant influencer l'interprétation qualitative des images et la valeur des paramètres anatomiques ou fonctionnels reflétant l'état de l'organe étudié.

Dans ce chapitre nous allons passer en revue les différentes techniques de compression, leurs avantages et leurs inconvénients.

Les méthodes de compression peuvent être regroupées, en deux classes :

1- Les méthodes sans perte d'information (sans distorsion ou réversible).

2- Les méthodes avec perte d'information (avec distorsion ou irréversible).

2.1.Méthodes de compression sans perte d'information

Les méthodes de compression sans pertes d'informations permettent de retrouver exactement toute l'information contenue dans l'image numérique originale. Il existe plusieurs méthodes de compression sans pertes, basées sur le codage ou prédiction nous présentons ici celles que l'on retrouve souvent dans la littérature et qui sont basées sur le codage entropique.

Notion d'entropie d'une source

Shannon adapte le concept d'entropie, introduit par Boltzmann et Gibbs en thermodynamique, aux probabilités, et introduit l'entropie d'une probabilité afin de mesurer la quantité d'information ou l'incertitude d'une source d'information : si *E* est un ensemble fini, et *P* une probabilité sur *E*, l'entropie de *P*, dite entropie de Shannon, est donnée par

$$H = -\sum_{i=1}^{i=N} p(i).\log_2 p(i) \quad [bpp] \qquad \text{V.1}$$

a) Codage RLC (Run Length Coding)

Plutôt que de coder seulement le message lui-même, il est plus intéressant de coder un message contenant une suite d'éléments répétitifs par des couples (nombre de symboles S consécutifs, S). Le codage RLC ne perd pas d'information il est dit réversible, il est efficace quand le message est composé de suites de symboles identiques. Au lieu de coder indépendamment chaque symbole.

Voici un exemple de RLC applique sur des images binaires (N & B)

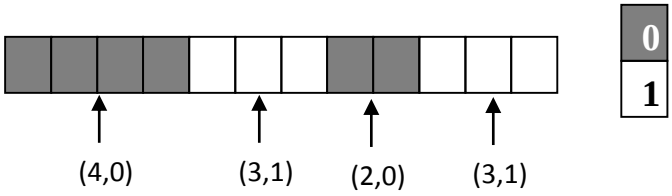


Fig. V.1: *Codage RLC d'une séquence*

b) Le codage de Huffman

Le mathématicien, David Huffman, a proposé en 1952 une méthode statistique qui permet d'attribuer un mot de code binaire aux différents symboles à compresser (pixels ou caractères par exemple). La longueur de chaque mot de code n'est pas identique pour tous les symboles: les symboles les plus fréquents (qui apparaissent le plus souvent) sont codés avec de petits mots de code, tandis que les symboles les plus rares reçoivent de plus longs codes binaires.

Le principe est le suivant:

1. Les probabilités d'occurrence de chaque message sont placées dans une liste dans un ordre décroissant. Nous dirons que la liste est composée d'enfants.
2. Les deux probabilités les plus faibles sont identifiées en fin de liste.
3. La somme des deux probabilités est placée à sa place dans la liste triée. Elle constitue un nœud parent. Les deux enfants sont retirés de la liste.
4. Le chemin «enfant de plus faible probabilité, parent» est codé par un 1, l'autre par un 0.
5. La procédure reprend à l'étape 2 jusqu'à ce qu'il ne reste plus qu'une probabilité dans la liste.

c) La compression LZW

Le système de compression d'image le plus utilisé à travers le monde reste la compression LZW (acronyme de ses inventeurs Lempel-Ziv-Welch). Cet algorithme utilise, comme la compression de Huffman vue précédemment, un tableau, un dictionnaire pour réaliser une compression du type non-destructrice. Contrairement au codage précédent, la compression LZW n'encode pas dans le fichier le dictionnaire, celui-ci sera reconstruit lors de la décompression. Le LZW est un dérivé du codage LZ. Les concepteurs, Abraham Lempel et Jakob Ziv utilisaient principalement le principe de compression LZ dans un autre format, nommé LZ77, dédié aux programmes d'archivage. Les formats ZIP, ARJ et LHA basent leur compression sur cet algorithme.

2.2.Méthodes de compression avec perte d'information par transformation

Les méthodes de compression par transformation n'agissent pas directement sur l'image numérique dans sa représentation canonique, mais dans le domaine de la transformée. Il est bien connu qu'une transformation permet de mettre en évidence certaines propriétés de l'image que la représentation originale ou canonique ne laisse pas apparaître.

En partant d'un ensemble de valeurs numériques corrélées d'une image, le but est d'obtenir un autre ensemble de valeurs le moins corrélées possible dans l'espace transformée. En général, les schémas de codage par transformation subdivisent l'image de taille $N \times N$ en sous images de taille plus petites avant de faire subir à ces sous images une transformation. Nous privilégions les transformations unitaires et qui conservent l'énergie. La transformation consiste en la décomposition de l'image dans une base adéquate de fonctions telles que les coefficients de la transformation soient indépendants et qu'un nombre minimum de ces coefficients contienne une proportion importante de l'énergie de l'image. Ainsi, on pourra mettre à zéro certains d'entre eux sans nuire de manière significative ni à la quantité d'énergie,

ni à l'aspect visuel de l'image reconstruite. Une transformation adéquate pour la compression d'image devrait permettre la décorrélation des coefficients transformés, la conservation d'énergie ou sa condensation dans un nombre minimum de coefficients et enfin posséder un algorithme rapide. Les transformations linéaires sont les plus utilisées car ayant des expressions analytiques simples et s'implémentant assez vite. Pour satisfaire la contrainte de décorrélation, on utilise les bases orthogonales et les transformations utilisées en compression sont orthogonales. Autrement dit, ce sont des opérations séparables, c'est-à-dire que l'opération en deux dimensions est équivalente à deux opérations successives à une dimension, l'une horizontalement et l'autre verticalement. Il existe de très nombreuses de transformations orthogonales parmi lesquelles, la transformée de Karhunen- loeve, la transformée sinus, cosinus…

a) Transformation de Karhunen- loève (KLT)

On appelle transformée de Karhunen- loève, la transformation optimale au sens où tous les coefficients obtenus sont décorrélés et que la quasi-totalité de l'énergie est conservée par un minimum de coefficients. Malheureusement les éléments de la transformation, notamment la matrice, dépendent de l'image dont il faut entre autre calculer la moyenne et la covariance. Par ailleurs, il n'existe pas d'algorithme rapide pour le calcul de la transformation de Karhunen-loève. Toutes ces raisons font que cette transformation soit très peu utilisée dans la pratique. On lui préfère des transformations qui sont indépendantes des images et qui ont des algorithmes rapides, tels que les transformations spectrales en ondelettes.

b) Transformations spectrales ou sinusoïdales

La transformation de Fourier et celles qui s'en déduisent, telles la transformation en sinus, la transformation en cosinus, sont très utilisées en analyse et en filtrage du signal. Ces transformations possèdent des algorithmes rapides comme la *FFT (Fast Fourier Transform)* et ses variantes. La variable de l'espace transformé étant la fréquence, une telle décomposition permet de mieux observer la répartition fréquentielle de l'image. Etant donné que ce sont les premiers harmoniques qui contiennent la quasi-totalité de l'énergie, il est donc possible de mettre à zéro une proportion importante des coefficients et de coder l'image à moindre coût.

Malgré la rapidité de la transformation de Fourier, elle décompose l'image en une partie réelle et une partie imaginaire pouvant se convertir en module et argument ce qui n'est pas facile à manipuler ou à interpréter. Les traitements de ces données peuvent s'avérer lourds, d'où la préférence accordée à la transformation en cosinus qui bénéficie de toutes les caractéristiques de la *FFT*. La transformée en cosinus discrète *DCT (discret Cosine Transform)* a été choisie

comme standard par *JPEG (Joint Photographic Experts Group)* pour le codage d'images fixes et a fait l'objet de beaucoup d'études et d'applications de la compression dans tous les domaines de l'imagerie, y compris le médical. Contrairement à la transformation *KLT*, la matrice de transformation *DCT* est complètement indépendante de l'image.

D'autre part, cette norme *(JPEG)* présente un certain nombre d'inconvénients :

- L'efficacité de codage est limitée.
- Le codage par blocs de 8×8 pixels génère un effet de mosaïque à bas débit très gênant visuellement.
- La transmission d'images codées est très peu robuste en environnement bruité.
- Les applications liées à l'image sont de plus en plus spécifiques et nécessitent de nouvelles fonctionnalités non résolues par *JPEG*.

Donc c'est pour cela, nous allons introduire une autre transformation qui ignore en quelque sorte ces inconvénients et améliorer la compression d'image, c'est cette transformation que nous allons appliquer par la suite avec un nouveau codage plus puissant.

c) La transformation par ondelette discrète (DWT)

Les ondelettes c'est d'abord une théorie mathématique récente d'analyse du signal, développée dans les années 80. On peut considérer qu'il s'agit d'une extension de l'analyse de Fourier **.** L'intérêt de cette théorie est au départ l'analyse des signaux.

En traitement du signal, une analyse par Ondelettes est équivalente à un filtrage passe-bande.

En traitement d'images, la transformation en Ondelettes d'une image de résolution k donne :

- 3 sous images détails (coefficients d'Ondelettes) de résolution k+1, CV(k+1), CH(k+1) et CD(k+1), mettant en évidence les contours (localisation et orientation),
- 1 image d'approximation de l'image de départ à la résolution k+1, CA (k+1) / (Image de départ d'une nouvelle analyse (niveau k+2)).

Toutes les sous images de niveau k+1 sont sous échantillonnées (par rapport au niveau k).

La technologie de compression à base d'ondelettes offre une plus grande finesse au niveau de l'analyse du signal, et permet de mieux s'adapter aux propriétés locales de l'image.

L'intérêt de la transformation par ondelettes par rapport aux autres transformées de compression est que celle-ci ne considère pas l'image dans son ensemble pour la coder mais, la travaille par couche, cherchant à enregistrer les détails les plus importants à chaque résolution

Les étapes de compression par ondelettes sont usuellement :

1. Transformation par ondelettes.

2. Quantification : les valeurs des coefficients de détails inférieurs à un certain niveau sont éliminées, en fonction de l'efficacité recherchée. C'est cette étape qui introduit des pertes.
3. Codage des valeurs restantes : les données restantes sont transmises à un encodeur entropie, c'est à dire à un algorithme de compression de données (LZW, HUFFMAN, RLE,...).

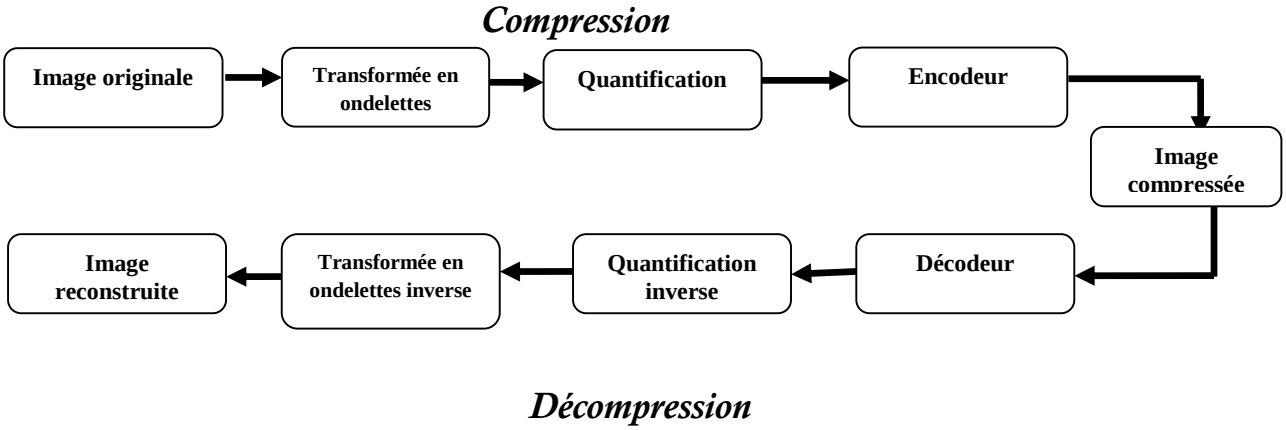


Fig. V.2: *Schéma général d'un algorithme de Compression / décompression par ondelettes*

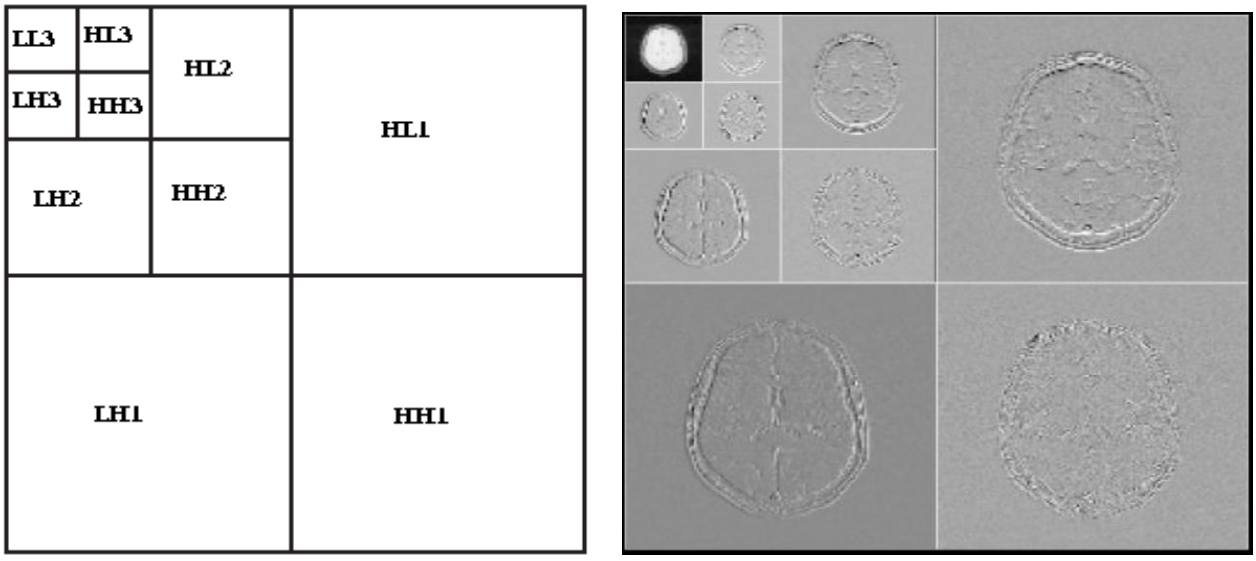


Fig. V.3: *Décomposition par ondelette (niveau de décomposition 3)*

Un coefficient d'Ondelette mesure la corrélation entre l'Ondelette et le signal dans l'intervalle considéré. Plus de 4 niveaux de décomposition n'améliore pas de manière sensible le taux de compression.

La transformation en ondelettes permet d'obtenir une représentation temps fréquence ou temps échelle. Elle a des propriétés d'adaptation ou de flexibilité très attrayantes notamment

le choix des fonctions de bases des ondelettes (orthogonales ou non à support compact ou infini, etc.…) et des paramètres de dilatation et translation .Les transformées en ondelettes conservent l'énergie du signal et possèdent notamment des algorithmes rapides, elles sont donc bien adaptées à la compression d'image (Figure II.3) .

L'intérêt des Ondelettes par rapport aux sinus et aux cosinus se situe surtout à deux niveaux :

- Contrairement aux sinus et cosinus qui ne sont bien localisés qu'en fréquence, les ondelettes le sont également en temps. Par conséquent tout changement de fréquence dans la transformée en ondelettes ne produira de changements que sur une certaine partie du domaine temporel.
- Les ondelettes permettent de représenter de manière compacte un grand nombre de fonction : ainsi les fonctions formées de pics près prononcés nécessitent beaucoup moins d'ondelettes que de sinus/cosinus pour être représentées

Les Ondelettes sont utilisées dans les deux catégories de techniques de compression que sont la compression sans pertes ou réversible (lossless) et celle avec pertes ou irréversible (lossy) .

D'autre part, cette norme (JPEG 2000) présente un certain nombre d'avantages :

Meilleur rapport compression/distorsion surtout pour les forts taux de compression.

- Le train binaire est organisé de façon progressive, soit par résolution, soit par raffinement de qualité.
- Le même algorithme autorise le codage avec et sans perte.
- Des régions d'intérêt peuvent être définies au codage et codées avec une meilleure qualité (éventuellement sans perte).
- des mécanismes de résistance aux erreurs de transmission peuvent être intégrés, permettant notamment de sécuriser la transmission

2.3.La stratégie de quantification

La quantification est un processus qui permet d'associer un nombre réel (respectivement vecteur de réels) à un nombre entier (respectivement un vecteur d'entiers).

On distingue en générale deux types de quantification :

-La quantification scalaire & -La quantification vectorielle

a) Quantification Scalaire

La quantification scalaire est une forme particulière de la QV, celle où la dimension des vecteurs est égal à un. La figure I.4 illustre la caractéristique en marche d'escalier du plus simple des quantificateurs scalaires (QS), celui uniforme à débit fixe qui est entièrement déterminé par :

les L+1 niveaux de décisions : $d_0, d_1, d_2, \dots, l$ qui partitionnent en L intervalles égaux l'axe des réels R et détermine le pas de quantification.

Les L valeurs de reproduction : qui sont les centres de masses de chacun des intervalles de décision.

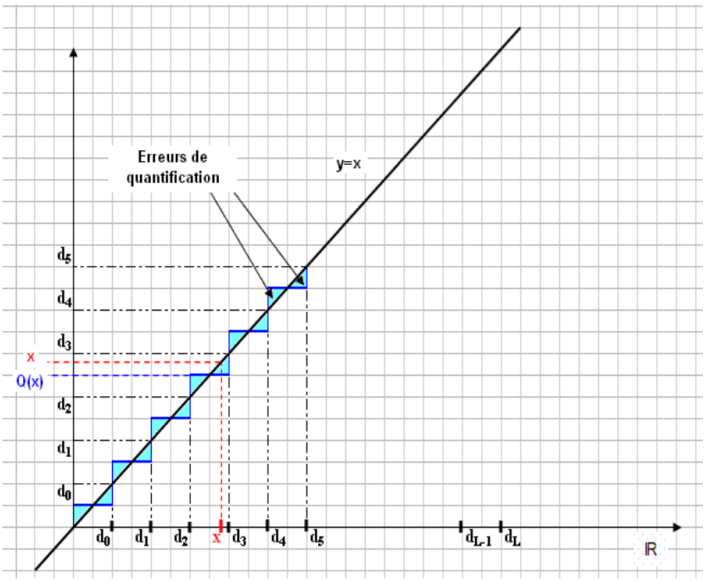


Fig. V.4 : *Exemple d'un QS uniforme pour L=5*

b) Quantification vectorielle

Le principe de la quantification vectorielle (QV) est très simple, il consiste à coder l'image est découpée en blocs qui ne se chevauchent pas mais qui couvrent toute l'image. Chaque bloc de taille *k* est comparé aux imagettes d'un ensemble de blocs, appelé dictionnaire.

$$C = \{y_1, y_2, \dots, y_N\} \subset \mathcal{R}^k \qquad \text{V.2}$$

Ces blocs prédéfinis sont nommés mots de code ou vecteurs de reproduction. La comparaison consiste à calculer une mesure de distance entre le bloc (vecteur) à coder et les mots de code. Le codage s'effectue en ignorant le bloc original et en gardant seulement l'indice

(l'adresse) du mot de code le plus proche. La distance appliquée est en général la distance euclidienne, ce qui est équivalent à la minimisation de l'erreur quadratique moyenne.

Le décodeur reprend tout simplement les mots de code correspondants aux indices reçus (transmis ou stockés), et reconstruit ainsi l'image (décompression).

Les opérations effectuées par un quantificateur vectoriel sont alors très similaires à la quantification scalaire. La QV réalise une fonction $Q : \mathfrak{R}^k \rightarrow C$, qui est la combinaison de deux opérations, celle du codeur et du décodeur *: Q(x)=D(E(x)).*

Le codeur est une fonction *: E :* $\mathfrak{R}^k \rightarrow I$ *où I = {1,2,..., N},* et le décodeur est la fonction *D : I* $\rightarrow$ *C*. Le bloc reconstruit est donc choisi par la fonction :

$$Q(x) = y_i : \left||x - y_i|\right| \leq \left||x - y_j|\right| \quad \forall j \in \{1 \dots N\}. \qquad \text{V.3}$$

Le taux de compression dépend du nombre de mots de code ainsi que de leur taille. Avec une taille du dictionnaire égale à $N=2^n$, le taux de compression η s'exprime par :

$$\eta = \frac{mk}{n} \qquad \text{V.4}$$

Où k est le nombre de pixels dans un bloc et m désigne le nombre de bits par pixel dans l'image originale.

n : est le nombre de bits par mots de code (en relation avec le nombre de bits par pixel dans l'image reconstruite).

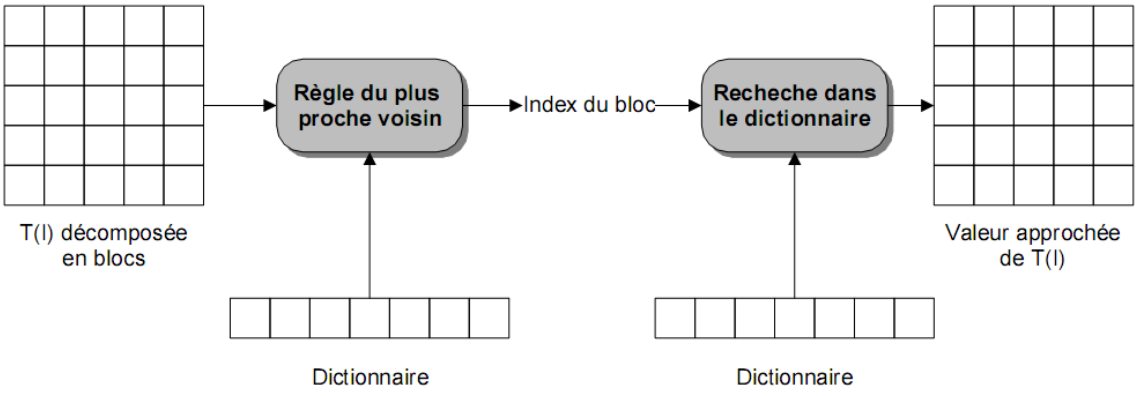


Fig.V.5 : *Principe de la quantification vectorielle*

Il y a plusieurs algorithmes basés sur la transformée en ondelette pour la compression des images. Ceux-ci incluent EZW, SPIHT, SFQ, CREW, EPWIC, EBCOT, SR, codage d'image en utilisant Embedded Zerotree Wavelet (EZW) et Partitioning In Hierarchical Tree (SPIHT).

3. Techniques de codage de sous bandes

Les deux grandes techniques utilisées dans la plupart des algorithmes sont le codage de Huffman et le codage arithmétique , toutes deux reposent sur un modèle statistique de l'image à coder. La compression consiste à coder le symbole le plus probable avec moins de bits que le symbole le moins probable.

Le codeur arithmétique donne les meilleurs résultats surtout quand il utilise un modèle adaptatif, il est d'ailleurs utilisé dans les algorithmes EZW et SPIHT. Le codeur et le décodeur doivent bien entendu avoir accès au même modèle puisque c'est lui qui détermine la distribution des probabilités de présence des différents symboles.

D'autre part le codeur arithmétique a l'avantage de faire clairement la distinction entre le modèle choisi pour représenter les données et le codage des informations avec ce modèle. L'implémentation proposée dans la littérature est d'ailleurs faite de telle sorte que l'on puisse facilement changer de modèle.

3.1.L'algorithme de codage EZW (Embedded Zerotree Wavelet)

L'idée de base de cet algorithme qui est proposé par Shapiro , est de trouver le meilleur ordre de transmission des coefficients de représentation en ondelettes.

Il est clair que la transmission des coefficients dans l'ordre décroissant de leur valeur absolue est la meilleure solution, puisque les coefficients les plus signifiants sont ceux dont la valeur absolue est la plus élevée. Shapiro proposa de transmettre les coefficients sous forme d'une suite de bits obtenue par enchaînement progressif des bits des coefficients les plus signifiants en commençant par les bits les plus importants. Cette nouvelle conception offre l'avantage à l'algorithme EZW de faire la transmission progressive d'image puisque le décodeur peut s'arrêter au niveau de n'importe quelle suite de bits. De surcroît nous aurons une meilleure image reconstruite avec cette suite de bits tronquée. Cet algorithme présente en plus l'avantage de ne nécessiter ni phase d'apprentissage, ni dictionnaire, ni l'information sur l'image source.

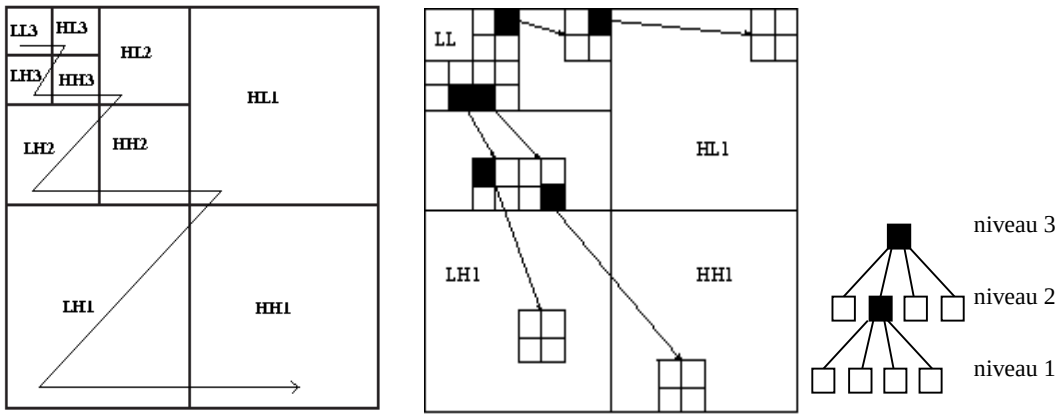
3.1.1. Schéma de l'algorithme EZW :

Après avoir calculé la transformée en ondelettes de l'image, l'algorithme code les coefficients transformés à l'aide d'une suite décroissante de seuils $T_{0.....}\ T_{N-1}$, avec $T_i = \frac{T_i}{2}$ et -

$T_0 < 2|c|$ pour tout coefficient *c* de la représentation en ondelettes. Pour coder les coefficients, l'algorithme effectue récursivement deux passes successives, ne traitant à chaque fois que les coefficients significatifs par rapport au seuil courant : ceux dont la valeur absolue est supérieure au seuil. Dans la première passe, la dominante de l'algorithme parcourt les coefficients de la transformée en ondelettes suivant l'ordre donné par la figure (V.6-a) pour la recherche des coefficients significatifs par rapport au seuil courant, en utilisant la hiérarchie donnée par la figure (V.6-b).

L'algorithme produit alors une sorte de carte marquant la position des coefficients significatifs ainsi que leur signe. Cette carte est obtenue en associant à chaque coefficient suivant sa valeur absolue et celle de ses fils l'un des symboles suivant : Zerotree (Z), Isolated Zero(IZ), Positive signifiant (POS) et Negative signicatif(NEG). **(L'algorithme de passe dominante)**

- Un coefficient est un Zerotree si lui et tous ses descendants ne sont pas significatifs, aucun symbole n'est alors associé à ses descendants.
- Izolated Zero signifie que le coefficient n'est pas significatif mais a des bases descendantes qui le sont.
- Les coefficients significatifs (valeur absolue supérieure au seuil) sont marqués Positive ou Negative selon que le coefficient soit positif ou négatif.



a- Ordre de parcours des coefficients *b- Organisation hiérarchique des coefficients*

Fig. V.6: *Les relations entre les coefficients d'ondelettes dans différents sous bandes*

Chaque coefficient significatif est ensuite mis à zéro dans la transformée en ondelettes afin que sa position ne soit plus encodée et sa valeur absolue est placée dans une liste pour la coder par approximations successives. En effet chaque carte est suivie d'une suite de symboles

'0' et '1' qui permettent au décodeur de fixer une valeur de reconstruction approximative aux coefficients significatifs. Cette valeur s'affine pour se rapprocher de plus en plus de la valeur réelle des coefficients au fur à mesure que des suites de symboles sont encodées **(l'algorithme de passe secondaire)** Cette suite est obtenue comme suit :

Si T_i est le seuil courant, alors les coefficients marqués dans la passe précédente ont leur valeur absolue dans l'intervalle $[T_i, 2T_i[$, cet intervalle est alors divisé en deux $\left[T_i, \frac{3T_i}{2}\right[$ et $\left[\frac{3T_i}{2}, 2T_i\right[$.

Les coefficients dont la valeur absolue se trouve dans le premier intervalle sont codés par le symbole '0', alors que ceux se trouvant dans le second intervalle nous leur associons le symbole '1'. Lorsque la seconde passe est finie, l'algorithme reprend le processus et génère la carte suivante dont le nouveau seuil étant T_{i+1}. Dans cette seconde étape un nouvel intervalle s'ajoute au deux précédents : $[T_{i+1}, T_i[$. Ces trois intervalles sont alors raffinés comme dans l'étape du cycle précédent pour transmettre une suite de symboles '0' ou '1', chaque symbole étant associe à un coefficient significatif. Lorsque le seuil initial T_0 est un multiple d'une puissance de deux, cette stratégie peut être vue comme la transmission des bits de la valeur absolue des coefficients, en commençant par les bits les plus significatifs. Ce processus récursif s'arrête lorsque T_{N-1} est atteint ou que le nombre de bits souhaité a été transmis.

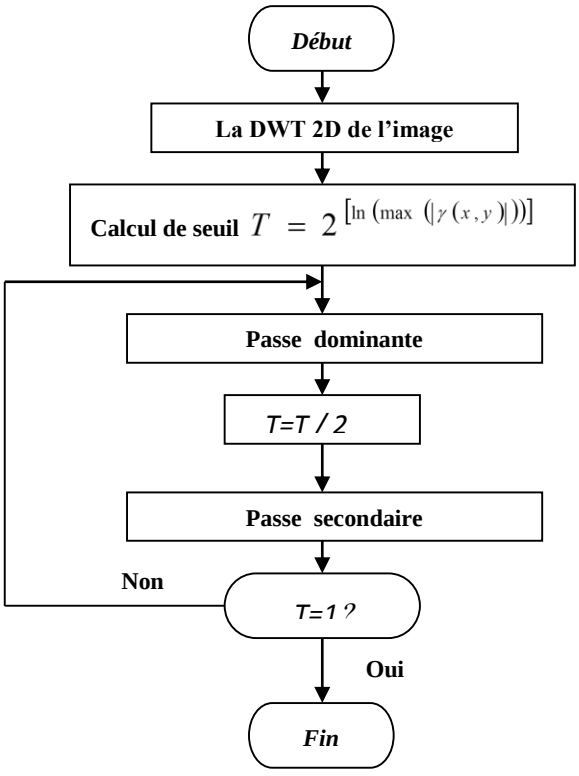


Fig. V.7: *Algorithme de EZW*

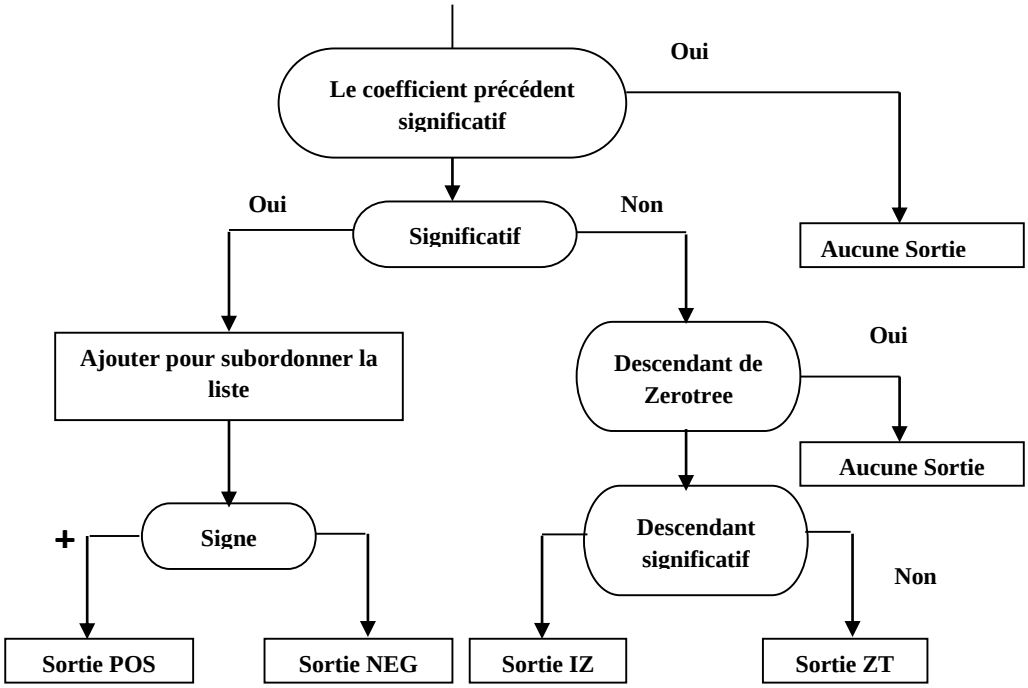


Fig. V.8: *Organigramme de passe dominante*

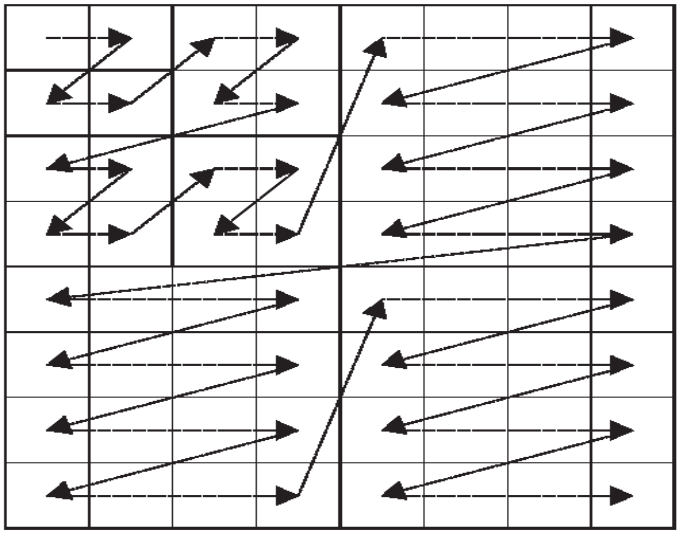


Fig. V.9: *Balayage du codage EZW*

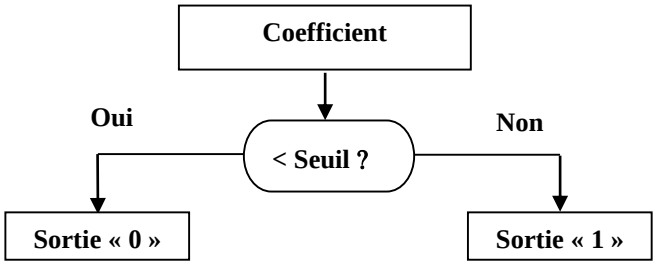


Fig. V.10: *Organigramme de passe secondaire*

3.2.L'algorithme de codage SPIHT (Set Partitioning In Hierarchical Tree)

L'algorithme SPIHT (*Set Partitioning In Hierarchical Tree*), proposé par Saïd et Pearlman, est une amélioration du schéma de codage EZW. Il repose sur les mêmes concepts : codage progressif par plans de bits et utilisation des dépendances hiérarchiques qu'entretiennent les coefficients d'une pyramide de décomposition 2D. L'algorithme est cependant plus sophistiqué : contrairement à l'algorithme EZW qui n'utilise qu'un seul ensemble décrivant la signifiance des coefficients, SPIHT met en jeu une liste des ensembles insignifiants (LEN), une liste des coefficients insignifiants (LCN) et une liste des coefficients significatifs (LCS). Tout comme EZW, SPIHT utilise une passe de description des coefficients significatifs et une passe de raffinement. Enfin, du fait de sa meilleure modélisation de la signifiance des coefficients, l'algorithme SPIHT offre une meilleure efficacité de codage que EZW.

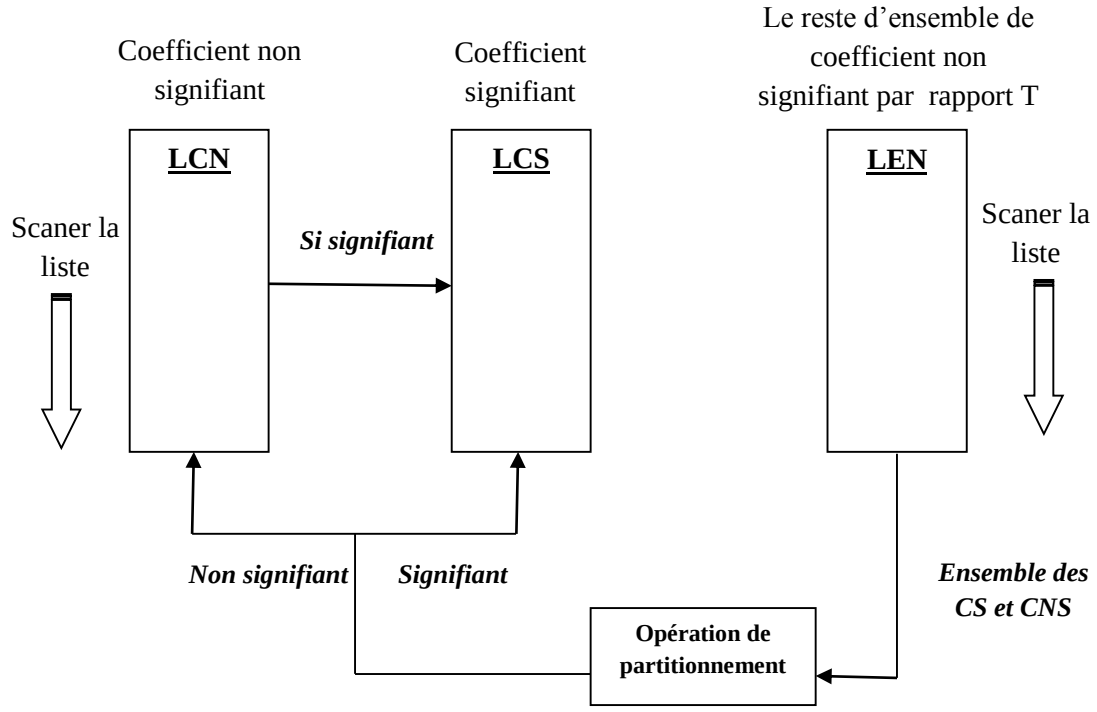


Fig. V.11: *Organigramme de l'algorithme de SPIHT*

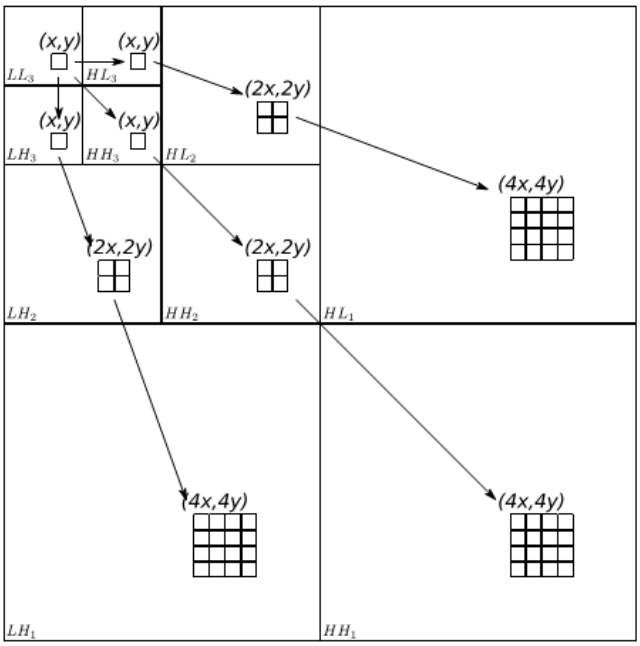


Fig. V.12: *Relation parent enfants de l'algorithme SPIHT pour la décomposition par ondelettes*

4. Paramètres d'évaluation de la qualité de compression

Les techniques irréversibles de compression modifient l'image en y introduisant une distorsion. Il faut donc évaluer le niveau de cette distorsion, qui permettra de contrôler la qualité des images reconstruites, d'évaluer et comparer les différentes approches. Dans la pratique, plusieurs techniques subjectives et objectives sont utilisées **.**

4.1.Techniques subjectives

La mesure subjective est basée sur l'évaluation de la qualité par des observateurs humains. Ces méthodes consistent à faire attribuer une note de qualité (Mean Opinion Score ou MOS) par un ensemble d'observateurs. Cette notation, lourde à mettre en oeuvre, est adaptée lorsque les images sont exploitées par des observateurs humains.

Le critère MOS est obtenu en calculant la moyenne des résultats d'une série de tests standards où les observateurs donnent leur avis sous la forme de points pour évaluer la qualité de l'image**.**

Les tests standards exigent que les observateurs examinent les images dans les mêmes conditions, telles que la taille de l'image, la durée d'exposition et l'environnement lumineux dans lequel se déroule l'expérience. Une échelle de note entre 5 et 1 (MOS) a été définies (Table II.1)

Table II.1– Echelle de notation pour le MOS

5	Qualité excellente
4	bonne
3	acceptable
2	Mauvaise qualité
1	inacceptable

Le MOS est défini comme suit:

$$MOS = \frac{1}{S}\sum_{i=1}^{5} i\ p(i) \qquad \text{V.5}$$

où *i* est l'image score, *p(i)* est la probabilité d'image score et *S* est le nombre d'observateurs.

4.2.Techniques objectives :

Les mesures objectives sont basées sur des critères mathématiques pour évaluer la qualité des images. Les critères de qualité utilisés pour mesurer les performances des instruments optiques sont, par exemple, le rapport signal/bruit (SNR), l'erreur quadratique moyenne (MSE).

Ils donnent une mesure de performance de la méthode de compression utilisée. Les principaux critères d´évaluation de toute méthode de compression sont :

a- Le taux de compression

Le taux de compression donne une mesure de performance des méthodes de compression des images fixes

$$T_C = \frac{Nombre\ de\ bites\ \ dans\ l'image\ originale}{Nombre\ de\ bites\ \ dans\ l'image\ comprimée} \qquad \text{V.6}$$

b- Entropie (Taux d'information)

L'entropie est une grandeur qui caractérise la quantité d'information que contient une image et représente aussi une quantité qui définit le taux de compression maximal sans perte d'information. (Voir la section 1.2.1.1)

c- Mesures de fidélité (distorsion)

Il s'agit de définir des quantités permettant d'évaluer numériquement la qualité de l'image reconstruite. Après l'opération de compression en introduite une erreur qui appelée la distorsion, due fait qu'éventuellement l'image reconstruite n'est pas exactement identique à

l'image originale. La mesure de fidélité utilisée généralement en compression d'image est l'erreur quadratique moyenne MSE. Cette grandeur (erreur) est définie par la moyenne des carrés entre le pixel (i, j) de l'image originale $I(i, j)$, et le pixel (i, j) de l'image reconstruite $\hat{I}(i, j)$.

$$MSE = \frac{1}{M.N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left[I(i, j) - \hat{I}(i, j) \right]^2 \qquad \text{V.7}$$

Le rapport signal sur bruit crête **[24]** :

$$PSNR = 10.\log_{10} \frac{\left(2^R - 1\right)^2}{MSE} \left[dB\right] \qquad \text{V.8}$$

Généralement une image est codée sur 8 bits est représentée par 256 niveaux de gris qui varient entre 0 et 255, l'étendu ou la dynamique de l'image est alors $2^8 - 1 = 255$

d- L'indice de similarité structurelle (SSIM)

Pour les applications d'imagerie médicale, où les images sont dégradée doit éventuellement être examinés par des experts, les paramètres d'évaluation traditionnelle reste insuffisante. Pour cette raison, les approches objectives sont nécessaires pour évaluer l'imagerie médicale qualité.

Nous évaluons ensuite un nouveau paradigme pour estimer la qualité des images médicales, en particulier ceux compressés par la transformée en ondelettes, basée sur l'hypothèse que le système visuel humain (HVS) est particulièrement adapté pour extraire des informations structurales.

L'indice de similarité compare la luminosité, le contraste et la structure entre chaque paire de vecteurs, où l'indice de similarité structurelle (SSIM) entre deux signaux x et y est donnée par l'expression suivante:

$$SSIM(x, y) = l(x, y)c(x, y)s(x, y) \qquad \text{V.9}$$

Cependant, la comparaison de la luminosité est déterminée par l'expression suivante:

$$l(x, y) = \frac{2\mu_x \mu_y + C_1}{\mu_x + \mu_y + C_1} \qquad \text{V.10}$$

Où l'intensité moyenne du signal de x est donnée par: $\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i$, $C_1 = (K_1 L)^2$, La constant $K_1 << 1$, et L est la rangée dynamique des valeurs de pixels (255 pour une l'image en échelle de gris codé sur 8 bits). La fonction de comparaison de contraste prend la forme suivante :

$$c(x,y) = \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2 + C_2} \qquad \text{V.11}$$

Où $\sigma_x = \sqrt{\mu_x(x^2) - \mu_x^2}$ est l'écart type du signal x initiale, $C_2 = (K_2 L)^2$, et la constant $K_2 << 1$.

La fonction de comparaison structure est définie comme suit:

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x \sigma_y + C_3} = \frac{\mathrm{cov}(x,y) + C_3}{\sigma_x \sigma_y + C_3} \qquad \text{V.12}$$

Où $\mathrm{cov}(x,y) = \mu_{xy} - \mu_x \mu_y$, et $C_3 = \frac{C_2}{2}$.

Alors, l'expression de l'indice de similarité structurelle devient:

$$SSIM(x,y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 \sigma_y^2 + C_2)} \qquad \text{V.13}$$

Enfin, la mesure de la qualité peut fournir une carte spatiale de la section locale qualité d'image, qui fournit plus d'information sur la qualité de l'image de dégradation, ce qui est utile dans les applications d'imagerie médicale. Pour l'application, nous avons besoin d'une seule mesure globale de l'ensemble qualité d'image qui est donnée par la formule suivante:

$$MSSIM(I, \hat{I}) = \frac{1}{M}\sum_{i=1}^{M} SSIM(I_i, \hat{I}_i) \qquad \text{V.14}$$

Où I et $\hat{I}$ sont respectivement les images de référence et dégradée, I_i et $\hat{I}_i$ est le contenu des images à la fenêtre i-ème local.
M est le nombre total de fenêtres locales dans l'image. Les valeurs MSSIM présentent une plus grande cohérence avec la qualité visuelle.

5. Conclusion :

En somme, nous avons vu qu'il existait de nombreuses manières de coder, de représenter, de compresser des images médicales. Aujourd'hui, avec la considérable avancée technologique, les algorithmes se permettent de réaliser de nombreux calculs pour compresser et décompresser une image. Nous avons introduit les différentes méthodes de codage entropique et de compression réversible ou irréversible des images médicales basées sur la transformation ondelette associés aux différents types d'encodage, tel que les algorithmes EZW, SPIHT.

SERIE TD N°5

Exercice 1 :

Soit deux images en niveaux de gris :

234	234	234	212	212	212
90	234	234	212	150	150
80	90	212	234	150	110
90	110	150	150	100	90
150	150	150	110	90	50
100	110	100	90	50	212

234	234	234	234	234	234
234	234	234	150	150	150
150	150	150	150	150	150
150	150	150	150	110	110
150	150	150	110	110	110
150	150	150	150	110	110

1) Appliquez la compression RLE sur ces deux images.
2) Calculez le taux de compression dans chacun des deux cas (chaque nombre est codé sur 1 octet).

Exercice 2 :

Soit l'image suivante :

2	1	3	6	7
1	2	4	4	1
3	5	1	3	7

1) Appliquez l'algorithme de compression de Huffman.

2) Calculez le nombre de bits moyen utilisés pour le codage

3) Calculez le taux de compression. On considère que chaque pixel est codé sur un octet et que l'on ne prend pas en compte les entêtes de fichiers.

Exercice 3 :

Après l'Application de la transformée en ondelettes de Haar sur l'image I (4*4) avec un niveau de décomposition de 2 nous obtenons la matrice R.

$$I=\begin{bmatrix}0 & 250 & 25 & 50\\ 50 & 50 & 50 & 25\\ 25 & 50 & 0 & 250\\ 75 & 200 & 200 & 0\end{bmatrix} \overset{T.O}{\Longrightarrow} R=\left[\begin{array}{cc|cc} \mathbf{80.95} & 26.95 & 6.25 & 35.93\\ -8.10 & -18.35 & 25 & -6.25\\ \hline -18.75 & 29.68 & 18.75 & -7.81\\ -31.25 & -12.5 & -46.87 & 12.5 \end{array}\right];$$

1. Nous quantifions ce résultat à l'aide d'une quantification uniforme, de pas de quantification 10, et de largeur 30. Trouvez la matrice de quantification obtenus R_Q ?
2. Coder le résultat obtenu à l'aide de Huffman ? (arbre de Huffman est obligatoire)
3. Calculer la taille de l'image compressée et le taux de compression ?

Solution Série TD N°5

Exercice 1 :

1. **Compression RLE**

a) image 1:

3	234	3	212	1	90	2	234	1	212	2	150	1	80	1	90	1	212

1	234	1	150	1	110	1	90	1	110	2	150	1	100	1	90	3	150

1	110	1	90	1	50	3	100	1	90	1	50	1	212	50 octets

b) image 2:

9	234	13	150	2	110	3	150	3	110	4	150	2	110	: 14 octets

2. **Taux de compression T:**

Taille de l'image = 36 octets, T1=36/50 =0.72% et T2=36/14 = 2.57%

Exercice 2 :

1) Algorithme de compression de Huffman

NG	#	Prob.	Passe 1	Passe 2	Passe 3	Passe 4	Passe 5
1	4	0.266	0.266	0.266	0.266	0.466	0.533
3	3	0.200	0.200	0.266	0.266	**0.266**	0.466
2	2	0.133	0.133	0.200	0.266	0.266	
4	2	0.133	0.133	**0.133**	**0.200**		
7	2	0.133	**0.133**	**0.133**			
5	1	**0.666**	0.133				
6	1	**0.666**					

NG	#	Prob.	code
1	4	0.266	**0**
3	3	0.200	**1**
2	2	0.133	**00**
4	2	0.133	**01**
7	2	0.133	**10**
5	1	0.666	**110**
6	1	0.666	**111**

2) nombre de bits moyen utilisés pour le codage:

4*1 + 3*1 + 2*2 + 2*2 + 2*2 + 1*3 + 1*3= 25 bits

3) Taux de compression:

Nombre de bits avant compression= taille image x 8 bits

= 15 * 8 = 120 bits

Taux de compression = 120/25 = 4,8%

Exercice 3 :

Après l'Application de la transformée en ondelettes de Haar sur l'image I (4*4) avec un niveau de décomposition de 2 nous obtenons la matrice R.

$$I=\begin{bmatrix}0 & 250 & 25 & 50\\ 50 & 50 & 50 & 25\\ 25 & 50 & 0 & 250\\ 75 & 200 & 200 & 0\end{bmatrix} \overset{T.O}{\Rightarrow} R=\left[\begin{array}{cc|cc} \mathbf{80.95} & 26.95 & 6.25 & 35.93\\ -8.10 & -18.35 & 25 & -6.25\\ \hline -18.75 & 29.68 & 18.75 & -7.81\\ -31.25 & -12.5 & -46.87 & 12.5\end{array}\right];$$

1. Nous quantifions ce résultat à l'aide d'une quantification uniforme, de pas de quantification 10, et de largeur 30. Trouvez la matrice de quantification obtenus R_Q ?

3. $$R_Q=\begin{bmatrix}\mathbf{80.95} & 0 & 0 & 30\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ -30 & 0 & -40 & 0\end{bmatrix}$$

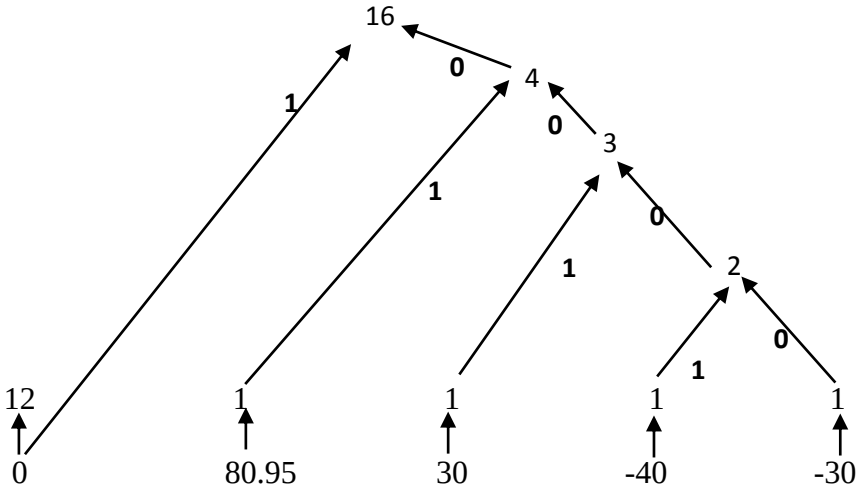
1. Coder le résultat obtenu à l'aide de Huffman ? (arbre de Huffman est obligatoire)

Tableau 1

Symbole	NUM occur
0	12
-30	1
-40	1
30	1
80.95	1

Tableau 2 (Après la construction de l'arbre Huf)

Symbole	Code Binaire
0	1
-30	0000
-40	0001
30	001
80.95	01



Arbre de Huffman

Le message binaire compressé : 01-1-1-001-1-1-1-1-1-1-1-1-0000-1-0001-1

3. Calculer la taille de l'image compressée et le taux de compression ?

La taille de l'image non compressé : Ti=L*H*Poid-------Ti=4*4*1=16 Octet .

La taille de l'image Compressé :

$$T_i^{comp} = \sum_{symbole} nombre\ de\ symbole \times T\ symbole$$

$$T_i^{comp} = (12 * 1) + (1 * 4) + (1 * 4) + (1 * 3) + (1 * 2) = 25\ bits$$

Taux de compression :$\tau = \frac{T_i^{comp}}{Ti} = \frac{25}{16*8} = 19.53\%$

CHAPITRE VI: SECURISATION DES DONNEES MEDICALES

Partie 1 Généralités sur la cryptographie

La cryptologie est un ensemble de techniques permettant d'assurer la sécurité des systèmes d'information. Cette discipline permet notamment de conserver aux données leur caractère de confidentialité, de contrôler leur accès ou d'authentifier des documents.

L'utilisation de la cryptographie est de plus en plus répandue et les utilisateurs des systèmes cryptographiques doivent être en mesure non seulement de comprendre leur fonctionnement mais aussi d'en estimer la sécurité.

I. Introduction

L'utilisation des réseaux informatiques PACS pour la transmission d'informations médicales pose le problème de la sécurisation. Pour pallier à ce problème, des techniques de chiffrement de messages plus ou moins robustes ont été développées. Ces algorithmes utilisent des clefs de chiffrement et de déchiffrement soit identiques, soit différentes. Parmi les plus courantes, nous pouvons citer le chiffrement de Vigenère à une seule clef, l'algorithme DES à clefs secrètes et l'algorithme RSA à clefs publiques et privées .

La cryptographie peut être utilise pour atteindre la flexibilité, la conformité et l'intimité des données qui est une exigence dans les systèmes d'aujourd'hui.
Le but de ce chapitre est de donner une introduction à la cryptographie moderne utilisée dans la transmission et le stockage sécurisé de données. Après un rapide historique de la cryptographie on examinera un algorithme cryptographique appliqué aux images médicales.

II. Terminologies

- **Texte en clair :** est le message à protéger;l'information à transmettre
- **Texte chiffré :** est le résultat du chiffrement du texte en clair.
- **Chiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte enclair en texte chiffré en envisageant la protection d'information contre toute prise de connaissance
- (confidentialité) ou de modification (intégrité) du contenu..(afin de la rendre illisible sans avoir appliqué l'algorithme inverse)
- **Déchiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.Retour au texte en clair.

  Clé : est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui
- n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

  Cryptographie : cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer
- et de déchiffrer un texte en clair afin de le rendre incompréhensible pour qui conque n'est pas en possession de la clé à utiliser pour le déchiffrer.
- **Cryptanalyse :** c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.

  Cryptologie : il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires, la cryptographie et la cryptanalyse.

- **Décrypter :** c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans posséder la clé qui a servi au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.
- **Crypter :** en relisant la définition du mot décrypter, on peut se rendre compte que le mot crypter n'a pas de sens et que son usage devrait être oublié. Le mot cryptage n'a pas plus de sens non plus.
- **Coder, décoder :** c'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. Le Morse est donc un code puisqu'il transforme des lettres en trait et points sans notion de secret. L'ASCII est lui aussi un code puisqu'il permet de transformer une lettre en valeur binaire.

III. Objectifs de la cryptographie

Il existe quatre grands objectifs pour le cryptage des données numériques :

III.1 Confidentialité : la confidentialité ou masquage des données, le contenu des données va être sauvé de toutes les personnes, machines et systèmes à l'exception de ceux qui ont le droit d'accès.

III.2 Authentification : permet à l'émetteur de signer son message, ainsi, le récepteur n'aura pas de doute sur l'identité du premier.

III.3 Intégrité : les données vont être protégées du changement (suppression, ajout, mise à jour) de la personne non autorisé.

III.4 Non-répudiation : est la garantie qu'aucun des deux individus ayant effectué une transaction ne pourra nier avoir reçu ou envoyé les messages.

IV. Les déférents algorithmes de cryptage et décryptage :

On distingue les méthodes de cryptage classiques et les méthodes de cryptage modernes

IV.1 Méthodes de cryptage Classiques :

IV.1.1 Cryptage par substitution : Les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion.

On distingue deux méthodes de substitution, la substitution mono-alphabétique et la substitution poly-alphabétique.

- **Substitution mono-alphabétique :** consiste à remplacer chaque alphabet clair par un autre alphabet codé.

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

Tableau I-1 substitution mono-alphabétique

- **Exemple :**

Texte claire« la cryptographie »

Texte Crypté« iweqbgndtqwgkcy »

- **Substitution poly-alphabétique :**le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prisedans plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutionsmono-alphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texteen clair. On choisit une clé qui sert d'entrée dans la grille poly alphabétique incluant autant desymboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettreparticulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondantdu texte en clair en utilisant la grille poly alphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de

départ). L'exemple leplus célèbre est l'algorithme de VIGENERE et de BEAUFORT. L'illustration la plus simple quicorresponde à ce principe est l'utilisation d'une fonction à base de ou exclusif (XOR).

IV.1.2 Cryptage par transposition : Les transpositions consistent à mélanger les symboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces règles sont déterminées par la clé de chiffrement. Une suite de transpositions forme une permutation.

IV.1.3 Cryptage par produit : C'est la combinaison de chiffrement par substitution etchiffrement par transposition. La plupart des algorithmes à clés symétriques utilisent le chiffrement par produit. On dit qu'un « round » est complété lorsque les deux transformations ont été faites une fois (substitution et transposition). Ces successions des rondes portent également le nom de réseaux S-P de Shannon.

IV.2 Méthodes de cryptage Modernes :

On distingue deux méthodes majeures de cryptage modernes :

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

IV.2.1 Cryptage symétrique

Ce type de cryptage se base sur l'utilisation d'une clé pour crypter et décrypter les messages. La sécurité de cette solution repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message.

L'exemple historique de l'utilisation du cryptage symétrique est le fameux téléphone rouge qui reliait le Kremlin à la Maison Blanche. La clé privée était alors transmise dans une valise diplomatique. Pour une meilleure sécurité, elle était détruite et réinitialisée après chaque conversation.

Le cryptage symétrique fonctionne selon deux procédés différents :

- le cryptage par flot : le cryptage s'effectue en continu, bit par bit
- le cryptage par bloc : le cryptage s'effectue sur des blocs de bits

✓ **Avantages du cryptage symétrique :**

-La rapidité d'exécution (une seule clé utilisée)

-La simplicité d'implémentation (gestion d'une seule clé).

- Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, etc...)
- Clés relativement courtes.

✓ **Inconvénients du cryptage symétrique :**

- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.
- La sécurisation de la chaîne de transmission de la clé.
- Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique**.**

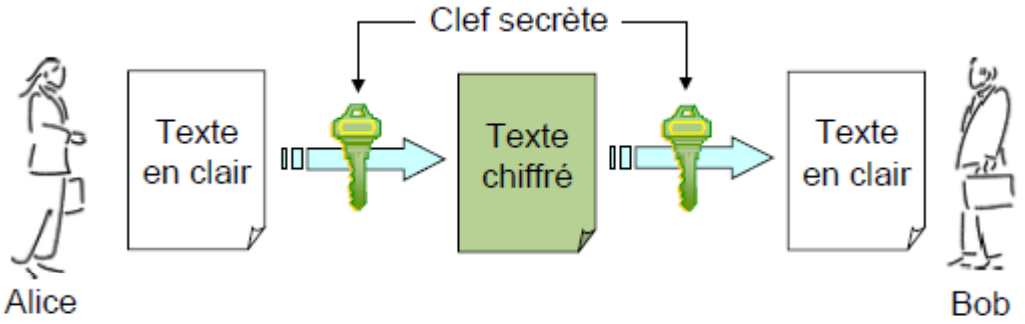


Figure I.1.Principe de cryptage symétrique

IV.2.2 Cryptage asymétrique

Ce cryptage, contrairement au symétrique, se base sur l'utilisation de deux clés, l'une publique(Pour crypter, elle est accessible publiquement) et l'autre privée (pour décrypter le message, elle estgardée secrète). Ce type de cryptage élimine la problématique de la transmission de la clé. Ce mode de cryptage est également nommé le cryptage à clé publique. Il est essentiel Que l'on ne puisse pas déduire la clé privée de la clé publique.

Pour bien comprendre le principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur etun destinataire**.**

- l'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique au destinataire.
- le destinataire utilise la clé publique pour crypter son message ; il envoie tout à l'émetteur initial
- l'émetteur utilise sa clé privée pour décrypter le message.

✓ **Avantages du cryptage asymétrique :**

- l'élimination de la problématique de la transmission de clé
- la possibilité d'utiliser la signature électronique
- l'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.

-Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé Symétrie.

✓ **Inconvénients du cryptage asymétrique :**

- Un temps d'exécution plus lent que le cryptage symétrique
- le danger des attaques par substitution des clés (d'où la nécessité de valider les émetteurs des clés)

-Taille des clés, plus grand que celle des systèmes symétriques.

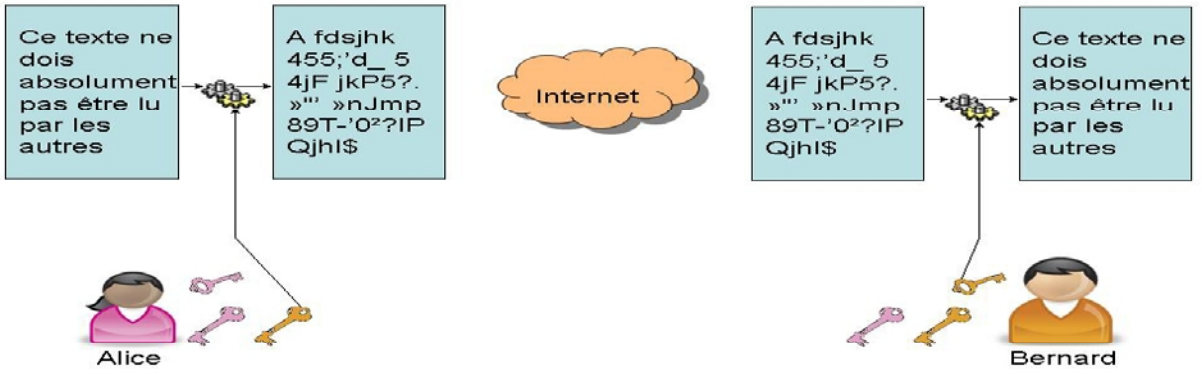


Figure I.2.Principe de cryptage Asymétrique

IV.2.3 Exemples d'algorithmes de cryptage symétriques et asymétriques

IV.2.3.1 Cryptage DES (Data Encryptions Standard) :

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16 Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7.2*1016) clés différentes **.**

IV.2.3.2 Cryptage AES (Advanced Encryption Standard)

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours**.**

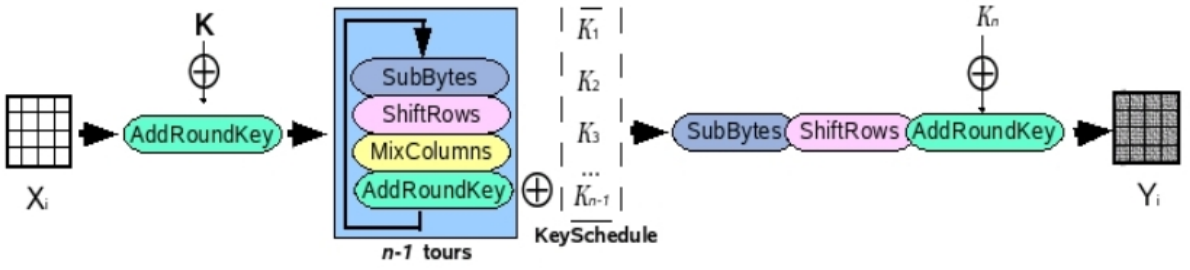


Figure I.3 Le schéma général d'AES.

IV.2.3.3 Méthode de cryptage RSA

La méthode RSA est asymétrique, cette méthode utilise une paire de clés (des nombres entiers) composé d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permet à n'importe lequel de ses correspondants de vérifier la signature.

Une condition indispensable est qu'il soit « calculatoire ment impossible » de déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique, c'est-à-dire que les moyens de calcul disponibles et les méthodes connues au moment de l'échange (et le temps que le secret doit être conservé) ne le permettent pas.

Le chiffrement RSA est souvent utilisé pour communiquer une clé de chiffrement symétrique, qui permet alors de poursuivre l'échange de façon confidentielle : Bob envoie à Alice une clé de chiffrement symétrique qui peut ensuite être utilisée par Alice et Bob pour échanger des données .

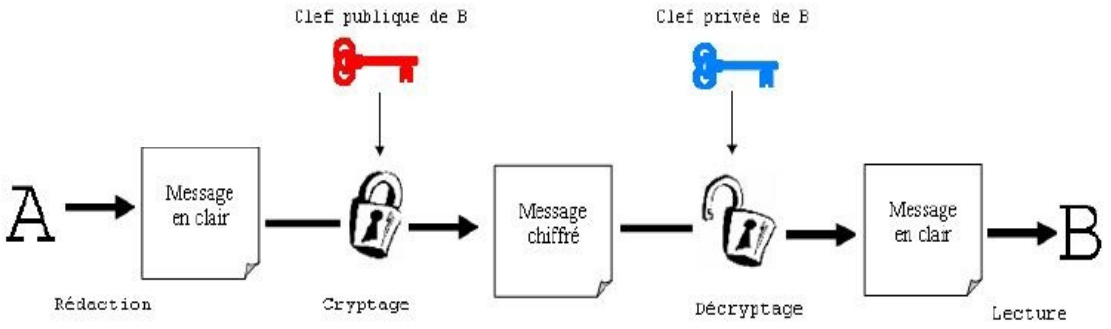


Figure I.4 Principe général de chiffrement RSA.

IV.2.3.4 Cryptage par flot

Les algorithmes de cryptage par flot peuvent être définis comme étant des algorithmes de chiffrement par bloc, où chaque bloc est de dimension unitaire (1 bit, 1 octet, etc.) ou relativement petit. Leurs principaux avantages sont leur extrême rapidité et leur capacité à changer à chaque symbole du texte clair. Avec un algorithme de chiffrement par flot, il est possible de crypter séparément chaque caractère du message clair un par un, en utilisant une fonction de cryptage qui varie à chaque fois (ces algorithmes ont donc besoin de mémoires). Généralement, les algorithmes de chiffrement par flot sont composés de deux étapes : la génération d'une clef dynamique et la fonction de cryptage de sortie dépendant de la clef dynamique.

Quand la clef dynamique est générée indépendamment du texte clair et du texte chiffré, l'algorithme de chiffrement par flot est dit synchrone. Avec un chiffrement par flot, l'émetteur et le récepteur doivent se synchroniser en utilisant la même clef et en l'utilisant à la même position. Les chiffrements par flot synchrone sont utilisés principalement dans des environnements où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs. Concernant les attaques actives comme l'insertion, la suppression et la copie de digits du texte chiffré par un adversaire actif, celles-ci produisent immédiatement une perte de synchronisation. Le processus de cryptage d'un chiffrement par flot synchrone est décrit (**Figure I.4)** où $f()$ est la fonction qui détermine l'état suivant, $g()$ est la fonction génératrice de la clef dynamique et $h()$ la fonction de sortie de cryptage :

$$\begin{cases} s_{i+1} = f(k, s_i) \\ z_i = g(k, s_i) \\ c_i = h(z_i, m_i) \end{cases} \quad \textbf{(1)}$$

où K est la clef, s_i, m_i, $c_i$et $z_i$sont respectivement le i^e état, le texte clair, le texte chiffré et la clef dynamique. Le processus de décryptage est illustré figure (**Figure I.5)**.

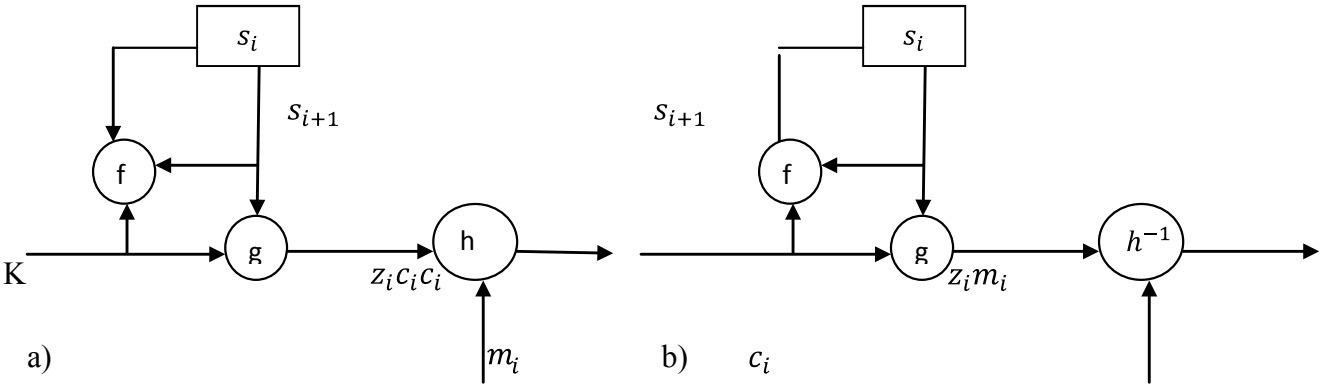


Figure I.5 Cryptage par flot synchrone. a) Cryptage. b) Décryptage.

Quand la clef dynamique est générée à partir de la clef et d'un certain nombre de digits précédemment cryptés, l'algorithme de chiffrement par flot est dit asynchrone, appelé aussi chiffrement par flot auto-synchronisant. La propagation des erreurs est limitée à la taille de la mémoire. Si des digits du texte chiffré sont effacés ou insérés en plus, le récepteur est capable avec la mémoire de se resynchroniser avec l'émetteur. Concernant les attaques actives, si un adversaire actif modifie une part des digits du texte chiffré, le récepteur est capable de la détecter. Le processus de cryptage d'un chiffrement par flot asynchrone est décrit (**Figure I.6)**, où $g()$ est la fonction génératrice de la clef dynamique et $h()$ la fonction de sortie de cryptage

$$\begin{cases} z_i = g(k, c_{i-t}, c_{i-t+1,\ldots\ldots,} c_{i-2}, c_{i-1}) \\ c_i = h(z_i, m_i) \end{cases} \quad \textbf{(2)}$$

où K est la clef, mi, ci et z_i sont respectivement le i^e texte clair, le texte chiffré et la clef dynamique. Nous pouvons remarquer équations (**2**) que la clef dynamique dépend des t digits précédents du texte chiffré. Afin d'être robuste à de nombreuses attaques statistiques, la fonction génératrice de la clef dynamique $g()$ doit produire une séquence d'une large période avec de bonnes propriétés statistiques qui peuvent être appelées séquences binaires pseudo aléatoires. Le processus de décryptage est illustré figure (**Figure I.5).**

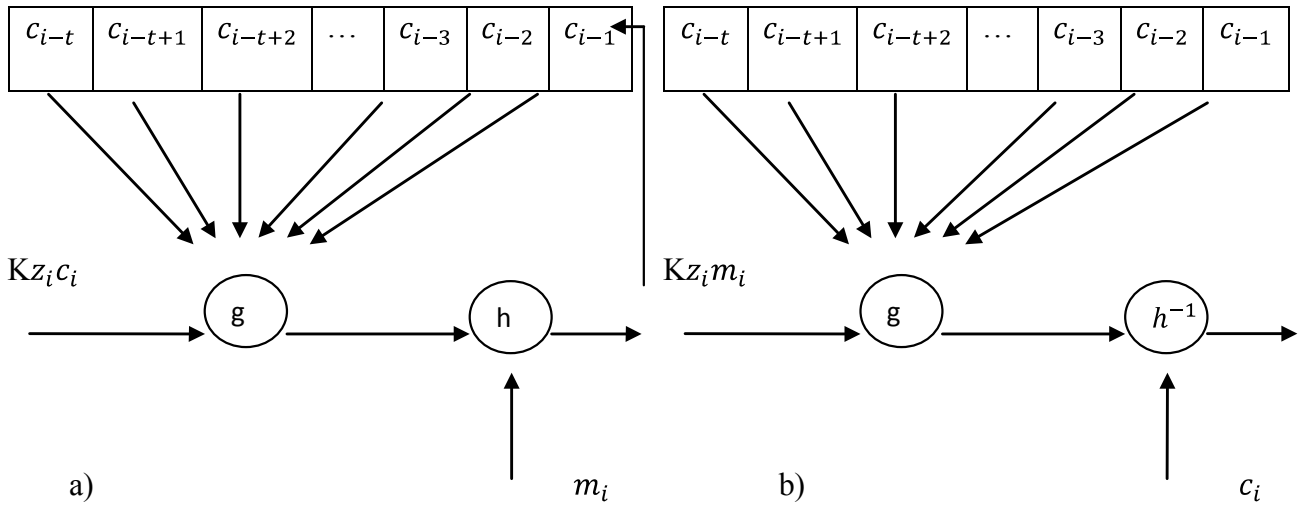


Figure I.6 Chiffrement par flot asynchrone a) Cryptage. b) Décryptage.

IV.2.3.5 Fonction de hachage

Cette fonction permet à partir d'un texte de longueur quelconque, de calculer une chaîne de taille inférieure et fixe appelée condensé ou empreinte (*message digest* ou *hash* en anglais). Ce dernier permet d'assurer l'i**ntégrité**des données, a**uthentification**de la source et la n**on-répudiation**de la source.

Une fonction de hachage doit être à sens unique, c'est à dire qu'il doit être impossible étant donné une empreinte de retrouver le message original, et sans collisions, ça veut dire l'impossibilité de trouver deux messages distincts ayant la même valeur decondensé. La moindre modification du message entraîne la modification de l'empreinte.

MD5 (Message Digest 5 - Rivest1991-RFC 1321) et SHA sont deux exemples de fonctions de hachage.

IV.2.3.6 Scellement (MAC) :

Est un mécanisme qui consiste à calculer (ou sceller) une empreinte à partir d'un message et d'une clé privée pour:

- Authentifier l'origine des données
- Vérifier l'intégrité des données

Le scellement d'une empreinte génère :

- un **sceau**ou**code d'authentification de message** *(MAC)*

Le scellement est calculé en appliquant une fonction de hachage à un message et une clé privée tel qu'illustré dans la figure suivante :

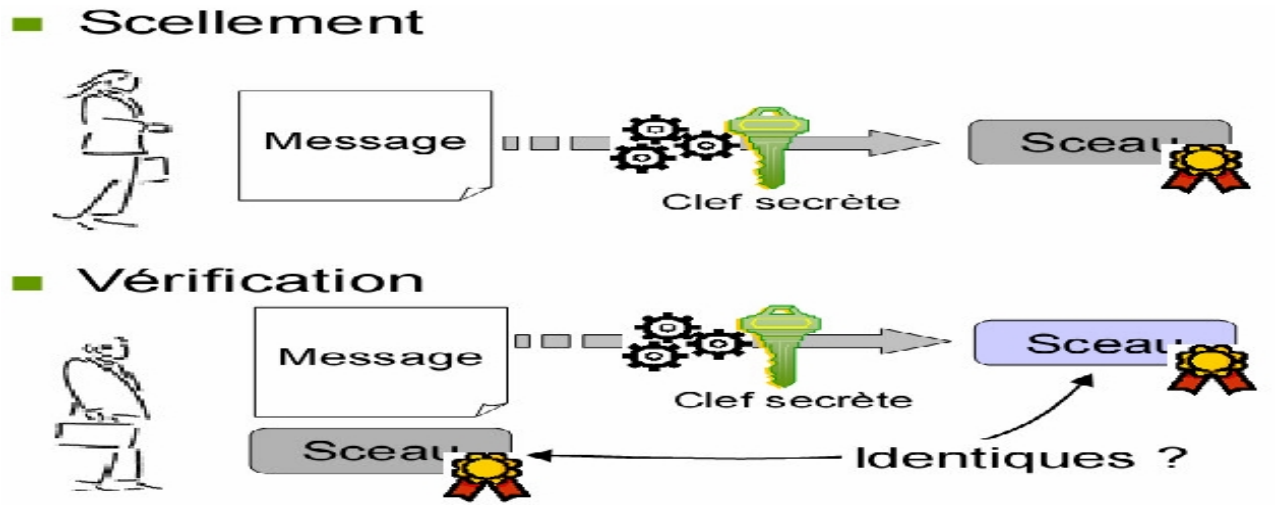


Figure I.7 Scellement

IV.2.3.7 Signature numérique

La signature numérique est définit comme des données ajoutées à un message ou une transformation cryptographique d'un message permettant à un destinataire :

- d'authentifier l'auteur d'un document électronique
- de garantir son intégrité
- de se protéger contre la contrefaçon (seul l'expéditeur doit être capable degénérer la signature) -> non-répudiation.

La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique.

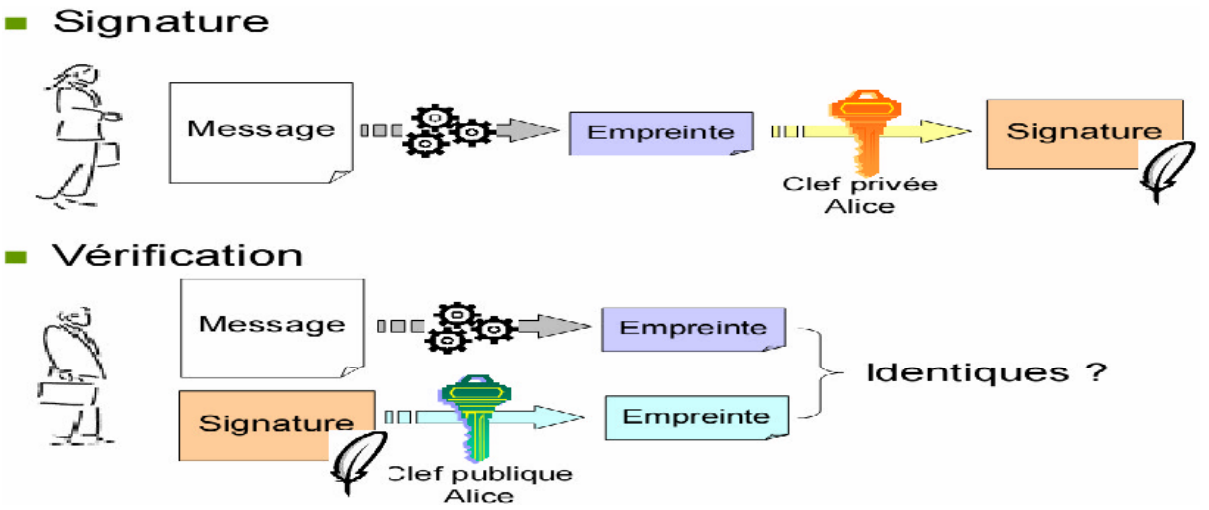


Figure I.8 Signature numérique

IV.2.3.8 Certificat électronique

Un certificat numérique est un bloc de données contenant, dans unformat spécifié, les parties suivantes :

- la clé publique d'une paire de clés asymétriques,
- des informations identifiant le porteur de cette paire de clés (qui peutêtre une personne ou un équipement), telles que son nom, son adresse IP, son adresse de messagerie électronique, son URL, son titre, son numéro de téléphone, etc...
- l'identité de l'entité ou de la personne qui a délivré ce certificat(autorité de certification), Ex. Verisign,
- La signature numérique des données générée par lapersonne ou l'entité prenant en charge la création ou l'authentificationde ce certificat et servant d'autorité de certification.

Usuellement, on distingue deux familles de certificats numériques :

- les certificats de signature, utilisés pour signer des e-mails ou s'authentifier sur un site web.
- les certificats de chiffrement : les gens qui vous envoient des e-mailsutilisent la partie publique de votre certificat pour chiffrer le contenuque vous serez seul à pouvoir déchiffrer.

Il existe deux façons distinctes de créer des certificats électroniques :

- le mode décentralisé (le plus courant) qui consiste à faire créer, parl'utilisateur (ou, plus exactement par son logiciel ou carte à puce) la biclef cryptographique et de remettre la partie publique à l'AC qui va yadjoindre les informations de l'utilisateur et signer l'ensemble(information + clé publique)

- le mode centralisé qui consiste en la création de la biclef par l'AC, quigénère le certificat et le remet avec la clé privée à son utilisateur.

Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse. On trouve parmi les plus connus et les plus utilisés :

- la norme X.509 en version 1, 2, et 3, sur lequel se fondentcertaines infrastructures à clés publiques.
- OpenPGP, format standard (normalisé dans le RFC 2440) delogiciels comme GnuPG.

5. Conclusion

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie qui est un domaine important pour la sécurisation d'information. En premier lieu, nous avons commencé par donner quelques terminologies. Puis nous avons cité les différents algorithmes de cryptage classiques et modernes. Nous avons observé que les clefs ont un rôle important pour chaque cryptosystème. Ce chapitre a introduit aussi les principaux algorithmes de cryptage symétrique, asymétrique, par flot et par bloc.

Nous terminons ce chapitre par une exposition d'un algorithme de cryptage asynchrone par flot, qui montre plusieurs avantages par rapport aux autres algorithmes.

Enfin, nous avons abordé la notion de signature numérique et certificat électronique.

Dans le partie 2 de ce chapitre, nous allons présenter les définitions et les propriétés générales des processus de tatouage des images numériques. Puis, nous présenterons le tatouage fragile pour le Contrôle d'intégrité, Enfin, nous terminerons cette partie où nous exposerons le tatouage robuste pour la protection des données médicales.

Chapitre 6: Partie 2

Tatouage des Images Médicales

1.Introduction

De nos jours, de plus en plus d'images numériques sont transférées sur les réseaux informatiques. Les études présentées dans ce chapitre montrent comment des algorithmes de tatouage permettent la sécurisation des images médicales. Pour ce faire, les images peuvent être tatouées au niveau des codages source afin de faire remonter cette fonctionnalité au niveau des couches hautes (applications). De cette manière, les fonctionnalités tatouage d'images sont insérées au niveau d'un logiciel. La protection est alors assurée pendant la transmission des images médicales mais aussi pour l'archivage de ces données numérique. Dans la section 3 nous mettrons en évidence les définitions et les propriétés générales des processus de tatouage des images numériques. Puis, dans la section 5 nous présenterons les différents techniques de tatouage . Enfin, nous terminerons nous exposerons le tatouage robuste pour la . . .protection des données médicales

2. Historique

Le tatouage numérique d'image est un concept récent. Les premières publications portant sur le tatouage d'images numériques fussent celles de Tanaka et al sur une méthode pour cacher de l'information dans une image en 1990.
En 1993 Le terme digital watermark (tatouage numérique) fut employé pour la première fois par Andrew Tirkel et Charles Osborne .

Depuis 1995, le tatouage numérique a occupé une place importante dans la recherche scientifique, plusieurs travaux ont été développés et implémentés dans ce domaine. Cox a implémenté des techniques d'étalement de spectre pour le tatouage numérique. L'invention des systèmes de re-synchronisation en 1998 marqua la discipline de même que le tatouage avec information adjacente .

Bender et al. en 1995 travaillent sur une méthode statistique appelée *Patchwork* qui consiste à sélectionner, selon une clé secrète, une séquence de n paires de pixels (a_i, b_i). Ensuite on augmente chaque a_i de 1 et on diminue chaque b_i de 1, la somme des différences donne 2n. Delaigle et al. en 1998 ont réalisé une technique sur la base du modèle perceptif humain.

3. Définitions

Le tatouage ou watermarking est une technique parmi d'autres techniques permettant de cacher ou dissimuler une information de copyright ou une marque (watermak) dans un document hôte (audio, vidéo) ou dans une image numérique d'une manière invisible, imperceptible ou inaudible. Comme définitions, nous pouvons retenir:

Miller et Cox 1997 *:*

Le tatouage numérique signifie l'intégration d'un signal invisible ou imperceptible dans un contenu ou des données comme une vidéo, une audio ou une image, le tatouage est essentiellement motivé par un besoin de fournir une protection du droit d'auteur, du contenu numérique (audio, vidéo et image) de l'identification du

propriétaire, de l'empreinte digitale et pour déterminer si les données ont été modifiées par rapport à l'originale .

Christian REY et Jean-Luc DUGELAY 2001:

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (i. e, invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc.).

Chun-Shien Lu 2004:

Le tatouage numérique est un signal intégré de façon permanente dans des données numériques qui peut être détecté ou extrait plus tard par l'exécution d'un algorithme informatique afin de faire des affirmations sur les données. Le tatouage est caché dans le document hôte de telle manière qu'il est inséparable des données et qu'il est résistant à de nombreuses opérations, sans dégrader la qualité du document hôte.

4. Schéma générale de l'implémentation de tatouage :

Le tatouage comporte deux phases fondamentales:

- **Phase d'insertion.**
- **Phase d'extraction**.

4.1. phase d'insertion de la signature ou de la marque

La figure 6.1 présente le schéma général de l'insertion de la marque W à l'aide d'une clé K . L'image originale I est tatouée de la marque W par la propriétaire de la clé K . L'image marquée I_w est visuellement équivalente à I .

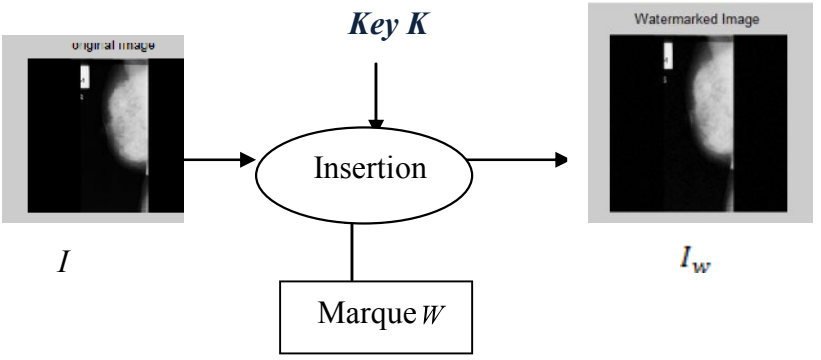


Figure 6.1- Schéma général de l'insertion d'une marque

4.2. Phase d'extraction /détection de la signature ou de la marque

La figure 6.2 présente le schéma général d'extraction ou de détection de la marque. On peut classifier le schéma de détection selon la nécessite de l'utilisation de l'image originale I et la clé K en trois classes :

- **Non aveugle**: si l'utilisation de l'image originale et la clé sont nécessaires.

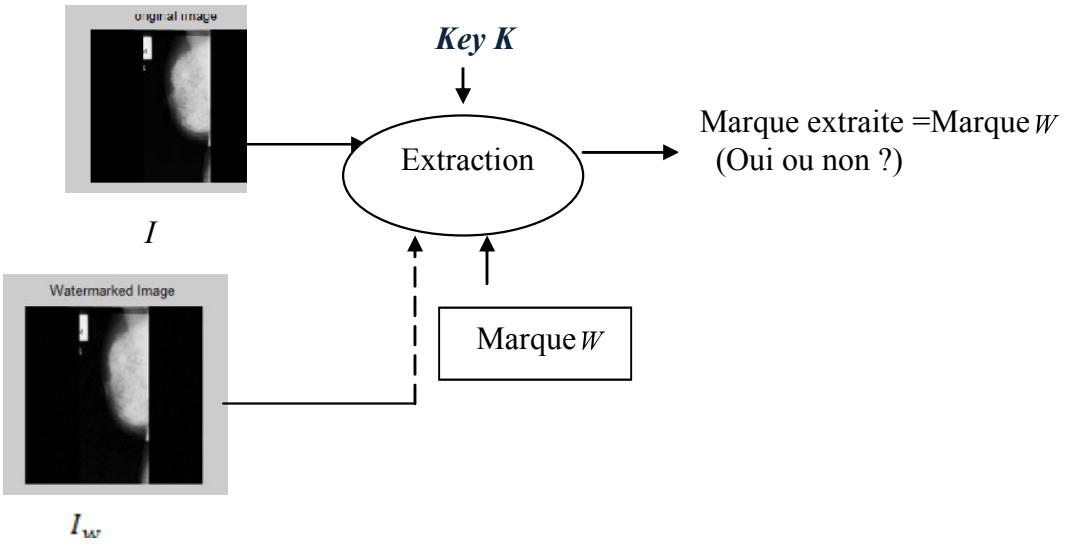


Figure 6.2 - Schéma général d'extraction non aveugle d'une marque.

- **Semi aveugle** : schéma d'extraction n'a pas besoin forcement de l'utilisation l'image originale mais seulement de quelques caractéristiques de celle-ci.

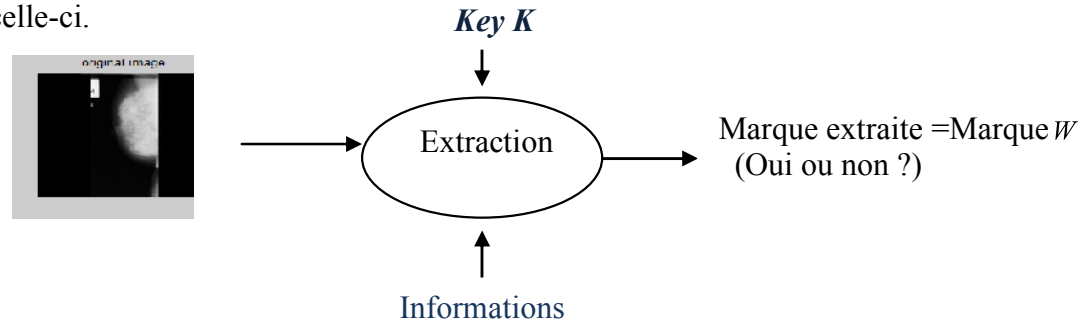


Figure 6.3 - Schéma général d'extraction semi aveugle d'une marque.

- **Aveugle:** le schéma d'extraction n'utilise pas l'image originale et la marque (la connaissance n'est pas obligatoire).

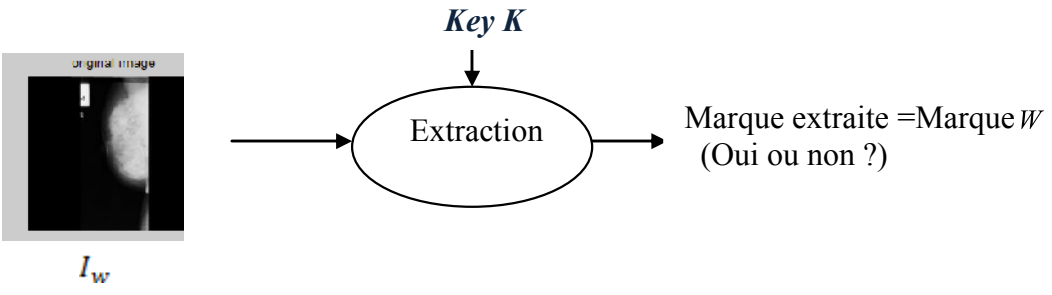


Figure6.4 - Schéma général d'extraction aveugle d'une marque.

5. Les techniques du tatouage

a) Cryptographie

La cryptographie est parmi les premières propositions pour assurer la sécurité de la transmission et le transfert de documents à travers le Net.
La cryptographie permet de rendre un message illisible pour garantir une parfaite sécurité (authentification, intégrité et confidentialité,...). Elle consiste à transformer un texte clair en cryptogramme: $C = E_{K_C}\ (M)$, à l'aide d'une clé K_c.Pour le décodage ou déchiffrement du cryptogramme en texte en clair on applique la transformation inverse avec une clé K_D : $M = D_{K_D}\ [E_{K_C}\ (M)]$.

E: Fonction de chiffrement.
D: Fonction de déchiffrement.

Des techniques de chiffrement de messages utilisent des clefs de chiffrement et de déchiffrement identiques (symétrique), ou différentes clé secrète ou privé et clé publique (asymétrique). Parmi les techniques les plus utilisés actuellement, nous pouvons citer l'algorithme symétrique DES et l'algorithme asymétrique RSA.

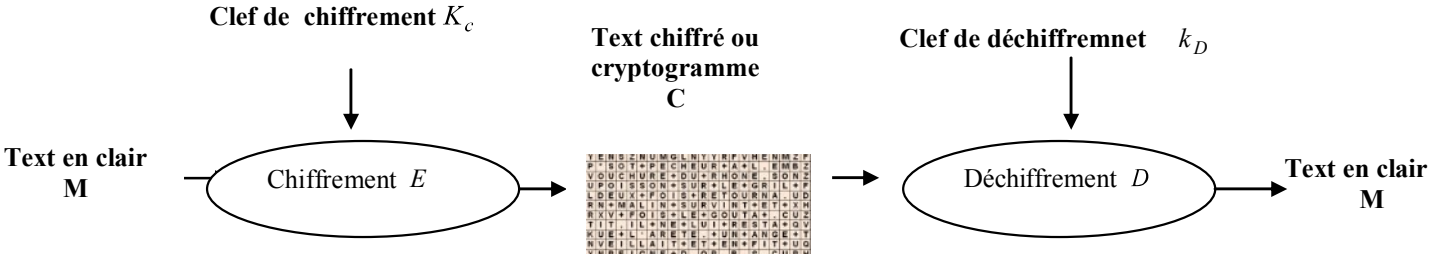


Figure 6.5 - Schéma générique de cryptologie

b) Stéganographie

La stéganographie comme le tatouage est une technique d'insertion permettant de cacher des données. Les objectifs sont différents :

Le tatouage permet de cacher une information de sorte que le message résiste à des attaques de la part des pirates on dit alors que le canal est fiable ou que la communication est fiable. La stéganoraphie permet de cacher des données secrètes dans un canal ou medium tel que l'attaque ne puisse savoir si l'information est cachée dans le canal (on parle de canal secret ou de communication secrète). On peut aussi faire appel aux méthodes de stéganographie à clef secrète ou à clef publique sur un modèle proche de ce qui se fait en cryptologie.

5.2.1. Stéganographie à clé secrète

Il est alors essentiel de protéger les clefs secrètes utilisées, à déterminer les endroits où cacher et où retrouver les informations.

5.2.2. Stéganographie à clé publique

Simplement à retrouver l'information cachée, l'utilisateur possède une clé privée (appelée encore clé secrète) et une clé publique. Il distribue sa clé publique et garde secrète sa clé privée. Il existe aujourd'hui un certain nombre d'implémentations pratiques, sous forme de programmes informatiques, de techniques stéganographiques pour établir une communication secrète.

6. Les propriétés d'un système de tatouage performant

6.1. Invisibilité ou imperceptibilité

Ce critère repose sur l'idée que l'insertion de tatouage n'influence pas sur la qualité visuelle de l'image pour deux raisons: pour ne perdre pas la qualité de l'image et aussi pour qu'il ne pourrait pas être détruit facilement par les pirates. Cox et al définissent l'invisibilité comme une similitude visuelle entre l'image originale et l'image tatouée.

6.2. Robustesse et fragilité

C'est une autre propriété plus difficile à vérifier qui permet de trouver la marque ou l'information insérée dans l'image tatouée malgré que cette dernière a enduré des attaques (supprimer ou modifier) de la part de l'attaquant. Aussi Cox et al définissent la robustesse comme capacité de détecter le watemark après des opérations de modifications(traitements), par exemple, plus la qualité d'information dans l'image augmente, plus la signature sera visible ou perceptible et donc la robustesse diminue.

6.3. Réversibilité ou irréversibilité

Les techniques de tatouage peuvent être classées en deux catégories, réversible et irréversible. Le tatouage réversible permet de retrouver ou de restaurer l'image original à partir de l'image tatouée en appliquant une transformation inverse sans produire des changements et permet d'éviter une distorsion irréversibles dans l'image originale en appliquant des techniques capable d'extraire l'image originale, Par contre le tatouage non réversible, il n'existe aucun moyen de retrouver l'image originale à partir de l'image tatouée .

6.4. Sécurité:

Le secret de la clé est capital. Un utilisateur ne connaissant pas la clé ne peut pas retrouver, modifier ou supprimer la marque insérée.

7. Les schémas de tatouage existants

7.1.Les schémas de tatouage selon le domaine d'application:

a.Protection de copyright

Les images médicales doivent être protégées avant leur diffusion, la protection est assurée par l'insertion d'une marque ou du copyright de propriétaire ou d'un organisme. Cette marque est insérée et extraite à l'aide d'une clé secrète de chiffrement /déchiffrement de la signature.

b. Suivi des transactions

Permet d'insérer une marque dans l'image, cette marque contient des informations relatives au propriétaire (patient ou médecins), à sa destination et de la façon de son utilisation .

c. Intégrité et Authentification des documents

Consiste de vérifier que l'image n'a pas été modifiée ou détectée par rapport à l'image originale en cours de route et en adéquation avec l'identité du patient ou du médecin.

d. Indexation

Le tatouage permet d'insérer une signature dans l'image pour rendre l'indexation plus simple. La signature générée par un créateur est une collection d'informations avec un sommaire ou un descripteur ou lien vers une autre information pour faciliter le classement et la recherche rapide dans une base de données.

7.2. Les schémas de tatouage selon le domaine d'insertion:

a) Domaine spatial

Les méthodes spatiales sont plus simples et plus coûteuses en temps d'exécution. Elles sont peu robustes aux attaques géométriques . Elles permettent d'insérer une marque directement dans l'image ou permettent de faire des modifications directes des composants de l'image.

b) Domaines transformés ou fréquentiel

Sont des méthodes utilisant des algorithmes basés sur l'insertion de la signature non pas directement dans l'image mais dans les coefficients de transformés de celle-ci, ce domaine est réalisé après une décomposition par transformé telle que DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform),SVD(Singular Value Decomposition). Les méthodes fréquentielles sont plus robustes à la compression et moins sensibles aux attaques géométriques. Figure 6.4 montre le schéma de tatouage selon l'espace de travail (domaine d'insertion de la signature), le type d'algorithme utilisé et le champ d'application.

c) Domaine basé sur la combinaison de domaines spatial et fréquentiel

Sont des techniques de tatouage permettant de fournir plus de marques et de réduire au minimum la distorsion de l'image tatouée. Elles se basent basé sur des algorithmes d'insertion de la marque dans la combinatoire de deux domaines spatial et fréquentiel.

Le principe consiste à partitionner la marque de l'image hôte en deux parties, respectivement, pour l'insertion spatiale et l'insertion fréquentielle qui sont réalisées en fonction de la préférence de l'utilisateur et de l'importance des données.

7.3. Les schémas de tatouage selon la façon de l'insertion:

On distingue les techniques de tatouage selon la façon de l'insertion de la signature dans un document. Soit de façon additive connue par les techniques additives, ou de façon substitutive connue par les techniques substitutives.

a) Schéma additif

Il permet d'insérer un bruit à l'image hôte. La marque générée est directement insérée dans l'image originale.

b) Schéma substitutif

La marque n'est pas ajoutée mais substituée à des composants de l'image (pixel, coefficient de transformés,....) sélectionnés à l'aide une clé secrète. La signature est insérée selon des contraintes appliquées sur les composants de l'image. Dans la phase d'extraction, on calcule le degré d'équivalence entre la marque retrouvée à partir des composants de l'image tatouée et la marque originale.

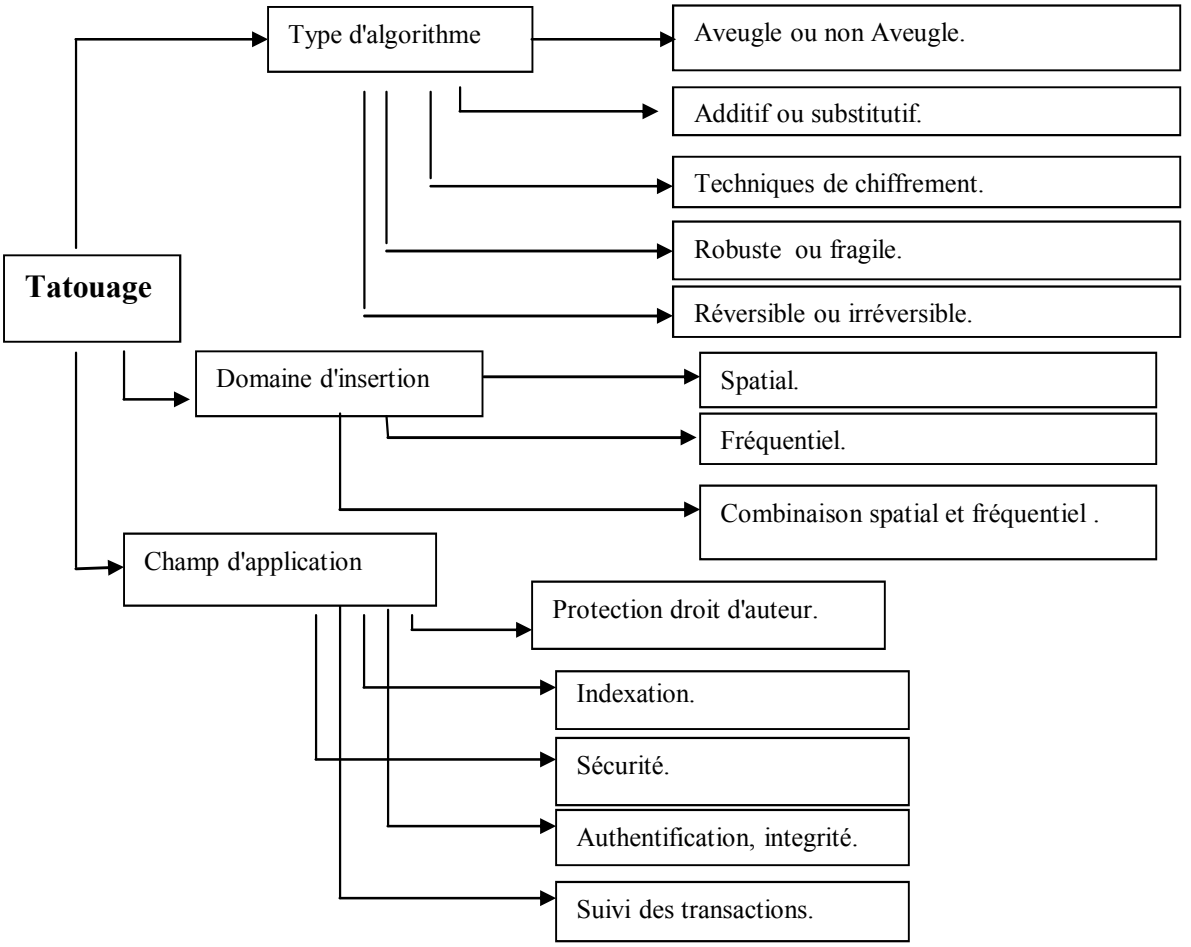


Figure 6.6: Schéma de classification de tatouage numérique.

8. Mesures visuelles de la qualité des images

Pour vérifier le critère d'invisibilité, l'image marquée doit être de même qualité que l'originale c-à-dire que l'image tatouée et l'origine soient perceptuellement équivalentes. Les mesures visuelles de qualité d'image sont effectuées sur le calcul de proximité de l'image tatouée par rapport à l'image originale ou bien sur la distorsion ou niveau de dégradation introduit par d'autres traitements sur l'image. Parmi ces mesures, on trouve des métriques basées sur la comparaison des pixels entre l'image hôte et l'image tatouée.

Parmi les métriques basées sur la différence des pixels, on cite: PSNR, MSE.(voir le chapitre 5 : compression d'images médicales

9. Les attaques

Une attaque est tout traitement sur l'image susceptible de modifier la marque ou de créer une situation ambigüe lors de son extraction. Il existe quatre types d'attaques:

a) Les attaques géométriques

Permettent de déformer ou déplacer l'image tatouée telles que la translation, la rotation, l'agrandissement, la réduction,...

b) Les attaques de traitement d'image

Elles s'inspirent du domaine de traitement d'image qui tente d'évaluer ou d'estimer l'image originale à partir de l'image tatouée en appliquant plusieurs traitements (compression, lissage, conversion analogique numérique, addition de bruit, filtrage,.....).

c) Les attaques cryptographiques

Elles relèvent du domaine de la cryptographie telle que la collusion (deux textes différentes donnant une même signature).

d) Autres attaques

Elles ne cherchent pas à supprimer la signature mais à insérer une autre signature pour fausser l'identification du propriétaire.

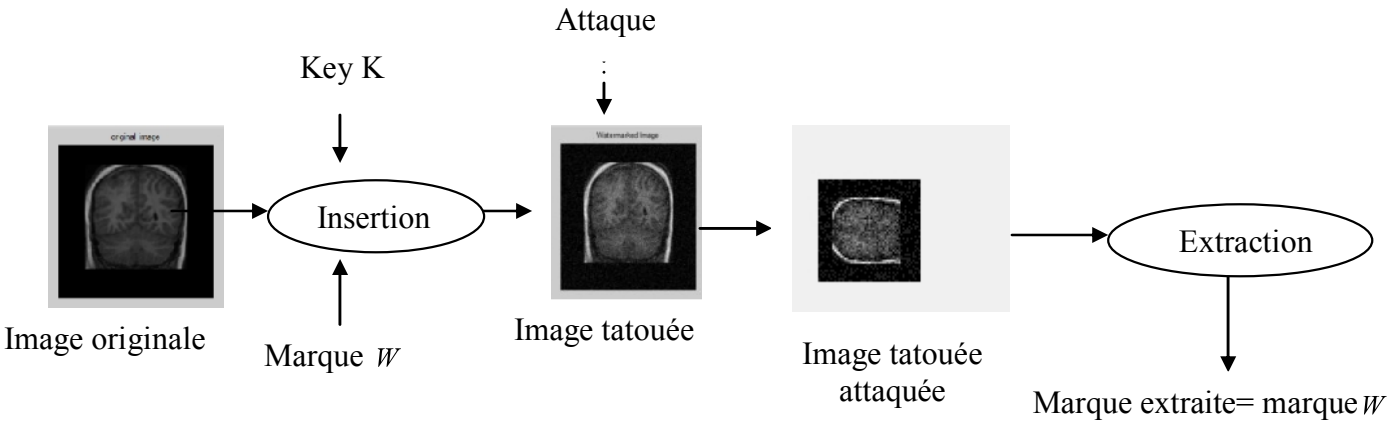


Figure6.7: Schéma général d'un système de tatouage attaqué par rotatıon.

10. Techniques de tatouage appliquées au domaine médical:

L'objectif du tatouage est d'insérer une information dans l'image de manière invisible et indélébile. L'insertion du message peut s'effectuer dans le domaine spatial ou fréquentiel, la technique du tatouage a pour but de résoudre des problèmes variés relatifs à la sécurité des données digitales telles que la protection des droits d'auteur, la prévention de la redistribution non autorisée, l'intégrité du contenu d'une donnée, etc.

Nous présentons quelques méthodes représentatives du tatouage d'image.

Ces méthodes sont classées selon le domaine d'insertion, le type d'algorithme utilisé et du domaine d'application ou types de propriétés de sécurité demandées.

10.1. axonomie des techniques du tatouage numérique

Cette partie n'a pas pour objectif de dresser une revue exhaustive de toutes les techniques disponibles dans la littérature. N´eanmoins, nous d´ecrivons les grandes lignes de certaines catégories du tatouage numérique dans le but de montrer à quel point le sujet est vaste. Les algorithmes de tatouage se distinguent les uns des autres essentiellement par les trois points clés suivants :

- La manière de sélectionner les points (ou blocs) dans l'image hôte qui porteront l'information cachée selon une clef secréte.
- Le choix d'un espace de travail pour réaliser l'opération d'enfouissement (dans le domaine spatial ou transformé comme DCT, ondelettes, Fourier,etc.).
- La manière de mélanger intimement le message avec l'image hôte ; l'idée de base consiste le plus souvent à imposer une relation binaire entre les bits du message et des caractéristiques choisies de l'image hote.

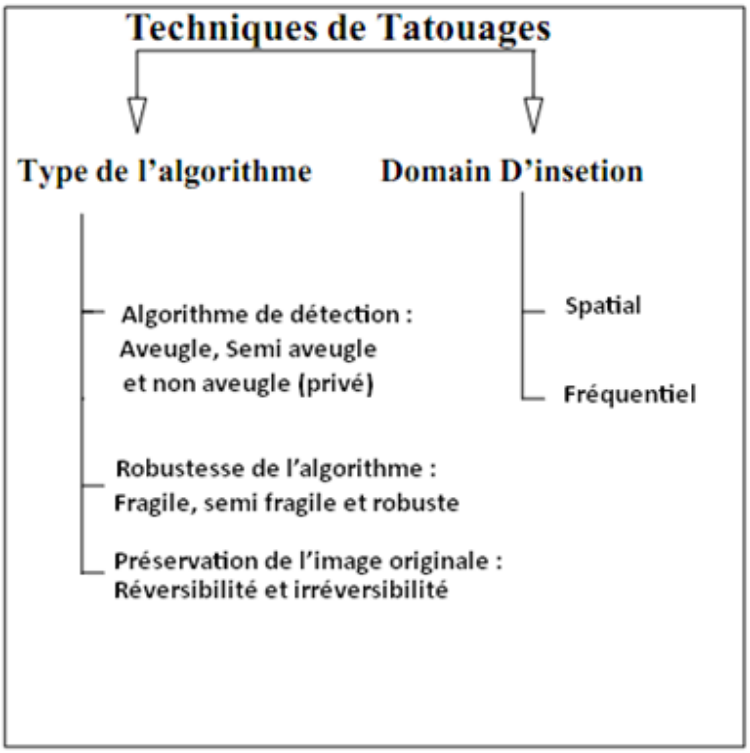


Fig. 2.5 : Taxonomie des techniques du tatouage numérique.

Une taxinomie des techniques de tatouage est présentée sur la base de plusieurs publications. La raison de cet arrangement est de fournir une vue générale de plusieurs principaux domaines du tatouage. Nous avons choisit le domaine d'insertion comme un critéres pour regrouper les techniques du tatouage. (voir figure 2.5)

10.2 Classification des algorithmes selon le domaine d'insertion

Les techniques courantes décrites dans la littérature peuvent etre regroupées en deux principales classes : techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

a.***Domaine spatial :*** Cette approche consiste en la modification directe des pixels de l'image. Afin d'assurer l'imperceptibilité de la marque, cette modification doit rester limitée. Une des toutes premières approches utilisée consiste à insérer les bits du message dans les bits de poids faible de chaque pixel (least significant bits, LSB) . Une autre approche, appelée patchwork , est la modification des propriétés statistiques de petites régions de l'images, comme la moyenne ou l'écart-type, le message étant représentée par exemple par la différence des ces propriétés entre deux régions adjacentes.

b. Domaine de transformée en cosinus discrtète (DCT) :

b.1 La transformée en cosinus discrète

La transformée en cosinus est une variante de la transformée de Fourier discrète. Elle transforme un signal réel en un autre signal réel, la notion de phase disparaissant en même temps que la partie imaginaire. On considère cependant qu'on obtient toujours une représentation fréquentielle du signal de base.

Le calcul de la transformée discrète en cosinus d'une image x de dimensions NxN s'effectue grâce à la formule:

$$DCT(m,n) = \frac{1}{\sqrt{2N}} c(m).c(n) \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} x(k,l) \cos\left(\frac{(2k+1)m\pi}{2N}\right) \cos\left(\frac{(2l+1)n\pi}{2N}\right) \quad (2.3a)$$

$$avec\ c(m) = \begin{cases} \frac{1}{\sqrt{2}} \ si\ i = 0 \\ 1 \ si\ i > 0 \end{cases} \quad (2.3b)$$

b.2 Méthodes de tatouage utilisant la transformée en cosinus discrète

La principale méthode utilisant la DCT est celle de Zhao . Elle consiste tout d'abord à diviser l'image source en un certain nombre de carrés de 8x8 pixels, puis à effectuer la transformée en cosinus de ces blocs. Les bits du watermark sont alors insérés sur les moyennes fréquences, sachant que la modification des basses fréquences modifierait trop l'image et que les hautes fréquences sont enlevées par la compression JPEG. La clé de codage utilisée correspond à l'emplacement des blocs marqués, et est nécessaire pour décoder le tatouage. Par contre, l'algorithme d'extraction n'a besoin ni du support non marqué, ni de la marque.

Contrairement à Zhao, Piva propose d'effectuer la transformée en cosinus de toute l'image puis, en s'inspirant de la compression JPEG, de réordonner les coefficients en zigzag. Certains de ces coefficients seront modifiés en leur additionnant la marque suivant un facteur de pondération lié au SVH. Ces coefficients ne sont ni les premiers (pour des raisons d'invisibilité), ni les derniers (pour des raisons de robustesse). La détection de la marque s'effectue en calculant la corrélation entre le marquage supposé et les coefficients extraits de l'image marquée. Cette méthode est donc aveugle de type I.

c.Utilisation de la transformée multi résolutions

c.1 La transformée en ondelettes

La transformée en ondelettes est basée sur le même principe que la transformée de Fourier, si ce n'est que la sinusoïde complexe y est pondérée par une fonction centrée, fenêtrée, et d'intégrale nulle. Cette fonction peut être de différents types, mais a toujours la particularité, suite à une compression ou une expansion, de s'adapter à la fréquence du signal. En effet, une compression temporelle de l'ondelette entraîne une augmentation de la fréquence, alors qu'une expansion temporelle la diminue.

Tout signal f peut s'écrire sous la forme d'une superposition d'ondelettes $\psi_{a,b}$ obtenues par translation et dilatation de l'ondelette mère ψ.

$$f = K \int T(a,b).\psi_{a,b}(t).\frac{da}{a}db \qquad (2.5a)$$

$$avec\ \psi_{a,b}(t) = \frac{1}{a}\psi(\frac{t-b}{a}) \qquad (2.5b)$$

En pratique, pour des images, la décomposition en ondelettes est effectuée grâce à une décomposition multi résolutions effectuée avec un banc de filtres. Elle est en effet réalisée grâce à une succession de filtrages passe-bas et passe-haut directionnels, suivis de sous-échantillonnages. Ces filtrages et sous-échantillonnages sont réalisés n fois, n correspondant alors au niveau de la décomposition.

Pour chaque niveau on obtient 4 images:

- l'image passe-bas, ou d'approximation qui sera filtrée au niveau suivant,
- l'image passe-haut horizontale,
- l'image passe-haut verticale,
- l'image différence résultante, abusivement appelée passe-haut diagonale.

Les 3 images passe-haut sont aussi appelées images détails.

c.2 Méthodes de tatouage utilisant la transformée multi résolutions

Les informations rendues accessibles par la décomposition DWT (fréquence, emplacement, orientation) permettent une grande finesse de réglage lors de l'insertion, et donc un panel de possibilités extrêmement important, d'où la profusion des techniques de tatouage se basant sur les ondelettes. Pour avoir une description de ces techniques, le lecteur pourra se reporter à M. Peter .

L'algorithme de Xie, insère la marque dans l'image approximation. Le niveau de décomposition dépend de la taille des informations que l'on souhaite insérer, de l'invisibilité et de la robustesse recherchées. L'insertion s'effectue en quantifiant les coefficients à modifier suivant la valeur du bit à insérer. La table de quantification utilisée est générée à partir des valeurs des coefficients voisins. La détection ne nécessite ni l'image non marquée ni la marque insérée.

Kunder et Hatzinakos,proposent une technique du tatouage fragile. Le watermark est une sequence binaire. Il est inséré dans les coefficients des détails de l'image hote avec l'utilisation d'une clef. Cette clef est générée aléatoirement et est employée pour choisir les endroits exacts dans le domaine de l'ondelette. Pour chaque coefficient, la clef a une valeur correspondante de 1 ou de 0 pour indiquer si le coefficient doit etre marqué ou pas, respectivement. Le nombre de 1 dans la clef doit etre plus grand ou égal à la taille du watermark.

10.3 Evaluation des algorithmes de tatouage

Bien que travaillant sur des différentes méthodes de tatouages, il est intéressant d'évaluer ces méthodes. Nous devons retenir un critère de dissimilarité entre l'image de départ et l'image tatouée. La plupart des publications utilise le PSNR comme critère de dissimilarité. Ainsi nous devons tester les algorithmes contres les transformations (attaques) les plus courantes utilisées.

La mesure de distortion la plus populaire en traitement d'image étant tout simplement le rapport signal sur bruit (PSNR Peak Signal Noise Ratoi). Il est mesuré en décibel (dB) à partir de relation suivante :

$$(PSNR)_{dB} = 10log_{10}(M.N \max {I^2}_{m,n} / \sum(I_{m,n} - {I'}_{m,n})^2) \qquad (2.6)$$

Où $I(m,n)$ est la valeur du pixel(m,n) de l'image référence et $I'(m,n)$ celle de l'image à tester, les deux images étant de taille $[M\ N]$. On considère généralement en tatouage d'images qu'un tatouage est imperceptible pour un PSNR supérieur à $36\ dB$, et plus il est élevé, moins la distortion est importante.

Attaques :

Il existe des transformations appliquées sur les images qui peuvent apporter des distorsions importantes à la marque insérée et changer son comportement. Ces transformations peuvent être vues comme des attaques malveillantes (compression, filtrage, zoom, rotation…) . Nous allons présenter dans cette partie une liste ces manipulations.

Rehaussement et lissage

Le rehaussement correspond à l'augmentation des composantes hautes fréquences de l'image. L'image devient alors plus contrastée. Le lissage est l'opération contraire du rehaussement, il atténue les composantes hautes fréquences de l'image qui devient alors plus floue. Ces opérations peuvent modier également les composantes hautes fréquences du message et leur faire perdre leurs particularités.

Transformations géométriques usuelles

Parmi les transformations géométriques, la plus usuelle est la modication des dimensions de l'image et les transformations afines telles que la rotation, la translation et le zoom. Ce genre de transformation provoque dans la plupart des cas une désynchronisation de la marque insérée lors de l'extraction.

Bruitage et filtrage

Le bruit est une altération de l'image, des exemples de bruit artificiel peuvent etre le bruit gaussien qui consiste en ajouts successifs de valeurs générées aléatoirement à chaque pixel d'une image, ou encore le bruit sel et poivre qui transforme aléatroirement des pixels de l'image en pixel noir ou blanc. Pour récupérer l'information pertinente dans l'image on put utiliser différents types de filtres : median, gaussien, laplacien…

Le gigue (Jittering) est un phénomène connu en télécommunications. Lorsque le délai de transmission du signal varie, il en résulte une réplication ou une suppression d'un morceau du signal. Ceci peut se produire dans le domaine spatial ou temporel sur les images, il peut y avoir un ajout ou une suppression de lignes ou de colonnes.

Stirmark[1] est un logiciel qui permet d'apprécier la robustesse d'un procédé de marquage. Ce logiciel propose une banque de tests avec une grande variété de traitements sur les images, comme les manipulations présentées précédemment et plusieurs distorsions géométriques.

10.3.1 Vérification d'intégrité

10.3.1.1 Notion d'intégrité

La notion d'intégrité visuelle est un concept bien connu en sécurité. Sa définition repose sur une décision binaire qui garantit que les données reçues sont rigoureusement identiques à celles émises. En d'autres termes, le problème de l'intégrité des images se pose principalement en termes de contenu sémantique ; c'est-à-dire la détection des modifications du document pouvant engendrer une gêne dans sa visualisation et/ou une erreur dans son interprétation. Dans le but d'assurer un service d'intégrité approprié aux images, il est donc primordial de distinguer les attaques consistant à détourner le contenu initial de l'image, des manipulations liées à son utilisation ou son stockage sous une forme numérique (conversion de format, compression, ré-échantillonnage, filtrage, etc.).Par exemple, dans le cas de l'imagerie médicale, des manipulations anodines, comme une simple compression, voire le processus de tatouage lui-même, peuvent causer la disparition de certains signes visibles d'une pathologie faussant alors le diagnostic du médecin. Dans ce contexte, l'utilisation des méthodes de tatouage fragile sera plus appropriée pour garantir une intégrité stricte du document.

10.4 Tatouages fragiles

10.4.1 Principe

Les premières méthodes proposées pour assurer un service d'intégrité étaient basées sur l'utilisation d'un tatouage fragile. Le principe de cette approche est d'insérer une marque ou un logo binaire dans l'image hôte de telle manière que les moindres modifications apportées à l'image se répercutent également sur la marque insérée (Figure 2.6.a). Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence de cette marque (Figure 2.6.b).

[1] http ://www.petitcolas.net/fabien/watermarking/stirmark/

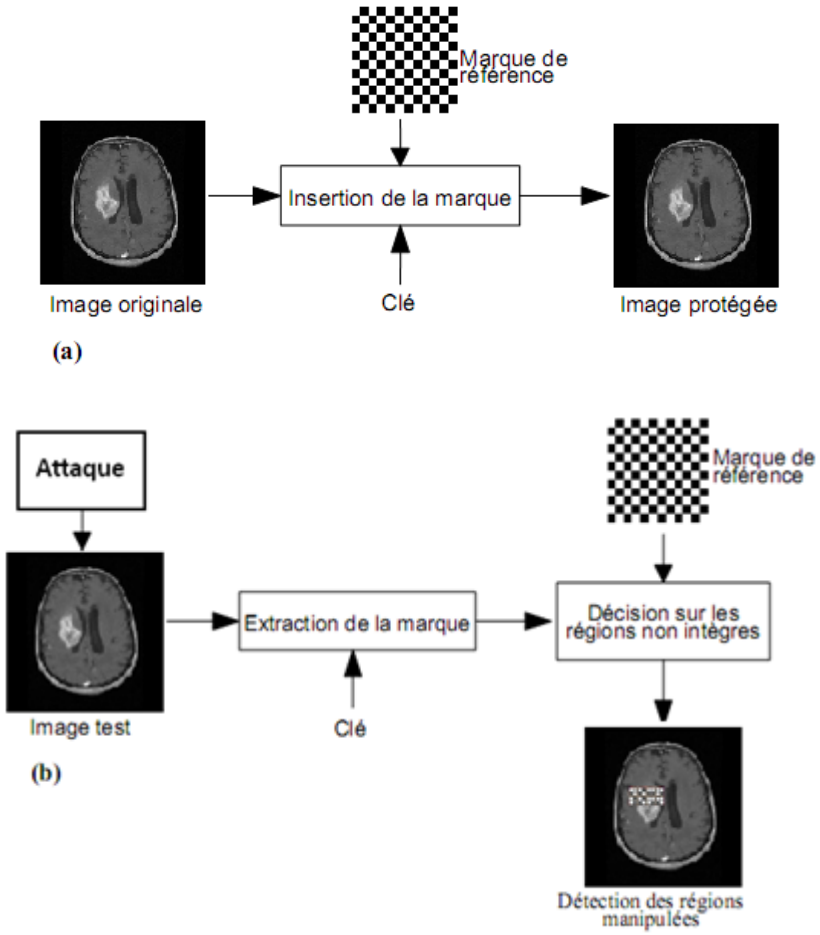


Fig. 2.6 : Schéma général d'un système d'intégrité basé sur un tatouage fragile.

Nous avons implémenté deux algorithmes parmi les différentes méthodes fragiles.
Le choix s'est porté sur les algorithmes les plus utilisés et sur ceux qui, d'après la littérature, obtiennent les résultats les plus intéressants, soit:
-l'algorithme de Fridrich (insertion dans le domaine spatial),
-l'algorithme de Kundur (insertion dans le domaine de la transformée multi résolutions).

10.4.2 Algorithme de Fridrich

Fridrich , propose une technique de tatouage fragile. La marque binaire utilisée correspond à un signal pseudo-aléatoire généré à partir d'une clé secrète et du numéro du bloc. Ensuite chaque de ce dernier est tatoué en utilisant l'algorithme suivant :

1) Les pixels de l'image sont assemblés en groupes de pixels (blocs...).
2) Deux fonctions commutatives $f(x_1; x_2; \dots)$ et $F(X)$ sont définies :

- la fonction f dite de discrimination , cherche à mesurer la régularité des groupes de pixels.Cette fonction peut-être, par exemple, la fonction 'variation'

$$f(x_1, x_2, \dots) = \sum_{i=1}^{N-1} |x_{i+1} - x_i|$$

- la fonction F de permutation tel que $F(F(X)) = X$. Cette fonction peut-être par exemple la fonction qui à 1 associe 0 et à 0 associe 1, à 3 associe 2 et à 2 associe 3, ...

3) Pour chaque groupe de pixels est attribuée une catégorie R, S ou U suivant le schéma suivant :
   - R (Regular) si $f(F(G)) > f(G)$
   - S (Singular) si $f(F(G)) < f(G)$
   - U (Unusable) si $f(F(G)) = f(G)$
4) La carte binaire de localisation contenant les positions de R et S est compressée et rajoutée aux données à embarquer.
5) Le code 0 est attribué au groupe R, le code 1 au groupe S. Pour faire changer d'état un groupe de pixels, il suffit de lui appliquer la fonction F.
6) Lors de la reconstruction, il suffira de réappliquer la fonction de permutation, suivant la carte de localisation, sur un pixel pour obtenir la valeur initiale du pixel.

Exemple

Soit le groupe de pixel G suivant :

A	B
C	D

La fonction de discrimination est calculée sur ce groupe :

$$f1 = f(A,B,C,D)$$

La fonction de permutation est calculée pour chaque pixel :

$$A' = F(A)\ B' = F(B)\ C' = F(C)\ C' = F(C)$$

La fonction de discrimination est calculée sur le nouveau groupe :

$$f2 = f(A',B',C',D')$$

Si $f1 = f2$ le groupe est dit "unusable" et donc non retenu.
Si $f1 > f2$ le groupe est dit "singular" et équivaut à la valeur 1.
Si $f1 < f2$ le groupe est dit "regular" et équivaut à la valeur 0.

Si le groupe ne correspond pas à la valeur désirée pour le marquage, les valeurs (A,B,C,D) du groupe de pixels sont substituées par les valeurs du groupe permuté (A',B',C',D').

Lors de la reconstruction suivant la carte embarquée, il suffira de réappliquer la fonction de permutation sur (A',B',C',D') pour obtenir (A,B,C,D).

10.4.3 Algorithme de Kundur

Kundur ,propose d'utiliser la transformée en ondelettes (DWT) car celle-ci permet à la fois d'avoir une localisation des dégradations et un étalement spectral de la marque. Les données sont insérées en quantifiant certains coefficients des images détails des trois premiers niveaux. Le choix de ces coefficients est déterminé par une clé de façon à ce que les données insérées soient étalées spatialement et sur toutes les résolutions. La quantification de ces coefficients suivant les données à insérer s'effectue en découpant l'espace des réels avec un pas de quantification Δ. A chaque intervalle est associée, alternativement, la valeur binaire 0 ou 1 (Figure 2.7). Ainsi, si au coefficient d'ondelettes correspond la valeur binaire à insérer, le coefficient d'ondelettes n'est pas modifié. Par contre, si les valeurs ne correspondent pas, le coefficient est modifié en lui ajoutant ou lui soustrayant Δ, suivant qu'il est négatif ou positif, respectivement.

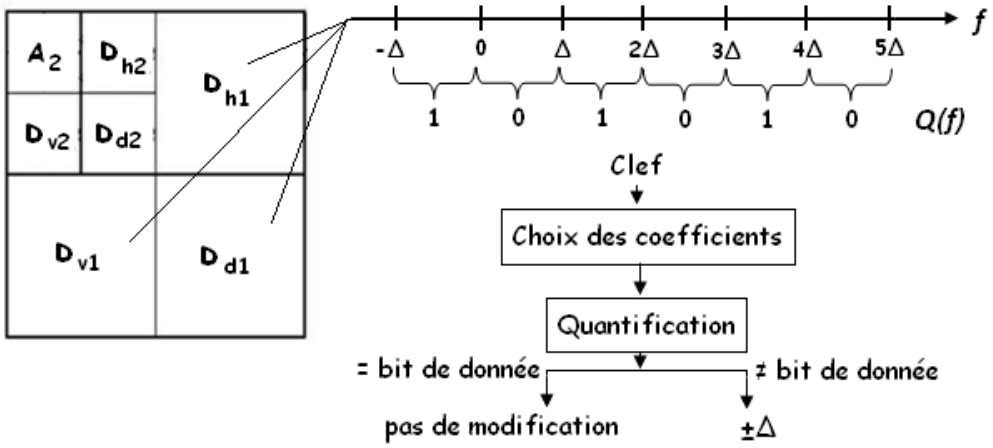


Fig. 2.7 : mécanisme d'insertion dans la méthode de Kundur.

La principale difficulté d'implémentation de cet algorithme est l'obligation, après la transformée en ondelettes inverse, de retrouver des valeurs de pixels entières (d'où des précautions dans le choix de Δ et de l'ondelette utilisée).

Pour répondre à ce problème, Kundur propose d'utiliser la transformée en ondelettes basée sur l'ondelette de Haar. En effet, celle-ci permet d'obtenir des coefficients de la forme $r/2^l$où r est un entier et l le niveau de résolution du coefficient considéré. Les modifications de coefficients se font alors en ajoutant ou retranchant un multiple de $1/2l$, ceci garantissant de retrouver un entier lors de la transformée inverse.

La règle de quantification est alors la suivante:

$$Q_\delta(f) = \begin{cases} 0, si \ \left\lfloor \frac{f}{\delta 2^l} \right\rfloor \ est \ pair \\ 1, si \ \left\lfloor \frac{f}{\delta 2^l} \right\rfloor \ est \ impair \end{cases} \quad (2.7)$$

Où δ est un entier positif donnant le pas de quantification Et⌊. ⌋ est la fonction arrondie à l'entier inférieur.

a. Algorithme implémenté

a.1 Insertion de la marque

La première étape consiste à appliquer une décomposition en ondelettes avec l'ondelette mère Haar jusqu'à l'échelle D. Nous sélectionnons ensuite un ensemble de coefficients de détails à partir d'une clef secrète, notés $c_{hD}(x,y)$, $c_{vD}(x,y)$ et $c_{dD}(x,y)$.

L'insertion consiste à déplacer les coefficients ($c_{hD}(x,y)$, $c_{vD}(x,y)$ et $c_{dD}(x,y)$) en fonction de la valeur du bit de la marque W pour cette coordonnée, et d'un pas de quantification, défini par l'équation de quantification (2.7).

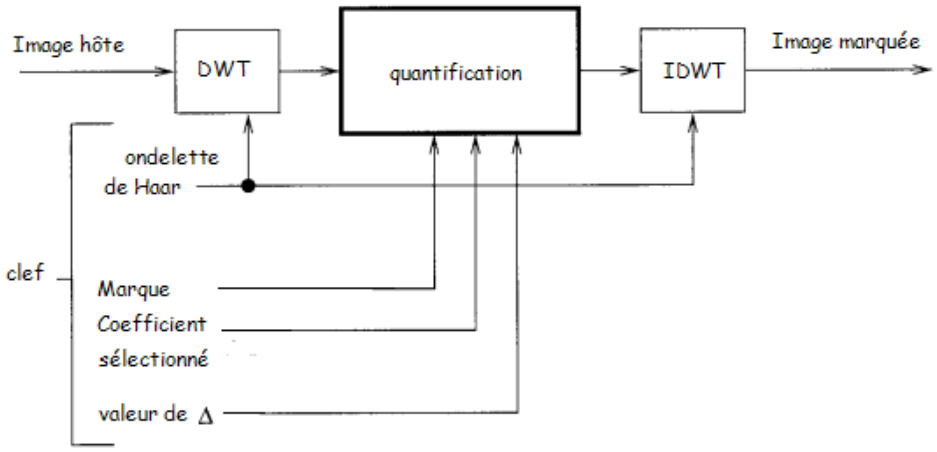


Fig. 2.8 : Schéma d'insertion.

Sur la figure 2.9, nous observons un exemple de quantification de deux coefficients $c_{1D}(x,y)$ et $c_{2D}(x,y)$, en fonction de Δ. Suivant la valeur de la marque, les coefficients $c_{1D}(x,y)$ et $c_{2D}(x,y)$ marqués, notés $c_{1DW}(x,y)$ et $c_{2DW}(x,y)$, seront placés à un nombre pair (si $W(x,y) = 1$), ou impair (si W(x, y) = 0) de Δ.

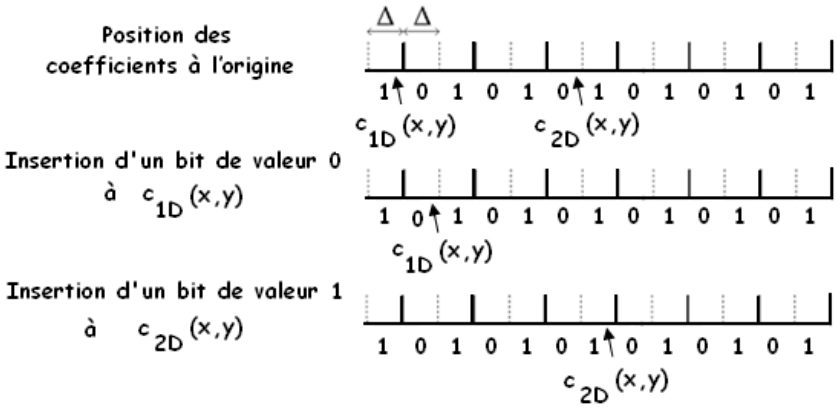


Fig. 2.9 : Exemple d'insertion. (Algorithme de Kundur)

Cette opération est répétée pour chaque coefficient. Puis l'image est reconstruite dans le domaine spatial.

a.2 Détection de la marque

La détection de la marque est basée sur le même schéma que celui présenté en figure 2.8. Après avoir effectué une transformée en ondelettes de l'image à l'échelle D, les coefficients sont sélectionnées

à partir de la clef secrète. Ensuite, le pas de quantification Δ est évalué selon la valeur Q, la valeur du bit de la marque détectée à la coordonnée (x, y) est lue en fonction de la position des coefficients sélectionnés par rapport à la valeur Δ défini par l'équation de quantification (2.7)

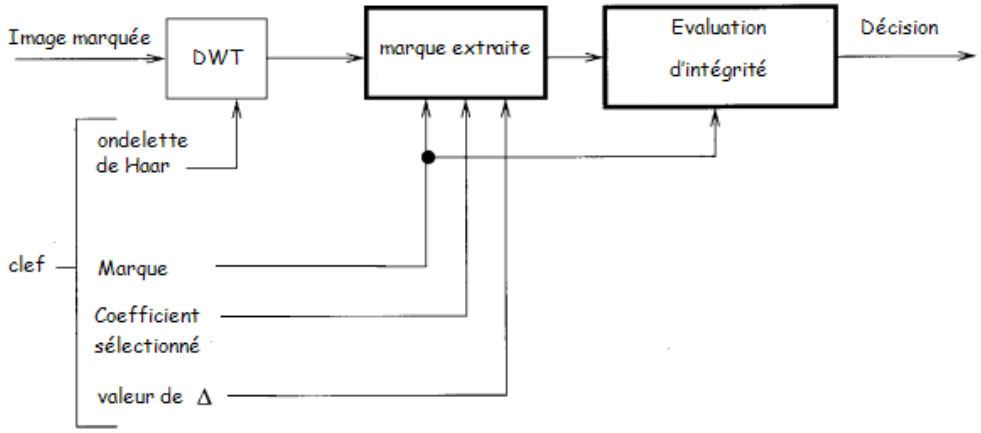


Figure. 2.10 : Schéma de détection. (Algorithme de Kundur)

a.3 Décision

La dernière étape de l'algorithme consiste à décider si la marque détectée correspond effectivement à la marque insérée. Pour cela, une mesure de TAF est proposée par Kundur , telle que :

$$TAF(w,w') = \frac{1}{N_w}\sum_{i=1}^{N_w} w(i) \oplus w'(i) \qquad (2.8)$$

Où W la marque insérée, W' la marque extraite, N_w la longueur de la marque et $\oplus$ est l'opérateur ou exclusif XOR.

La présence d'une altération est déterminé si TAF (w, w ') ≥ T, T étant le seuil de décision notons que 0≤T≤1. Si TAF <T, alors les modifications de l'image sont considérées négligeable ou les deux marque coïncident parfaitement.

11 Protection des données médicales

Dans cette section nous allons présenter des solutions de sécurité pour les images médicales, basées sur les concepts avancés pour but d'assurer la confidentialité des données.

11.1 Tatouage robuste

L'objectif est d'insérer directement dans l'image les données pertinentes du patient d'une manière secrète et robuste. Ceci permettra en plus de faire transiter l'image seule, sans avoir besoin de l'accompagner d'un fichier textuel. Les méthodes utilisées doivent donc être robustes.

Parmi les algorithmes de tatouages robustes présentés dans la littérature, nous avons choisi l'algorithme de Xie à implémenter et tester.

11.1.1. Algorithme de Xie

Xie , insère la marque dans l'image approximation d'une décomposition multi niveaux. Le niveau de décomposition dépend de la taille des informations que l'on souhaite insérer, de l'invisibilité et de la robustesse recherchées.

L'insertion s'effectue en faisant évoluer dans toute l'image approximation, une fenêtre b_j de taille 3x1 sans chevauchement. Pour chaque position de la fenêtre, les trois coefficients sont rangés dans l'ordre croissant de leur valeur. Ensuite, l'espace entre la valeur minimale b_1 et la maximale b_3 est divisé en intervalles de longueur S_α:

$$S_\alpha = \alpha \frac{b_{(3)} - b_{(1)}}{2} \qquad (2.9)$$

On obtient alors la configuration suivante:

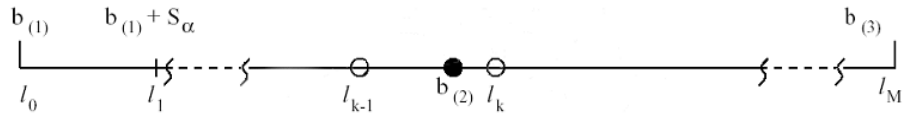


Fig. 2.11 : Ordonnancement des coefficients avant insertion. (algorithme de Xie)

Quatre cas peuvent alors se présenter, suivant que le bit à insérer (x) soit "0" ou "1" et que k soit pair ou impair.

Si k est pair:

Si $x = 0$, alors $b_{(2)}$ est mis à la valeur de l_k

Si $x = 1$, alors $b_{(2)}$ est mis à la valeur de l_{k-1}

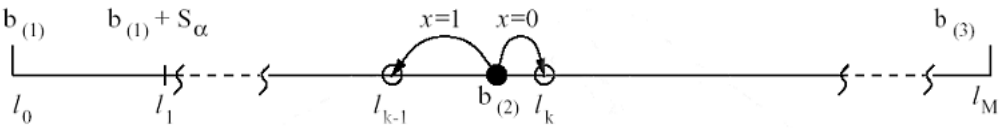


Fig. 2.12 : Cas où k est pair.

Si k est impair:

Si $x = 0$, alors $b_{(2)}$ est mis à la valeur de l_{k-1}

Si $x = 1$, alors $b_{(2)}$ est mis à la valeur de l_k

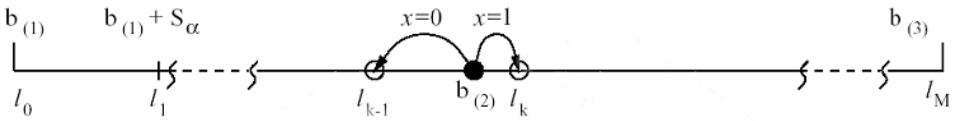


Fig. 2.13 : Cas où k est impair.

Enfin, les coefficients sont réinsérés à leur place initiale dans l'image approximation.

La détection s'effectue en réeffectuant, pour chaque position de la fenêtre (que l'on fait à nouveau évoluer dans toute l'image d'approximation à l'aide de la clé secrete), l'ordonnancement des coefficients et la division de l'espace entre les deux extrêmes. Il suffit alors de prendre le l_k le plus proche du $b_{(2)}$. Si k est pair, le bit inséré était "0", sinon c'était "1".

La détection ne nécessite donc ni l'image non marquée, ni la marque insérée. Cette méthode est donc aveugle.

Le mécanisme d'insertion de cet algorithme peut être réglé par certains paramètres qui modifient considérablement le nombre de bits de données insérés, la robustesse de la marque et l'impact visuel de l'insertion. Ces paramètres sont:

- De 1 à 4 est le niveau de décomposition en ondelette.
- Le pas de quantification (déterminé par α).
- Il faut choisir la fenêtre $b(j)$ de telle manière, les trois coefficients sont différent entre eux.

Ces trois paramètres combinés entraînent une palette de réglages très importante, et donc de résultats extrêmement divers.

12. Conclusion

Le tatouage des images joue un rôle important dans le domaine de l'imagerie médicale et particulièrement dans les applications de télémédecine afin d'assurer lasécurité des images médicales et les données correspondantes relatives au propriétaire.

Dans ce chapitre, nous avons présenté la technologie du tatouage numérique d'une manière générale.
Nous nous sommes intéressés aux terminologies et notions liées aux techniques du tatouage invisible et aveugle des images médicales.Ces terminologies sont nécessaires dans le domaine de la sécurisation de l'information médicales ,telle que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle.

Plusieurs travaux et méthodes ont été réalisés dans le but de vérifier l'une ou l'autre des propriétés de sécurité. Dans le but de contribuer à réunir les trois propriétés de ,sécurité (confidentialité, intégrité et authentification); nous avons présenté aussi une taxonomie des techniques du tatouage selon le domaine d'insertion.

Les techniques de ce dernier peuvent être regroupées en deux catégories : ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel. Dans cette dernière catégorie plusieurs transformées peuvent être utilisées telles que la DFT, DCT et DWT.

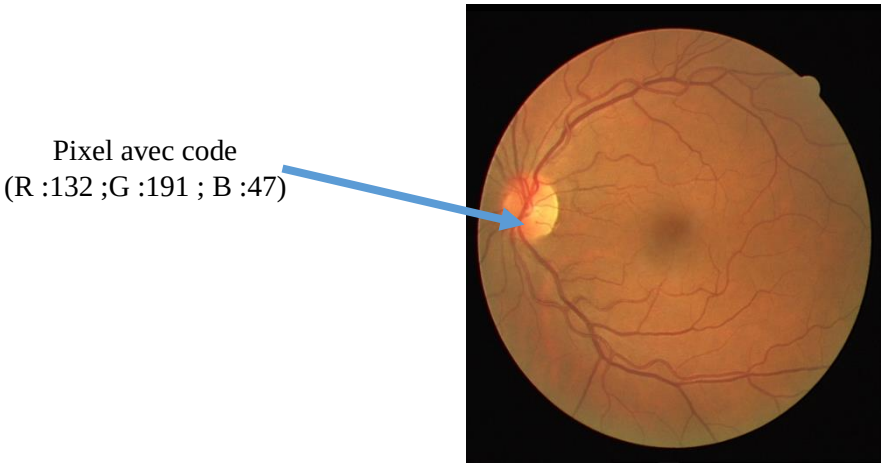
Série TD N°6 : CRYPTAGE ET TATOUAGE

Exercice 1 : Codage RSA

En imagerie médicale, les communications réseaux et les fichiers informatiques utilisent le standard *DICOM*. Le chiffrement permet de limiter la visualisation des informations d'une image aux seules personnes possédant la clé de déchiffrage. Un algorithme de cryptographie asymétrique comme par exemple *RSA* peut être utilisé. Le destinataire des images génère une paire de clés : une clé publique et une clé privée, ces deux clés sont liées. Le destinataire communique uniquement sa clé publique aux personnes souhaitant lui communiquer de manière chiffrée des images, mais lui seul pourra les déchiffrer à l'aide de sa clé privée qu'il ne communique à personne.

Dans le domaine médical, les images médicales sont cryptées pour de nombreuses raisons.

1. Quels sont ces raisons ?



2. Nous voulons chiffrer une image rétinienne couleur (RGB) avec l'algorithme RSA, l'un des plus utilisé actuellement. On applique l'algorithme RSA sur le Pixel avec code (R :132 ;G :191 ; B :47),calculer la clé publique et la clé privé.
3. Chiffrer chaque code couleur de notre image.
4. quels est l'inconvénient de l'algorithme RSA ?
5. Ecrire un programme Matlab qui permet de :
   5.1.générer les deux clés privée et public.
   5.2. Chiffrer l'image médicale avec la clé publique
   5.3.Déchiffrer l'image médicale avec la clé privée
6. Le nom du patient est pseudonymisé à l'aide d'une fonction de hachage cryptographique comme *HMAC* qui nécessite une clé secrète uniquement connue par le

responsable du traitement, et les autres informations sur l'identité du patient sont anonymisées en les remplaçant simplement par 'XXXXXXX'. Cette sera archivée dans le *PACS* avec comme nom de patient le code d'authentification *HMAC*, elle pourra par la suite être retrouvée dans le *PACS* en recalculant le code *HMAC* à partir du nom du patient.

Ecrire un programme en Matlab qui permet d'afficher le code *HMAC* correspond au nom du patient et sa date naissance,et prodonomiser cette image DICOM

Exercice 2 : tatouage fragile (algorithme de fridirich)

Soit le groupe de pixel G suivant de l'espace ROUGE de l'image rétinienne donné dans l'ex 1 :

$$G= \begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}$$

1. Appliquer l'algorithme de fridirich sur ce groupe de pixel en calculant les deux fonctions cummutatives $f(x_1,x_2,\ldots x_n)$ et F(X).
2. quel est votre constatation à propos de l'application de cet algorithme sur des images médicale ? Proposer une solution adaptative sur ce type d'image par un algorithme modifié ?
3. cité d'autres algorithmes de tatouage performant aux images médicales.

Solution série TD N°6

EX N°1 :

Rappel de cours : L'algorithme RSA a été décrit par Ron Rivest, Adi Shamir et Len Adleman.. Cet algorithme asymétrique par bloc est très populaire pour le cryptage des données numériques. La sécurité du RSA repose sur la difficulté de factorisation de grands nombres entiers. Soit $n = pq$, où p et q sont premiers. $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ et $\mathcal{K} = (n, p, q, a, b)$. La fonction de cryptage e_K et décryptage d_K sont définies par les équations :

$$y = e_K(x) = x^b \bmod n \quad \text{et} \quad d_K(y) = y^a \bmod n$$

où $(x, y \in \mathbb{Z}n)$, $\varphi(n) = (p-1)(q-1)$ et $ab \equiv 1 \bmod \varphi(n)$. Les valeurs n et b sont publiques et p, q et a sont privées. Les étapes suivantes font une synthèse de la construction d'un cryptosystème RSA.

a) Choisir aléatoirement p et q, deux grands nombres premiers distincts.
b) Calculer $n = pq$ et $\varphi(n) = (p-1)(q-1)$.
c) Désigner un entier b, avec $1 < b < \varphi(n)$ tel que $pgdc(b, \varphi(n)) = 1$.
d) Calculer $a = b^{-1} \bmod \varphi(n)$ avec l'algorithme Euclidien.
e) Divulguer la clef publique (n, b).

1. Les images médicales sont cryptées pour de nombreuses raisons, y compris :

- Identifier le créateur de l'image
- Protéger les informations de droit d'auteur
- Dissuader le piratage
- Bloquer les images d'être vu par des utilisateurs qui ne devraient pas y avoir l'accès.

2. On va chiffrer cette image par l'algorithme RSA

- Choisir deux entiers premiers ; p =7 et q=19

Calculer $n = pq = 133$

et $\varphi(n) = (p-1)(q-1) = (7-1)(19-1) = 108.$

On choisit e supérieur à 1 , premier avec 108 comme exposant de chiffrement donc e = 5

La clés publique (e=5 ;n=133)

Calcul d tel que :

Comme e est premier avec φ(n), d'après le théorème de Bachet-Bézout il existe deux entiers d et k tels que ed + kφ(n) = 1, c'est-à-dire que ed ≡ 1 (mod φ(n)) : e est bien inversible modulo φ(n).

Le couple (n,e) est la clé publique de chiffrement, alors que (n, d) est la clé privée.

Pour k =1 ; 5 d = (7-1) (19-1)+1 donc 5d=109 et d =21.3 ….erreur

Pour k=3 ; 5d=3*(7-1)(19-1)+1 donc 5d=109 et d=65

La clé privé est (d=65 ; n=133)

3. Chiffrer chaque code couleur de notre image.

   On prend le code couleur d'une pixel de l'image (R :132,G :191,B :47) ;

   3.1.Chiffrement du code ROUGE (132)

   $C \equiv M^e \pmod n$--------$C=132^{5} \bmod(133)$;donc C=132

   Déchiffrement : $M \equiv C^d \pmod n$--------$M=132^{65} \bmod(133)$;donc M=132

   3.2.Chiffrement du code vert (191)

   $C \equiv M^e \pmod n$--------$C=191^{5} \bmod(133)$;donc C=39

   Déchiffrement : $M \equiv C^d \pmod n$--------$M=39^{65} \bmod(133)$;donc M=191

   3.3.Chiffrement du code bleu (47)

   $C \equiv M^e \pmod n$--------$C=47^{5} \bmod(133)$;donc C=73

   Déchiffrement : $M \equiv C^d \pmod n$--------$M=73^{65} \bmod(133)$;donc M=47

Donc le code pixel pour l'image crypté par RSA est de (R :132,V :39,B :73)

4. Quels est l'inconvénient de l'algorithme RSA ?

Parmi les inconvénients de RSA, on peut citer :

- Ses calculs consomment énormément de mémoire, il est considéré comme 1000 fois plus lent que son concurrent direct le DES.
- Un mauvais choix de ces paramètres p et q peut rendre le système de codage vulnérable et cassable par un bon algorithme de factorisation spécialisé.

5. programme Matlab

5.1. Générer une paire de clés : une privée et une public

```
// générer une paire de clés privée / public
pairKeys = generatePublicPrivateKeys()
// envoyer par email la clé public aux personnes souhaitant me communiquer des images cryptées
sendByEmail(pairKeys.public, ['ismaill80@yahoo.fr','clinique_azzouni@yahoo.fr'])
// conserver sur ma clé USB la clé privée pour décrypter des images
saveInFile(pairKeys.private, '/USB/myPrivateKey.txt')
```

5.2. Chiffrer l'image DICOM avec la clé publique :

```
// charger le fichier dicom en mémoire
dicom = readDicomFile('dicomfile.dcm')
```

```
// chiffrer le nom du patient à l'aide de la clé public
dicom.patientName = crypt(dicom.patientName, publicKey)
// chiffrer la date de naissance du patient à l'aide de la clé public
dicom.patientBirthdate = crypt(dicom.patientBirthDate, publicKey)
// sauvegarder la version chiffrée dans un nouveau fichier
writeDicomFile(dicom, 'cryptedDicomFile.dcm')
```

5.3.Déchiffrer l'image DICOM avec la clé privée

```
// charger le fichier DICOM en mémoire
dicom = readDicomFile('cryptedDicomFile.dcm')
// déchiffrer le nom du patient à l'aide de la clé privée
dicom.patientName = decrypt(dicom.patientName, privateKey)
// déchiffrer la date de naissance du patient à l'aide de la clé privée
dicom.patientBirthdate = decrypt(dicom.patientBirthdate, privateKey)
// sauvegarder la version déchiffrée dans un nouveau fichier
writeDicomFile(dicom, 'decryptedDicomFile.dcm')
```

6. Pour afficher le code *HMAC* qui correspond au nom du patient et sa date naissance :

```
// l'utilisateur indique le nom du patient
patientName = readFromKeyboard()
// l'utilisateur indique la date de naissance du patient
patientBirthdate = readFromKeyboard()
// calculer l'empreinte HMAC de l'ensemble (Nom du patient et date de naissance) à l'aide de la clé secrète : "je suis le responsable du traitement"
hmac = HMAC([dicom.patientName, dicom.patientBirthdate], 'je suis le responsable du traitement')
// afficher à l'écran la clé HMAC
printToScreen(hmac)
```

- Pour pseudonymiser une image *DICOM* :

```
// charger le fichier dicom en mémoire et le parser
dicom = readDicomFile('dicomfile.dcm')
// calculer l'empreinte HMAC de l'ensemble (Nom du patient et date de naissance) à l'aide de la clé secrète : "je suis le responsable du traitement"
hmac = HMAC([dicom.patientName, dicom.patientBirthdate], 'je suis le responsable du traitement')
// remplacer le nom du patient par la clé HMAC
dicom.patientName = hmac
// anonymiser le nom du patient
dicom.patientBirthdate = 'XXXXXX'
// sauvegarder les modifications dans un nouveau fichier
writeDicomFile(dicom, 'newdicomfile.dcm')
```

Exercice 2 :

1. Soit « 1 » le bit à cacher.

La fonction de discrimination est calculée sur ce groupe :

$f1(G) = \sum_{i=1}^{15} |x_{i+1} - x_i|$ Alors $f1(G) = 0$

La fonction de permutation est calculée pour chaque pixel :

$$G' = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}$$

La fonction de discrimination est recalculée sur le nouveau groupe :

$f2(G') = \sum_{i=1}^{15} |x'_{i+1} - x'_i|$ Alors $f2(G') = 0$

$f1 = f2$ Donc le groupe est dit "unusable" alors nous pouvons rien faire dans ce cas.

2. Nous constatons que l'inconvénient majeur de cette méthode sur les images médicales est la catégorie U (Unusable) du groupe de pixel, d'où nous ne pouvons pas utiliser cet algorithme dans ce domaine.

Nous proposons une modification sur cet algorithme pour éviter la catégorie U. Nous proposons deux fonctions de discrimination (la moyenne et la variance) et nous passons par deux phases de test, dans le cas où nous trouvons la catégorie U par la fonction de la moyenne, une grande probabilité de ne pas trouver cette catégorie par la fonction de la variance.

- Algorithme proposé :

Insertion

1- Découper l'image en bloc de taille $N * N$
2- Soit W la marque (séquence aléatoire)
3- Pour chaque bloc :
   - Calculer la moyenne du bloc original (M_o) et du bloc permuté (M_p).
   - Calculer la variance du bloc original (V_o) et du bloc permuté (V_p).

   Si $W = 1$ alors $bloc\_tatoué = max\ (M_o, M_p)$
   Si $W = 1$ et $M_o = M_p$ alors $bloc\_tatoué = max\ (V_o, V_p)$
   Si $W = 0$ alors $bloc\_tatoué = min\ (M_o, M_p)$
   Si $W = 0$ et $M_o = M_p$ alors $bloc\_tatoué = min\ (V_o, V_p)$
4- Reconstruction de l'image tatouée.

Extraction

1- Découper l'image en bloc de taille $N * N$

2- Pour chaque bloc :

- Calculer la moyenne du $bloc\_tatoué$ (M_t) et du $bloc\_tatoué\_permuté$ (M_{tp}).
- Calculer la variance du $bloc\_tatoué$ (V_t) et du $bloc\_tatoué\_permuté$ (V_{tp}).

Si $M_t > M_{tp}$ alors $marque\_extraite = 1$

Si $M_t < M_{tp}$ alors $marque\_extraite = 0$

Si $M_t = M_{tp}$ et $V_t > V_{tp}$ alors $marque\_extraite = 1$

Si $M_t = M_{tp}$ et $V_t < V_{tp}$ alors $marque\_extraite = 0$

Prenons le groupe de pixel G précédent :

Les fonctions de discrimination sont calculées sur ce groupe :

$M_o(G) = 0$

$V_o(G) = 0$

La fonction de permutation est calculée pour chaque pixel :

$$G' = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}$$

Les fonctions de discrimination sont calculées sur le nouveau groupe :

$M_p(G') = 1$

$V_p(G') = 0$

D'après l'algorithme modifié le group tatoué par le bit « 1 » est G'

$$G' = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}$$

3. Parmi les algorithmes de tatouage performant aux images médicales ce sont les algorithmes de kunder et Xie qui sont basé sur la transformée en ondelette ou sont classés comme des algorithmes de tatouage robuste pour la sécurisation des images médicales.

Chapitre 1 : système de gestion base de données

[1] Antoine Cornuéjols ,cours informatique 'base de donnée' 1er année .2011. http://www.lri.fr/~antoine/Courses/AGRO/TC/Cours-1A-BD-(v3)x2.pdf

[2] Maude Manouvrier, Systèmes de Gestion de Bases de Données (SGBD) relationnels, ENSTA,Mastèr Spécialisé en Architecture des Systèmes d'Information ;Cours C1-3. Maude Manouvrier - Univ. Paris Dauphine

[3] T. Connoly, C. Begg et A. Strachan, *Database Systems A Pratical Approach to Desigh, Implementation and Management*, 1998, ISBN: 0-201-34287-1,

[4] G. Gardarin, *Bases de Données - objet/relationnel*, Eyrolles, 1999, ISBN:2-212-09060-9, disponible à la BU 005.74 GAR

[5] R. Ramakrishnan et J. Gehrke, *Database Management Systems*, Second Edition; McGraw-Hill, 2000, ISBN: 0-07-232206-3, disponible à la BU055.7 RAM

[6] A. Silberschatz, H.F. Korth et S. Sudarshan, *Database System Concepts*,McGraw-Hill, 1996, ISBN: 0-07-114810-8, disponible à la BU 005.7 DAT

[7] J.D. Ullman et J. Widom, *A first Course in Database Systems*, Prentice Hall, 1997, ISBN: 0-13-887647-9, disponible à la BU 005.7 ULL

[8] C.J. Date, *An Introduction to Database Systems*, Addison Wesley

[9] C.J. Date, *A Guide to SQL Standard*, Addison Wesley

[10] R.A. El Masri et S.B. Navathe, *Fundamentals of Database Systems*, Prentice Hall

[11] Philip J. Pratt, *Initiation à SQL - Cours et Exercices corrigés*, Eyrolles, 2001 –BU : 005.72 SQL

[12] Christian Soutou, *De UML à SQL - Conception de bases de données*, Eyrolles,2002 – BU : 005.72 SOU

[13] F. Brouard, C. Soutou , *SQL (Synthèse de cours et exercices corrigés)*. Pearson Education 2005 – BU : 005.72 SQL

[14] Christian Soutou, *SQL Pour Oracle (avec exercices corrigés)*, Eyrolles, 2005 –BU 005.72 SOU

[15] Nicolas Larousse, Création de bases de données, Coll. Synthex, Pearson Education, 2006

Chapitre 2 : SYSTEMES D'INFORMATION HOSPITALIER

[1] Catherine Grasseler, Le Système d'information hospitalier entre culture et usages ; les enjeux de la formation des professionnnels de santé,Université de Provence Aix-Marselle 1, 2010-2011.

[2] Staccini Pascal, le Système d'information hospitalier, univérsité Nice-Sophia Antipolis, 2006-2007.

[3] émilie guiral ,« les systèmes d'information hospitaliers : histoire, enjeux et difficultés rencontres, devenir et lien avec la médecine de ville » thèse doctorat en pharmacie,septembre 2014 université toulouse iii paul sabatier, faculté des sciences pharmaceutiques, p : 51-54.

[4] F.KOHLER, Système d'information hospitalier, Université Henri Poincaré 03

[5] Alexis Gardan, « L'informatisation du dossier patient au centre Hospitalier de la Ferte- Bernard » : Les enjeux de la construction d'un hopital numerique. EHESP .Décembre 2015

[6] Cheick Oumar Bagayoko « Mise en place d'un Système d'information hospitalier en Afrique » Thèse doctorat , Universite Meditarranée Aix-Marseille 2, 04 octobre 2010.

[7] Gonnetan Claire. Avantages et incovénients du Dossier Médicale Informatisé dans le cadre de l'odondologie médico légale. 24 mars 2017 [16-32].

[8] Gabriel Piccoli, Informations Systèms for managers, Wiley, 2012,538p.

[9] La gestion des processus métier (BPM-Busniss Process Management System). Avril 2015.

[10] AsgaCs : Dossier Patient Informatisé, 26 décembre 2008.

[11] Thomas Bonthoux, Roman Lereun, Olivier Plassais. « Comprendre les problématiques du dossier patient informatisé et interopérable : du dossier papier au dossier informatisé, juin 2015

[12] Francoise Vendittelli, Bernard Hémery, Didier Lémery. « Quitter ou ne pas quitter son dossier papier ? Pour une informatisation du dossier médical » Réseau de santé Périnatal d'auvergne CHU de Clermont-Ferrand. 2010.

[13] MAHARRAR, Amina. La mise en place d'un système d'information formalisé dans les entreprises algériennes. Mémoire de Magister, Science de Gestion, TLEMCEN : Université Abou Bekr Belkaid de Tlemcen, FSECSG, 2014, p.9.

[14] DIFFALLAH Kamelia, SIFAOUI Fatma, système d'information hospitalier comme outil d'aide à la prise de décision, Mémoire du Master en science économique, option économie de la santé, l'université du Mouloud Mammeri TO, p, 74.

[15] DEGOULET, Patrice. Les Système d'information hospitalier. In: VENOT, Alain, BURGUN, Anito, QUANTIN, Catherine. Informatique médicale, e-santé, fondements et applications. Paris : Spinger-Verlag, 2013,p. 307.

[16] BOUAMRANE, Souad Fatima Zohra. Système d'Information Hospitalier : Admission et Planification des blocs opératoires. Mémoire de Magister en Informatique, ORAN : Université d'Oran, faculté des sciences, 2010, p. 16-17.

Chapitre III : Informatisation en Imagerie

[1] No PACS without HIS, De Valk J.P.J, Bijl K., Bakker AR, Towards New Hospital Information Systems, 1988

[2] Les standards en Imagerie Médicale, série documents d'initiation, 3-IHE : Integrating the Healthcare Enterprise, version 3, Joël Chabriais, GMSIH, 2004.

[3] Osman Ratib, Denis Hochtsrasser, Jean-Raoul Scherrer « Les réseaux de communication et d'archivage des images médicales », Information et Santé, volume 4, Springer-Verlag France, 1991

[4] www.assurancemaladie.sante.gouv.fr /actu/dmp.htm : relatif au Dossier Médical Patient et aux durées d'archivage

[5] www.afnor.fr : site relatif aux normes

[6] www.cybermed.jussieu.fr/Broussais.InforMed/LIVRES/TraitInfo/Fic/Chapitre13/ Chap13.html : Traitement de l'information médicale, Méthodes et applications hospitalières, Chapitre 13, L'imagerie médicale, Pat Degoulet et Marius Fieschi

[7] www.legifrance.gouv.fr : Site relatif au Code des Marchés Publics et au Code de la Santé

[8] Introduction aux réseaux d'images : Formation PACS UTC 2004, AGFA.

[9] Réseaux d'images, Support de formation CNEH 13, 14 et 15 décembre 2005 : Yves Martin Bouyer (CIMOP), Bernard Hervault (ETIAM), Martine Decouvelaere (Hôpitaux de Lyon), Pierre Duthil (Hôpitaux de Toulouse), Stéphane Pierrefitte (Hôpital Saint Anne).

[10] Picture Archiving and Communication System, Support de cours, Jean- François Lerallut, Département Ingénierie Biomédicale, Université de Technologies de Compiègne.

[11] PACS School, Support de formation, 26 et 27 Septembre 2005, CHU de Nancy.

Chapitre IV : DICOM

[1] Chabriais J , Gibaud B . « DICOM , le standard pour l'imagerie médicale ». EMC (Elsevier Masson SAS , Paris) ,Radiologie et imagerie médicale ; principes et technique-radioprotection, 35-120-A-10,2010.

[2] Oleg S. Pianykh " Digital Imaging and Communications in Medicine (DICOM); A Practical Introduction and Survival Guide", Department of Radiology, BIDM CHarvard Medical School. USA. ISBN 978-3-540-74570-9. DOI 10.1007/978-3-540-74571-6. Springer 2008.

[3] Eric PICEL , « comprendre le DICOM » , Support de cours, Université de Technologies de Compiègne, décembre 2005.
http://ultra.sdk.free.fr/docs/Image-Processing/Courses/TRAITEMENT%20NUMERIQUE%20D'IMAGES%20MEDICALES/formation%20dicom%202005.pdf

[4] Les standards en Imagerie Médicale, série documents d'initiation, 1-DICOM : Digital Image Communication in Medecine, version 1.0, Joël Chabriais, GMSIH, 2001.

[5] Les standards en Imagerie Médicale, série documents d'initiation, 2.2-HL7 : Health Level 7, version 3, Joël Chabriais, GMSIH, 2001.

[6] https://sti-biotechnologies-pedagogie.web.ac-grenoble.fr/content/fichiers-dicom-format-dcm-en-imagerie-medicale

Chapitre V : Compression des images médicales par ondelettes

[1] *J. TAQUET,* " Techniques avancées pour la compression d'images médicales ", Thèse de doctorat, Spécialité: Traitement du Signal et Télécommunications, Universié de Rennes 1, le 15 Décembre 2011.

[2] *J.J. Brault, D. Dougherty, "Les formats de compression d'image", Rapport de projet, Institut Universitaire de Technologie de Tours, Département Génie Électrique et Informatique Industrielle, 2004.*

[3] *P.BEUREPAIRE, "Compression d'Images Appliquée aux Angiographies Cardiaques: Aspects Algorithmiques, Evaluation de la Qualité Diagnostiques", Thèse de doctorat, Spécialité: Génie Biologique et Médical, école doctorale des sciences pour l'ingénieur, Lyon, 21 novembre 1997.*

[4] *T.TOTOZAFINY, "Compression d'images couleur pour application à la télésurveillance routière par transmission vidéo à très bas débit", Thèse de doctorat, Spécialité: Informatique, Université de Pau et des pays de l'adour, 3 juillet 2007.*

[5] *J. Ziv et A. Lempel. "A universal algorithm for data compression". IEEE Tran-sactions on Information Theory, vol. 23(3) : 337-343, 1977.*

[6] *M. Mekouar, " Compression d'images médicales par ondelettes et régions d'intérêt", Mémoire pour l'obtention de la maîtrise en technologie des systèmes, Université du Québec, Montréal, 12 juin 2001.*

[7] *BOUKLI HACENE I, " Compression des images médicales par ondelettes de secondes génération ", thèse doctorat en électronique biomédicale option : Imagerie Médicale, université de tlemcen. Septembre 2014*

[8] *T. Acharya,P-S. Tsai, "JPEG2000 Standard for Image Compression Concepts, Algorithms and VLSI Architectures", John Wiley & Sons, Inc, Canada, 2005*

[9] *T. Jonathan, "Techniques avancées pour la compression d'images médicales" , Thèse de Doctorat, université de rennes 1, soutenue à Rennes le 15 Décembre 2011*

[10] *M.LAHDIR, "Compression d'Images par Quantification Vectorielle en Sous bandes", Laboratoire d'instrumentation et d'études des phénomènes météorologiques (LIEPHM), Institut d'Electronique, université Moloud Mammerie de Tiziouzou, 2004.*

[11] *E.SJÖBLOM, "Compression of Medical Image Stacks using Wavelets and Zero Tree Coding", Master thesis, Division of Image Coding, Department of Electrical Engineering, Linköping University junry, 2002.*

[12] *J.SHAPIRO, "Embedded Image Coding using Zerotree of Wavelet Coefficients", IEEE trans. Signal processing. Vol. 41, pp. 3445-3462. Dec, 1993.*

[13] *A. K. MOORTHY, Z. WANG, and A. C. BOVIK, "Visual Perception and Quality assessment", Chapiter19 in Optical and digital image processing, Wiley, 2010.*

[14] *Z. WANG, Q. LI, "Information Content Weighting for Perceptual Image Quality Assessment", IEEE Transactions on Image Processing, Vol. 20, No. 5, pp 1185-1198, May 2011.*

[15] *L. QUART A "Une introduction (élémentaire) à la théorie des ondelettes " 22 novembre 2001. Institut de Mathématique Université de Mons-Hainaut. Belgique, 2001*

[16] *Y. Meyer. "Les ondelettes : algorithmes et applications." Armand Colin, 1992.*

[17] *D. L. Donoho and M. R. Duncan. "Digital curvelet transform: strategy, implementation and experiments". In Proc. Aero sense 2000, Wavelet Applications VII, volume 4056, pages 12-29. SPIE, 2000.*

[18] *D. A. Huffman. "A method for the construction of minimum-redundancy codes ". Proceedings of the IEEE, 40(9): 1098–1101, September 1952.*

Chapitre IV : cryptages et tatouages des images médicales par ondelettes

[1] *BACHAR Mohamed el Amine « Gestion des images médicales dans un centre hospitalier universitaire. Application au cryptage et tatouage des images médicales » ; Master en génie biomédical ; spécialité signaux et images en médecine, Université de Tlemcen. 24.06.2013*

[2] *J. M. M. RODRIGUES, "Transfert sécurisé d'images par Combinaison de techniques de Compression, cryptage et marquage ", Thèse de doctorat, Université Montpellier II, Octobre 2006.*

[3] *Bekkouche Souad « **Tatouage appliqué à l'Imagerie Médicale' » mémoire de magister en informatique ,Option:** Imagerie, Vision Artificielle et Robotique Médicale , département d'informatique ; faculté de sciences ; universite des sciences et de la technologie d'oran mohamed boudiaf, juin 2012*

[4] *I. J. Cox, M.L. Miller, A.L. McKellips, Watermarking as communication with side information, IEEE J. Selected Areas Communication. 16(4), 587-593, May 1998.*

[5] *E Koch, J Zhao, towards robust and hidden image copyright labeling, in: Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing June 20-22, Neos Marmaras, Greece, 1995*

[6] *C. REY and J. DUGELAY. Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images. Traitement du Signal, 18(4):283–295, 2001.*

[7] *I. Cox, M. Miller, and J. Bloom. Digital Watermarking Principles & Practices. Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.*

[8] *Bouderbala Ahmed. Implémentation d'un algorithme de tatouage Vidéo robuste dans Le domaine compressé. Thèse de Magister en électronique traitement de signal, Université Mentouri Ahmed Caustantine Algerie.2008.*

[9] *GaëL CHAREYRON. Tatouage d'image une approche couleu, Thèse de doctorat informatique, Université Jean Monnet Saint -Étienne, Décembre 2005.*

[10] *S.Bekkouche, A.Chouarfia . A new watermarking approach based on combination of reversible watermarking and CDMA in Spatial and DWT domain, proceedings of the 7th WSEAS International Conference on Multimedia Systems & Signal Processing, , Puerto Morelos, Mexico, January 29-31, 2011.*

[11] *EL HADJ MIMOUNE Khadîdja, MERABET Meriem ; « Etude de sécurité en base de données avec une application pour le contrôle d'accès ». Master en Informatique option système d'Information et de Connaissances (S.I.C) ; université de Tlemcen, 29 Septembre 2011.*