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

Université de Jijel
Faculté des Sciences et de la Technologie
Département d'Electronique

Mémoire de fin d'études pour l'obtention du Diplôme de

Master II en Electronique

Option : Electronique et Analyse des Systèmes

Thème :

Authentification d'Image Numérique basée sur le Contenu

Présenté par :

M^elle^ : BOUKEDJOUTA Meriem

M^elle^ : BOULARAOUI Warda

Encadré par :

Dr: *TALEB Ahcène*

Promotion : Juin 2015


بسم الله الرحمن الرحيم
وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا (85)
سورة الإسراء

Remerciements

La Louage est à Allah, *le Seigneur des mondes. Et que la prière et le salut soient sur celui qu'Allah a envoyé en miséricorde pour l'univers, ainsi que sur nos famille, ses compagnons jusqu'au Jour de la Rétribution.*

Nous voudrions remercier tout d'abord Allah, le tout puissant qui nous avons donné la force, la volonté et le courage pour accomplir ce modeste travail.

Nous tenaient à formuler nos gratitudes et nos profondes reconnaissances à l'égard de notre promoteur Mr : ***Taleb Ahcène*** *qui a supervisé ce travail de recherche. Ainsi que ses conseils judicieux tant lors de l'écriture de ce mémoire. Ses connaissances et ses jugements m'ont permis d'acquérir des compétences essentielles en recherche.*

Nous adressons également nos remerciements, à tous ***nos enseignants*** *et une remerciement spéciale à Mr :* ***Ammar Soukkou****, qui nous ont donné les bases de la science et sans oublier d'exprimer nos remerciements au* ***Chef du Département*** *d'Electronique.*

Mes remerciements aux ***membres du jury*** *qui m'ont fait l'honneur d'accepter de lire et de juger ce mémoire.*

Nous remercions l'ensemble des ***collègues et amis*** *qui nous ont aidé et supporté durant ces dernières années. Et nous remercions aussi toute personne ayant participée de près ou de loin.*

Enfin, ce travail ne voudrait rien dire sans remercier ***nos parents*** *pour leur dévouement incommensurable, qui nous ont toujours soutenue et poussée à donner le meilleur de moi-même ; pour l'éducation qu'ils m'ont offert et pour leur appui inconditionnel tout au long de ma vie.*

Dédicaces

C'est avec un grand amour, je dédie ce modeste travail de fin d'étude Aux être les plus chers.

Ma chère mère et Mon cher père

A mes frères et mes sœurs,

A mon oncle,
A toute ma famille,

A mes collegues,
A tous mes amis,

A mon binôme et à toute sa famille,

A tous mes enseignants depuis le primaire jusqu'à maintenant,

A tous ceux qui, de près ou de loin n'ont cessé de m'apporter leur soutien durant mes études,

Warda

Dédicaces

C'est avec un grand amour, je dédie ce modeste travail de fin d'étude Aux être les plus chers.

Ma chère mère et Mon cher père

A mon frère Faress,

A mes sœurs Halla, Khalida, Loubna, Sara,

A Aicha et Kamel,
A toute ma famille,

A tous mes amis,
A mes collegues,

A mon binôme et à toute sa famille,

A tous mes enseignants depuis le primaire jusqu'à maintenant,

Meriem

Table des matières

Chapitre I
Généralités sur La protection de données numériques

Chapitre II
Etat de l'art sur l'authentification des images

Chapitre III

Détection et extraction de caractéristiques

Chapitre IV

Résultats et simulation

Liste des figures

Liste des tableaux

Liste des abréviations

JPEG:	Joint Photographic Experts Group
LSB :	Least significant Bit
DCT :	Transformée Cosinus Discrète
DWT:	Discret wavelet Transform
BRIEF:	Binary Robust Independent Elementary Features
FAST:	Fast from Accelerated Segment Test
SIFT:	Scale Invariant Features Transform
MSER:	Maximally Stable Extremal Regions
SURF:	Speeded-Up Robust Features
BRISK:	Binary Robust Invariant Scalable Keypoints
FREAK:	Fast Retina Keypoint

Introduction générale

Introduction générale

Les besoins technologiques de la population mondiale révèlent une très forte croissance dans toutes les régions du monde. Une partie de cette technologie c'est les outils de traitement d'images. Ces développements soulèvent un nombre important de problèmes : la distribution illégale, la duplication, la falsification de supports numériques (*images, vidéo, audio ou texte*). Les auteurs et les fournisseurs de données multimédias sont réticents à permettre la distribution de leurs données dans un environnement réseau, parce qu'ils craignent la duplication et la diffusion sans restriction du matériel protégé, par exemple par les droits d'auteurs **[1]**.

Il' y a quelques années, l'information que nous échangeons a changé de forme de représentation. Aujourd'hui, l'utilisation d'images, sons, séquences vidéo fait généralement intervenir leur représentation digitale, c'est notamment le cas lorsque ces media sont véhiculés sur l'internet. Les avantages obtenus sont considérables, enter autre, cela permet une manipulation plus sure, un stockage moins coûteux, une transmission plus rapide et une indexation plus facile de l'information. Cependant avec l'apparition de ces nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes efficaces concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les copier, les modifier et enfin les diffuser illégalement, sans qu'elles perdent de leur qualité **[2]**.

Une des méthodes envisageable est d'insérer dans un document image une marque semi-fragile. L'existence et donc l'extraction de celle-ci permet d'attester de l'authenticité du contenu.

L'autre approche automatisée est d'extraire les caractéristiques de deux images de la même scène prise éventuellement sous des conditions différente d'éclairage, d'angle de prise de vue, etc. Dans ce cas, on ne cherche pas que les images soient identiques, mais présentant le même contenu. On va se baser sur la détection et l'extraction de caractéristiques de deux images où l'une est une version manipulée de l'autre, puis tester leur correspondance. Ce qui intéresse dans ce cas est que le contenu soit conforme à l'état original.

Ce mémoire est décomposé de quatre chapitres organisé de la façon suivante :

Au cours du premier chapitre, on présentera des généralités sur les techniques de protection des données.

Le deuxième chapitre sera consacré à un panorama des différentes méthodes permettant d'assurer une authentification adapté aux images numériques.

Dans le troisième chapitre, nous allons présenter une revue de différentes méthodes de détection et d'extraction les caractéristiques d'une image numérique.

Le quatrième chapitre rassemblera les différentes étapes d'algorithme utilisé et la méthodologie suivie pour la détection, l'extraction et la mesure de correspondance (*matching*) du contenu de deux images numérique, ainsi que les résultats de l'implémentation et discussion.

Enfin, nous allons terminer par une conclusion générale qui résumera les principaux résultats obtenus et les interprétations de celles-ci, suivie par des perspectives pour de futurs travaux.

Chapitre I

Généralités sur La protection de données numériques

I.1. Introduction

I.2. Sécurité des données

I.3. Les mécanismes de protection

I.4. La robustesse

I.5. Quelques attaques

I.7. Conclusion

Résumé :

L'objectif de ce chapitre est d'exposer les différents services de sécurité engagés dans la protection de données numériques ainsi que les mécanismes permettant de les assurer.

I.1. Introduction

De nos jours, l'information représente un réel enjeu stratégique et économique et de ce fait, qui contrôle l'information détient énormément de pouvoir. Par conséquent, les techniques de protection des media numériques représentent des enjeux économiques, stratégiques et juridiques considérables. Dans un contexte où les échanges d'informations dématérialisées se développent. Il est indispensable de pouvoir bénéficier de systèmes sécurisés, afin de protéger les données à caractère personnel ou confidentiel, ou pour assurer la sécurité de la transaction financière et commerciale **[3]**.

En effet, l'utilisation d'un réseau de communication expose les échanges de médias numérisés à certains risques, qui nécessitent l'existence de mesures de sécurité adéquates. Il est donc nécessaire d'avoir accès à des outils techniques, permettant une protection efficace de ces dernières contre les manipulations arbitraires. Cette nécessité a conduit de nombreux chercheurs à se pencher sur le problème de la sécurisation des données numériques face au piratage et à la contrefaçon, afin notamment de faciliter le développement économique des techniques de communication audiovisuelle en réseaux.

La cryptographie a très longtemps été le seul moyen efficace pour répondre à ces exigences. Cette technologie est ainsi reconnue comme étant un outil essentiel de la sécurité et de la confiance dans les communications électroniques.

Les nouvelles technologies de dissimulation de données apparaissent comme étant une alternative pouvant s'avérer efficace et complémentaire aux approches de type cryptographique. Elles vont être amenées à jouer un rôle croissant en matière de protection contre la fraude informatique, de sécurité des données, de protection de la confidentialité des correspondances, de protection du secret professionnel, et du commerce électronique **[4]**.

I.2. Sécurité des données

La protection des données numériques concerne principalement les quatre aspects suivants:

- La confidentialité
- L'intégrité
- L'authentification
- La non- répudiation

Ces services sont assurés par divers mécanismes de sécurité plus ou moins complexes, que nous exposerons en détail, plus loin dans ce chapitre.

Comme nous le verrons, ces mécanismes sont traditionnellement de nature cryptographique, mais la dissimulation de données, offre aussi une alternative intéressante, particulièrement pour les données de type images auxquelles nous nous intéressons particulièrement **[5]**.

I.2.1. La confidentialité

Il s'agit de garantir le secret du document numérique transmis ou archivé. Ce service de sécurité consiste à s'assurer que seules les personnes autorisées peuvent prendre connaissance des données échangées.

I.2.2. L'intégrité

Il s'agit de garantir qu'un message ou un document électronique n'a pas été altéré accidentellement ou frauduleusement pendant son transfert sur le canal de communication. Il est particulièrement important que, dans toute négociation ou accord contractuel, on puisse vérifier qu'aucune modification du document électronique n'a été faite.

Pour assurer l'intégrité, on peut utiliser le chiffrement sous sa forme symétrique ou asymétrique, la signature numérique ou encore les codes d'authentification de messages. L'intégrité est très liée à l'authentification de l'origine des données, et les deux services sont souvent fournis conjointement.

On distingue deux types d'intégrité :

- **L'intégrité en mode non connecté :** permet de détecter des modifications sur un datagramme individuel, mais pas sur l'ordre des datagrammes.

- **L'intégrité en mode connecté :** permet en plus de détecter la perte de paquets ou leur réordonnancèrent **[5]**.

I.2.3. L'authentification

C'est bien sur l'application qui nous intéresse le plus dans ce travail. Le but de cette application est d'apporter la preuve que le contenu d'un document n'a pas été modifié. Une façon d'agir est d'insérer dans un document image une marque qui puisse authentifier le document. La détection et l'extraction de cette marque fournie une assurance que le contenu de ce document n'a pas été modifié depuis l'insertion de celle-ci.

Dans certains cas on préfère assurer une authentification stricte ou exacte (*intégrité des données*). Pour cela, on utilise des marquages fragiles qui deviennent non détectables dès qu'une valeur (*un bit*) des données change dans le document. Ce type d'application est très demandé pour les images médicales. Mais dans d'autre cas, on voudrait assurer une authentification sélective du contenu. Pour cela, on utilise des marquages semi-fragiles qui tolèrent certaines modifications dites acceptables (*comme la compression*) et deviennent non détectables dès qu'il y a présence de modifications malicieuses portant atteinte à l'interprétation du contenu du document. Dans ce cas, le marquage est volontairement vulnérable aux attaques dans le but de détecter une manipulation éventuelle du document. C'est l'absence de la marque qui prouvera que le contenu est suspect. Plusieurs utilisations peuvent être envisagées :

- Justifier auprès d'un tribunal l'authenticité de documents tels que des enregistrements de caméras de surveillance (*authentification du contenu*).
- Le propriétaire d'une œuvre cherche à vérifier si le contenu de son œuvre a été modifié. Ce scénario se produit fréquemment dans le domaine militaire ou il faut sans cesse vérifie que les informations reçue par des alliés n'ont pas été altérées par un adversaire.
- L'utilisateur cherchera à s'assurer si l'œuvre qu'il s'est procuré est bien la version originale authentique et non pas une simple copie ou une version manipulée **[6]**.

I.2.4. La non-répudiation

Il s'agit de se protéger contre la contestation d'envoi ou de réception d'un message ou d'un document électronique lors d'une transaction. En d'autres termes, il s'agit de garantir

que les partenaires d'une transaction ne puissent nier avoir envoyé ou reçu le document en question [5].

I.3. Les mécanismes de protection

La cryptographie, la stéganographie et le tatouage sont des techniques destinées à transmettre une information à caractère confidentiel lors de la transmission. Elles répondent toutes les trois à des problèmes de sécurité.

La cryptographie et la stéganographie ont été utilisées depuis longtemps à des fins militaire. Elles font partie des sciences du secret. Le tatouage de documents est un domaine beaucoup plus récent qui s'apparente à la stéganographie [3].

I.3.1. La cryptographie

La cryptographie consiste à transformer un message pour qu'il devienne illisible ou indéchiffrable. Seule la connaissance d'une clef et du moyen de cryptage peut permettre de décoder le message afin de le rendre lisible. Cette technique permet de protéger le document pendant sa transmission. Mais, une fois le document décrypté, il ne présente plus aucune protection. Un des premiers procédés utilisés est celui par substitution, le message est crypté en substituant chaque lettre par une autre d'un alphabet décalé. La clef représentait le nombre de lettres de décalage [7].

I.3.1.1. Chiffrement symétrique

Le chiffrement symétrique consiste en l'échange d'une clef secrète entre les deux parties en communication (*Alice et Bob*). Lorsqu'Alice souhaite envoyer un message à Bob, elle crypte son message avec la clef secrète, et elle envoie le message à Bob. Une fois que ce dernier a reçu le message, il ne lui reste qu'à décoder le message grâce à cette même clef secret.

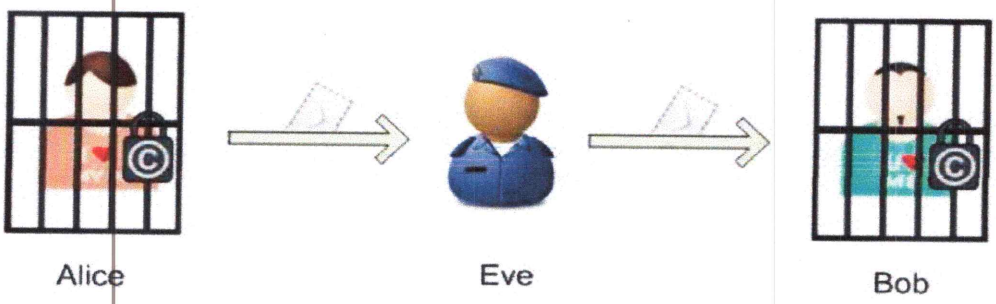

***Figure I.1** : Problème classique de communication secrète* [7].

Si, lors de la phase d'échange de massage, Eve en intercepte un, elle ne pourra le décoder son l'aide de la clef secrète.

Evidemment, le handicap majeur de cette méthode est que la clef secrète doit le rester! Le problème se situe donc dans l'échange de cette clef entre Alice et Bob. Pour pallier à ce problème, d'autre procédés sont employés pour l'échange de clef secrète, c'est notamment l'utilisation qui est faite de la cryptographie à clef publique, et du chiffrement asymétrique **[8]**.

I.3.1.2. Chiffrement asymétrique.

Le chiffrement asymétrique repose quant à lui sur un système à double clef : une clef publique et une clef privée. Chacune des deux parties (*Alice et Bob*) possède donc une paire de clefs, une publique qu'elle publie, et une secrète qu'elle conserve précieusement. Ces deux clefs peuvent servir à coder comme à décoder. Dans notre cas, le message est crypté à l'aide de la clef publique et décodé à l'aide de la clef privée **[8]**.

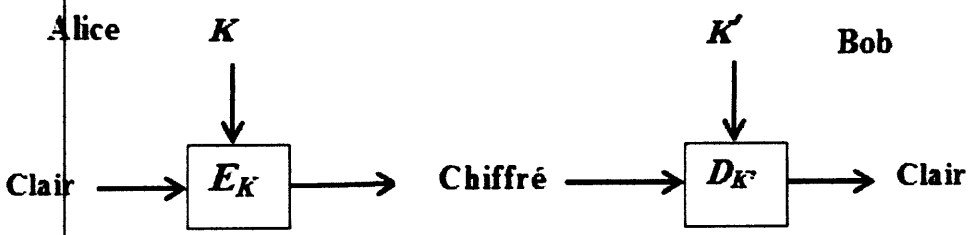

Figure I.2: *Schéma de chiffrement.*

I.3.1.3. Domaine d'utilisation de la cryptographie

De nos jours la cryptographie est une science étroitement liée aux systèmes de communication. Elle permet de multiples applications **[7]** :

1. Garantir l'intégrité des données : une fonction de hachage peut être associée au document, elle assure qu'il est inchangé.
2. Assurer la confidentialité des données : seule des entités autorisées peuvent accéder aux données.
3. Permettre l'authentification des entités en communication : seule des entités autorisées peuvent accéder aux données.

4. Veiller à la non-répudiation de l'origine : l'information qui a été émise par une source ne peut être réfutée.

Le chiffrement de messages consiste à transformer une information à l'aide d'une convention secrète. La fonction de transformation constitue l'algorithme cryptographique dont le secret réside dans des paramètres appelés clés. Lorsque l'on déchiffre le message, en connaissant ses clés on réalise l'opération inverse.

I.3.2. La stéganographie

I.3.2.1. Définitions

Le mot stéganographie (*en anglais: steganography ou data hiding*) tire son origine d'une étymologie grecque : steganos, signifiant caché et graphos, signifiant écriture, ce qui donne, littéralement, " *écriture cachée* ". La stéganographie est donc l'art de dissimuler un message secret au sein de données d'apparence anodine de façon à ce que sa présence soit imperceptible [10].

Durant l'ère médiévale, des pochoirs étaient superposés sur les messages pour pouvoir révéler les différents mots formant le message caché. En 1586, la police secrète de la couronne britannique a identifié des lettres qui contenaient un message dissimulé décrivant un complot contre la reine Elizabeth d'Angleterre. Le complot a pu être arrêté lorsque la police a inséré à l'une des lettres un message demandant les noms et les qualités des six personnes qui devaient accomplir le crime. A cette époque, certains postiers anglais avaient pour tâche d'enlever les formules de politesse des lettres ou encore de reformuler les télégrammes afin de détruire d'éventuels messages cachés. Durant la seconde guerre mondiale, la stéganographie était majoritairement représentée par l'utilisation d'encre invisible [11]. La stéganographie moderne utilisée aussi comme réceptacle des documents numériques comme le texte, les images ou encore le son ou la vidéo.

Pour résumer le problème de façons plus académique, utilisons une présentation proche de celle utilisée en cryptographie. Alice et Bob ont été arrêtés et emprisonnés. Ils désirent se communiquer des informations afin d'organiser leur défense lors du procès. Ils sont autorisés à communiquer quasi librement avec la restriction que tous les messages seront lus par les responsables de la prison. Ils utiliseront la stéganographie pour communiquer leur plan.

Pour pouvoir communiquer de façon secrète, il faut d'abord pouvoir communiquer tout simplement. On attachera à des messages anodins, un message secret. Afin de décoder ce message, le correspondant doit connaître un secret et/ou la technique pour déchiffrer et extraire ce message. Il est évident que ce message caché peut être lui-même codé et/ou signé en utilisant des méthodes cryptographiques. La stéganographie n'étant plus alors que la dernière étape de leur encodage. Celle-ci pouvant être destinée à cacher l'usage même de la cryptographie [12].

I.3.2.2. Domaine d'utilisation

De nombreux usages peuvent exister dans des domaines très variés [13] mais tous sensibles.

- Communiquer en toute liberté même dans des conditions de censure et de surveillance.
- Protéger ses communications privées là où l'utilisation de la cryptographie n'est normalement pas permise ou soulèverait des suspicions.
- Elle peut servir à publier des informations ouvertement mais à l'insu de tous, des informations pourront ensuite être révélées et dont l'antériorité sera incontestable et vérifiable par tous.
- Elle peut être utilisée pour la dissimulation des données hautement confidentielles ou interdites au grand public, par exemple dans le domaine militaire ou médical.
- Elle peut être utilisée en espionnage industriel : toute entreprise a des secrets à protéger (*par exemple une formule chimique d'un nouveau produit, etc.*)
- la stéganographie peut être aussi utilisée à de mauvaises fins : un hacker peut tenter de dissimuler n'importe quel code malveillant dans un media amovible ou encore de dissimuler des fichiers MP3 propriétaires sur un serveur donné.

I.3.2.3. Mode d'opération

Afin de récupérer le message secret, le correspondant doit connaître un secret et/ou la technique pour extraire ce message du stégo-médium. Il est évident que ce message caché peut être lui-même codé et/ou signé en utilisant des méthodes cryptographiques, la stéganographie n'étant plus, alors, que la dernière étape d'encodage [4].

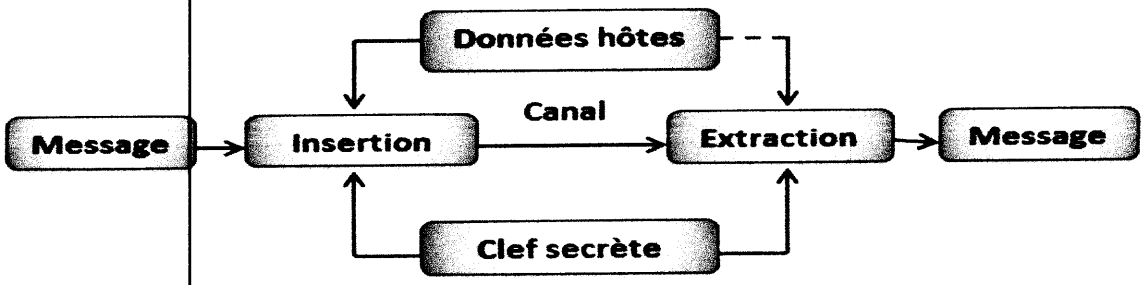

Figure I.3 : *Schéma générique de la stéganographie.*

I.3.2.4. Exemple de dissimulation d'images numériques

Nous prenons l'exemple des images en niveaux de gris. Supposant que chaque pixel de l'image serait un nombre entre 0 et 1 où le niveau de gris 0 correspond au noir, et le 1 au blanc. Le niveau 0.5 sera un gris moyen, un pixel proche de 0 serait gris foncé, un pixel proche de 1 serait gris clair. L'image sera quant à elle, représentée par une matrice de pixels de n lignes et m colonnes (nxm). Prenons comme exemple une matrice de 3 lignes et 4 colonnes (*les pixels de l'image correspondante sont fortement grossis*) :

$$M=\begin{pmatrix} 0.2 & 0.5 & 1 & 0 \\ 0 & 0.25 & 0.75 & 0.5 \\ 0.25 & 1 & 0.4 & 0.85 \end{pmatrix}$$

Matrice

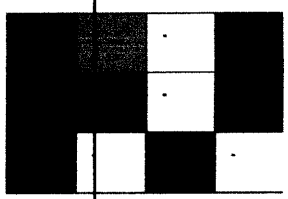

Image correspondante

Mathématiquement, on peut décrire le camouflage d'une image "*sous*" une autre par une combinaison linéaire des deux matrices *nxm* correspondantes si les dimensions des deux matrices sont identiques et si A est la matrice de l'image "*camouflant*" et B la matrice de l'image camouflée, alors on peut calculer la matrice de l'image combinée par :

$$C = A + \left(\frac{1}{K}\right) * B \qquad \textbf{(I.1)}$$

Ou K est un nombre bien choisi. L'image B (*qui sera peut-être légèrement différente de l'originale B*) sera trouvée par la formule :

$$B' = K(C - A) \quad \textbf{(I.2)}$$

❖ **Remarque**

Les pixels très proches de 1 dans l'image A peuvent poser problème. En effet, en leur additionnant un certain nombre, ils risquent de dépasser 1.ils seront alors tronqués à 1. Cela a pour conséquence que, une fois l'image C déchiffrée, l'image B' sera légèrement altérée par rapport à B (*voir l'exemple numérique ci-dessous*) **[7]**.

$$C=\begin{pmatrix}0.51 & 0.47 & 0.30 & 0.43\\ 0.12 & 0.95 & 0.41 & 0.47\\ 0.22 & 0.98 & 0.53 & 0.65\end{pmatrix}+\frac{1}{10}\begin{pmatrix}0.21 & 0.34 & 0.21 & 0.21\\ 0.54 & 0.43 & 0.76 & 0.33\\ 0.46 & 0.44 & 0.66 & 0.54\end{pmatrix}=\begin{pmatrix}0.531 & 0.504 & 0.321 & 0.451\\ 0.174 & 0.993 & 0.486 & 0.503\\ 0.266 & 1 & 0.596 & 0.704\end{pmatrix}$$

A **B** **C**

$$B'=10\begin{pmatrix}0.531 & 0.504 & 0.321 & 0.451\\ 0.174 & 0.993 & 0.486 & 0.503\\ 0.266 & 1 & 0.596 & 0.704\end{pmatrix}-10\begin{pmatrix}0.51 & 0.47 & 0.30 & 0.43\\ 0.12 & 0.95 & 0.41 & 0.47\\ 0.22 & 0.98 & 0.53 & 0.65\end{pmatrix}=\begin{pmatrix}0.21 & 0.34 & 0.21 & 0.21\\ 0.54 & 0.43 & 0.76 & 0.33\\ 0.46 & 0.20 & 0.66 & 0.524\end{pmatrix}$$

C **A** **B'**

I.3.3. Le tatouage

Définition : Le principe général d'une méthode de tatouage d'une donnée numérique consiste à transmettre un message en même temps que la donnée, en modifiant directement la valeur des échantillons de cette donnée. Cette définition est intéressante, car elle recouvre toutes les méthodes de tatouages, quelles que soient leurs applications. On remarque aussi que ces méthodes sont voisines de la discipline de la stéganographie **[1]**. Appliquée au tatouage d'image pour la protection du copyright et avec le vocabulaire introduit ci-dessus, cette définition peut-être reformulée de la manière suivante :

I.3.3.1. Principe du tatouage

Le schéma de tatouage d'image se décompose en deux opérations distinctes illustrées sur la figure I.5.

- **La phase d'insertion**: elle consiste à introduire une marque dans l'image en vue d'identifier son propriétaire (*le nom de l'auteur ou de l'entreprise par exemple*). Cette insertion peut se faire dans le domaine spatial ou dans le domaine transformé (*transformée de Fourier, en cosinus discrète, en ondelettes ...*)
- **La phase de détection**: elle permet de retrouver la marque ou la signature insérée. Cette étape est la plus souvent effectuée en aveugle, c'est à dire sans utiliser l'image

originale, (*utiliser l'image originale donnerait un schéma plus lourd et pourrait poser des problèmes de sécurité*). Entre l'insertion et la détection, l'image marquée peut subir des modifications licites ou illicites.

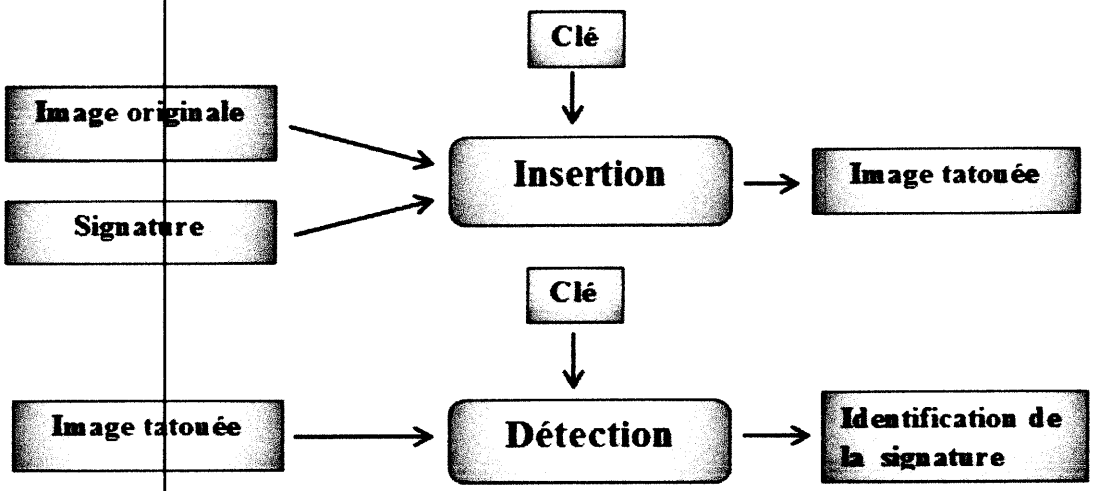

***Figure I.4** : Insertion et détection pour le tatouage d'image.*

I.3.3.2. Quelques applications du tatouage

Le tatouage numérique est considéré depuis quelques années comme une solution pour de nombreuses applications telles que la protection des droits d'auteur, l'intégrité des données multimédias, la prévention de la redistribution non autorisée, l'indexation et l'authentification du contenu. Dans ce qui suit, nous donnons un bref aperçu sur ces différentes applications.

- **Le tatouage et le problème du doit d'auteurs**

La première application envisagée pour le tatouage de document est la protection des droits d'auteur. Le tatouage offre une alternative intéressante à la cryptographie car il permet de protéger l'image même lorsque celle-ci est diffusée.

Le but du tatouage consiste ici en l'insertion d'une signature numérique qui atteste de l'identité du dépositaire de l'image. Cette signature ne doit être connue que de la personne ou de l'organisme qui a tatoué l'image. Elle dépend donc d'une clef secrète qui permet l'insertion de sa signature.

Pour une application du copyright, la signature ne doit pas obligatoirement porter une information conséquente, car la détection de la signature peut elle-même attester l'appartenance de la signature **[2]**.

- **l'authentification des documents numériques**

L'information insérée au sein de l'image permet de certifier qu'une image n'a pas été modifiée **[14]**. On entre ici dans une problématique de contrôle d'intégrité des documents. Dans ce cas précis, la signature ajoutée est dite fragile (*on parlera en anglais de "fragile watermarking"*). Elle doit être détectée tant que l'image n'a pas été manipulée **[15]**. Le tatouage fragile est "*évolué*" lorsque la dégradation provoquée par la compression, la transformation géométrique ou bien encore le filtrage de l'image n'altère pas le tatouage, mais que l'ajout ou l'effacement de l'objet dans l'image est détecté.

- **l'indexation des images**

L'indexation des images consiste à classer de manière automatique des images selon leur contenu, en facilitant ainsi la recherche dans la base de données. Le tatouage des images est aussi utilisé dans l'indexation. Il permet d'insérer une information décrivant le contenu de l'image ou bien un pointeur renvoyant vers une description plus complète **[16]**.

I.4. La robustesse

Il faut nécessairement faire un compromis entre le niveau de robustesse et la fonctionnalité du marquage. Le tatouage dédié à la protection des droits d'auteurs doit être aussi robuste que possible car la signature permet dans ce cas l'attester la propriété d'une image **[9]**.

La robustesse du tatouage dédiée à l'authentification de document doit être contrôlée : la marque doit pouvoir révéler une manipulation de l'image mais peut demeurer insensible aux traitements classiques " *innocent* " comme le filtrage ou la compression. Dans le cas du tatouage pour l'indexation de documents, la priorité doit être accordée à la quantité d'information insérée qui doit être maximale. La robustesse de la signature n'est pas une charge prépondérante, bien que selon les cas la marque doit survivre à des conversions analogiques numériques ou encore à des transformations géométriques simples (*rotation, translation*).

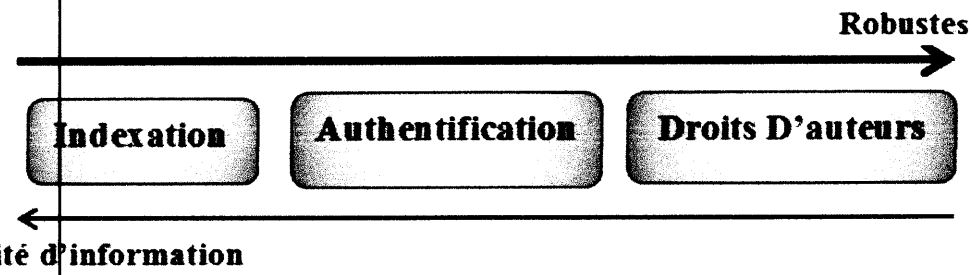

Figure I.5: *Robustesse versus Quantité d'information.*

I.5. Les attaques

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors de son extraction. Parmi ces types d'attaques citons.

1. Les attaques classiques

Les attaques classiques peuvent être simplement réalisées par un utilisateur de bonne foi lors de manipulations, ou par des utilisateurs malveillants. Parmi ces attaques nous retrouvons **[16]** :

- L'addition de bruit.
- Le filtrage.
- La compression avec pertes essentiellement JPEG.
- La conversion analogique / numérique.
- L'attaque "copier/coller" dans une image.

2. Les crackers

C'est l'ensemble des attaques qui perturbe et désynchronise l'image et rende la marque très difficile à détecter sans recourir à l'image originale. On cite les attaques géométriques dans lesquelles les images subissent des translations, des rotations ou des changements d'échelle. Les attaques de synchronisation empêchent de détecter des locations de marque c'est-à-dire que, le détecteur de la marque ne la retrouve pas aux endroits attendus et conclu son absence **[16,1]**.

3. La signature multiple

La présence de plusieurs signatures sur l'image conduit à une ambiguïté dans la détection du propriétaire de l'image. Considérons l'exemple suivant : Alice a une image I, elle

la marque avec une signature S et génère ainsi l'image Iw qu'elle rend publique. Bob marque à son tour l'image Iw avec une signature S' et obtient ainsi I'w. Dans ce cas, Alice et Bob peuvent réclamer la paternité de cette image. Si Alice possède l'image Iw, elle peut montrer que cette image contient sa marque alors qu'elle ne contient pas la marque de Bob. Ce dernier par contre ne possède aucune image qui ne contient pas la marque d'Alice, à condition que le tatouage d'Alice soit robuste [1].

I.6. Comparatif des différentes techniques

I.6.1. Cryptographie vs stéganographie

- La stéganographie aborde la protection des données par une approche différente de celle de la cryptographie. Comme dans le cas de la cryptographie, la technique permet d'échanger des messages avec un correspondant sans que des personnes non autorisées ne puissent en prendre connaissance. Mais alors qu'avec la cryptographie, la sécurité repose sur le fait que le message transmis est incompréhensible, en matière de stéganographie, la sécurité repose sur la remise en question même de l'existence du message secret.
- La cryptographie protège les données numériques durant leur transmission entre un émetteur et un récepteur. Après réception et déchiffrement, les données sont identiques aux données d'origine mais elles ne sont plus protégées. Donc le document peut être facilement recopié et redistribué. Avec la stéganographie le message secret reste protégé même après réception.
- Une autre différence très importante entre la cryptographie et la stéganographie se situe au niveau des attaques qui peuvent avoir lieu contre ces techniques. En cryptographie, l'ennemi va tenter de déchiffrer le message, alors qu'en stéganographie l'ennemi va tenter de découvrir le médium de couverture [4].

I.6.2. Stéganographie vs marquage numérique

- Dans le cas de la stéganographie, on cherche à cacher une quantité très importante de données qui peut aller jusqu'à dissimuler une image dans une autre image.
- Dans le cas du marquage numérique, on cherche juste à marquer une image en dissimulant une quantité limitée d'informations qui a pour but par exemple de démontrer l'intégrité du document ou encore de protéger les droits d'auteurs. Souvent, on se limite à la dissimulation d'un seul bit: image marquée/non marquée.

- Dans la stéganographie, l'existence du message caché doit rester secrète, alors que pour le marquage numérique, seul le message doit rester caché mais son existence, tant qu'on ne peut pas le supprimer ou le modifier, peut être connue. En fait, on peut considérer que le marquage numérique est une sous discipline de la stéganographie.
- En matière d'attaques, en stéganographie, le pirate va chercher à lire les données dissimulées dans le document, tandis que dans le cas d'un document marqué, l'attaquant va chercher à *"laver"* le document de toute signature possible.

Enfin, la cryptographie, la stéganographie, et le marquage numérique sont trois disciplines très proches les unes des autres puisque toutes les trois consistent à protéger une information à caractère sensible. L'approche de dissimulation d'informations dans des données hôtes en le laissant accessible est très intéressante, car il peut être accessible et protégé [4].

I.7. Conclusion

Au cours de ce chapitre, on a vu que l'information a toujours constitué une denrée prisée. Par conséquent, il faut savoir l'acquérir, vérifier la provenance et l'intégrité, et pouvoir la protéger.

Avec l'évolution des technologies et des connaissances, les réponses à chacune de ces préoccupations ont évolué. De nouvelles défenses ont contré de nouvelles attaques qui s'opposaient elles-mêmes à d'anciennes défenses. Nous avons présenté les objectifs de dissimulation d'information. Selon les attentes, les contraintes d'imperceptibilité, de capacité et de robustesse varient. Cependant, comme ces besoins sont à l'encontre les uns des autres, un compromis est toujours nécessaire.

Chapitre II

Etat de l'art sur l'authentification des images

II.1. Introduction

II.2. L'authentification

II.3. Revue des méthodes existantes

II.4. Les types d'authentification

II.5. Les attaques contre les systèmes d'authentification

II.6. Conclusion

Résumé :

L'objectif de ce chapitre est de passer en revu les différentes méthodes et techniques permettant d'attester que le contenu d'une image numérique n'a pu être modifié.

II.1. Introduction

Dans ce chapitre, nous nous concentrerons sur la vérification de l'authenticité d'une image numérique dont le contenu est d'une grande importance, comme les pièces à conviction dans un procès, les images militaires ou d'espionnage, etc. Donc, pour des applications dont nous devons être certains que des travaux n'ont pas été altérés. Il y a donc nécessité de vérification ou d'authentification de l'intégrité de contenus. Plus précisément, nous nous intéresserons aux méthodes qui nous permettent de répondre aux questions :

- Le travail a-t-il été changé de façon quelconque ?
- Le travail a-t-il été considérablement altéré ?
- Quelles parties du travail ont été altérées ?

Nous allons passer en revue des méthodes capable de répondre au moins a l'une des question si ce n'est pas a toutes. Nous allons avant tous donner quelques définitions des différents types d'authentification.

II.2. L'authentification

L'authentification 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. Cette définition est en principe applicable à tout type de documents numériques, néanmoins, dans la pratique elle s'avère être beaucoup trop stricte et inadaptée pour les documents de type image. Le problème de l'authentification 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 (*modification de la légende, disparition d'un visage, etc.*) Dans le but d'assurer un service d'authentification approprié aux images, il est donc primordial de distinguer les manipulations malveillantes 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, etc.) réalisés par des fournisseurs de contenu ou les utilisateurs eux-mêmes. Malheureusement cette distinction n'est pas toujours aisée d'un point de vue informatique et dépend en partie du type d'image et de son utilisation **[17]**.

En effet, selon l'aspect pratique, on peut souhaiter soit détecter tout type de modifications, soit un ensemble donné de transformations (*interdites*). On peut par exemple autoriser certains taux de compression, des changements d'échelle, etc.

Dans le premier cas, on utilisera des techniques de marquage fragile où le marquage disparaît à la moindre manipulation, et dans le deuxième des méthodes de marquage semi-fragile où le marquage résiste aux manipulations légitimes autorisées **[4]**.

II.2.1. Exemples classiques de manipulations malveillantes

Les messages véhiculés par les images ont un impact considérable. Toutes les images, y compris celles réalisées en toute innocence, ont la capacité d'être détournées de leur sens. Les manipulations, qui avant, nécessitaient des moyens coûteux sont désormais à la portée de tout le monde. Avec les progrès des techniques de traitement d'image et du tout numérique elles deviennent quasi indécelables. Dans ce contexte, un service d'intégrité d'image n'a bien évidement pas la prétention de véracité des évènements, mais de déceler des manipulations qui auraient pu y être apportées a posteriori, dans le but de détourner le contenu de l'image ou de rende impossible toute interprétation. Des exemples célèbres de manipulations intentionnelles d'images sont là pour attester de l'impact considérable que peuvent avoir ces dernières sur la société. La photographie truquée diffusée en 1995, dans l'émission de France 3, « *La marche du siècle* », où de jeunes " *beurs* " avaient été transformés à leur insu en redoubles intégristes, est un bel exemple de falsification d'image, ainsi qu'un véritable scandale journalistique qui a fait couler beaucoup d'encre à l'époque **[18]**. Les éléments ajoutés à la photographie créés de toutes pièces au moyen d'un logiciel de retouche à des fins de manipulation, exposèrent au grand jour le problème de la numérisation des images. Un autre exemple **[19]** qui a fait le tour du monde est celui de la photographie publiée à la une du quotidien autrichien " *Neue Kronen Zeitung* " en 1998, qui prétendait illustrer l'agressivité des manifestants opposés à l'entrée du parti de Haider dans le gouvernement autrichien. Par un truquage, on a recadré la photographie et raccourci la distance entre un manifestant et un policier apparemment directement frappé. En réalité, comme l'atteste l'image originale diffusée par la suite par l'agence Reuters, une distance de près de deux mètres séparait les deux protagonistes. Ainsi, l'utilisation de l'image ou la vidéo, élément à charge, sans être

couplée par des techniques d'authentification, devient plus que douteuse et critiquable à l'heure où les caméras de surveillance envahissent les villes, les stades et les routes.

II.2.2. Les applications de l'authentification d'images

Plusieurs champs d'application de l'authentification d'images peuvent être identifiés. Nous citons, quelques domaines potentiels :

- Archivage des images médicales : Les données d'authentification des patients peuvent être insérées au moment de la prise des images par l'hôpital afin de protéger leurs droits. Donc, en cas d'erreur médicale, ces images peuvent être utilisées par la justice.
- Enregistrement d'interrogatoires pour des enquêtes criminelles dans lesquelles la modification malveillante de certaines scènes (*par les enquêteurs, par exemple*) pourrait aboutir à des décisions juridiques graves si elle n'est pas détectée.
- Capture de scènes d'accidents à des fins d'assurance et des fins médicolégales : L'application d'une technique d'authentification d'images et de vidéos pourrait être utile dans la protection des droits des différentes parties, incluant la société d'assurance impliquée dans des accidents ou des catastrophes naturelles.
- Domaine militaire : L'authentification d'images permet aux services secrets militaires d'authentifier si les médias qu'ils ont reçus proviennent vraiment de leurs correspondants /ennemis et de vérifier si le contenu est vraiment original ou a été falsifié. Dans le cas où le contenu a été manipulé, un schéma d'authentification efficace pour ce type d'application, est celui qui permet, en plus, la localisation des modifications [17].

II.2.3. Caractéristiques d'un système d'authentification d'images

Dans cette section, on se propose de définir un schéma générique d'un système d'authentification d'image, dont différentes formulations ont été initialement proposées par Wu et Liu [20] et Lin et Chang [21]. Le schéma général d'un tel système est donné en figure II.1. Généralement, mais pas toujours, une même clef secrète disponible lors de la phase du marquage et de la phase d'authentification est utilisée pour générer une marque destinée à être insérée dans l'image hôte. L'image ainsi marquée est transférée à travers un canal de communication (*Internet, satellite, etc...*) ou sauvegardée dans une base de données. Pour authentifier une image marquée reçue ou extraite de la base, la même clef est utilisée pour extraire la marque aussi bien que pour générer la marque originale, puis les deux marques

sont comparées, La différence des deux marques, comparée à un seuil de tolérance, constitue la sortie du système, et atteste donc de l'authenticité ou de la non authenticité de l'image.

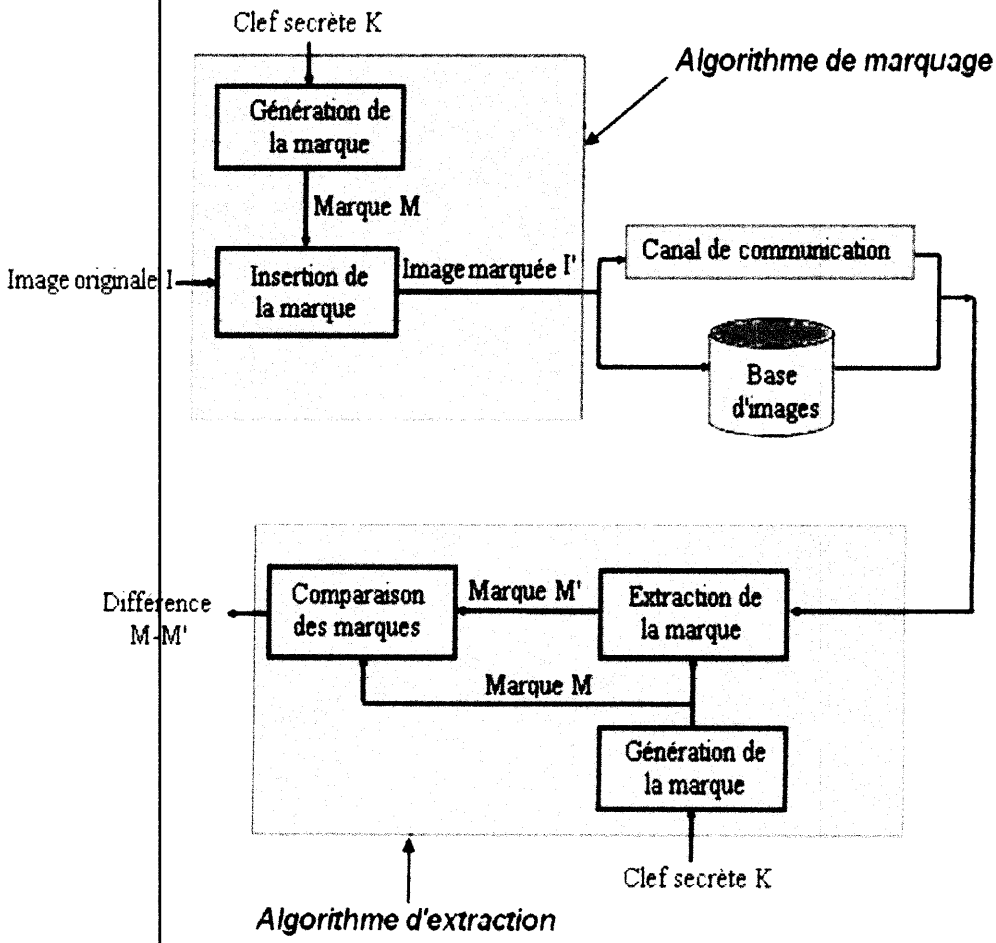

***Figure II.1** : Schéma générique d'un système d'authentification* **[17]**.

Pour être efficace, un système d'authentification d'image doit satisfaire les critères suivants **[20]** :

- **Sensibilité :** le système doit être capable de déceler des manipulations pouvant modifier l'interprétation que l'on a d'une image, telles que des recadrages ou des retouches locales.
- **Tolérance :** le système doit être tolérant vis-à-vis des algorithmes de compression avec perte tels que Jpeg, et plus généralement vis-à-vis des manipulations bienveillantes (*générées, par exemple, par les fournisseurs de contenu multimédia*).

- **Localisation des régions altérées :** le système doit être en mesure de donner à l'utilisateur une information visuelle permettant d'identifier les régions de l'image qui ont été manipulées.
- **Reconstruction des régions altérées :** le système doit éventuellement permettre une restauration partielle des zones de l'image qui ont été manipulées où détruites, afin de donner à l'utilisateur la possibilité de se faire une idée sur le contenu original de ces régions.

En plus des critères précédents, d'autres contraintes techniques sont également à prendre en considération :

- **Visibilité :** les données d'authentification doivent être invisibles (*dans les conditions normales de visualisation*). Il s'agit de faire en sorte que l'impact visuel du marquage soit le plus faible possible afin que le document marqué reste fidèle à l'original.
- **Robustesse et sécurité :** les données d'authentification ont tout à gagner à être protégées par des méthodes de chiffrement de manière à éviter qu'elles soient falsifiées ou manipulées.
- **Mode d'extraction :** suivant que les données d'authentification sont dépendantes ou non de l'image, on optera pour un mode d'extraction aveugle, la marque représentant les données d'authentification est récupérée à partir de l'image marquée seule (*éventuellement manipulée*), alors qu'en semi-aveugle il s'agit principalement de vérifier la présence de telle marque dans une image. Il est bien évident qu'un mode d'extraction non aveugle est dénué de sens pour un service d'intégrité dans la mesure où il fait appel à l'image originale.
- **Algorithme asymétrique :** contrairement aux services de sécurité plus classiques comme la preuve de propriété où l'on peut se contenter d'une même clef secrète pour l'insertion et l'extraction de la marque, un service d'intégrité nécessite de préférence l'utilisation d'un algorithme de marquage symétrique dans la mesure où tout un chacun doit pouvoir s'assurer de l'authenticité d'une image.

II.3. Revue des méthodes existantes

II.3.1. Marquage fragile

Les premières méthodes proposées pour assurer un service d'authentification étaient basées sur l'utilisation d'un marquage fragile, par opposition au marquage robuste classiquement utilisé pour la protection des droits d'auteur. Le principe de ces approches est

d'insérer une marque ou un logo binaire (généralement *prédéfini et indépendant des données à protéger*) dans l'image d'origine, de telle manière que les moindres modifications apportées à l'image se répercutent également sur la marque insérée. Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence de cette marque. Les techniques proposées en ce sens, réparties en différents domaines de travail sont les suivantes **[2]** :

II.3.1.1. Insertion dans le domaine spatial

a. Insertion de "*checksum*" dans les LSB

Une des premières techniques utilisées pour vérifier l'authentification d'une image visait à insérer des valeurs de " *checksum* " dans les bits les moins significatifs (*LSB*) des pixels de l'image.

L'algorithme proposé par Walton en 1995 **[22]** consiste à sélectionner, de manière pseudo-aléatoire (*en fonction d'une clé*), des groupes de pixels et de calculer, pour chacun d'eux, une valeur de « *checksum* ».

b. Schéma de Yeung et Mintzer [23]

Cette méthode encode un logo binaire dans les bits de poids faible, et la décision quant à l'authenticité de l'image s'effectue par rapport au logo qu'on sait y avoir caché.

c. Schéma de Wong

Ce schéma insère une empreinte de l'image dans elle-même. L'empreinte recalculée à la détection sera comparée à celle qui a été insérée, mettant ainsi en valeur les éventuelles modifications. Cette méthode insère au niveau des LSB, un logo binaire, permettant d'identifier le propriétaire de l'image, et une empreinte de l'image. L'image et le logo sont découpés en blocs. L'empreinte de chaque bloc de l'image est calculée

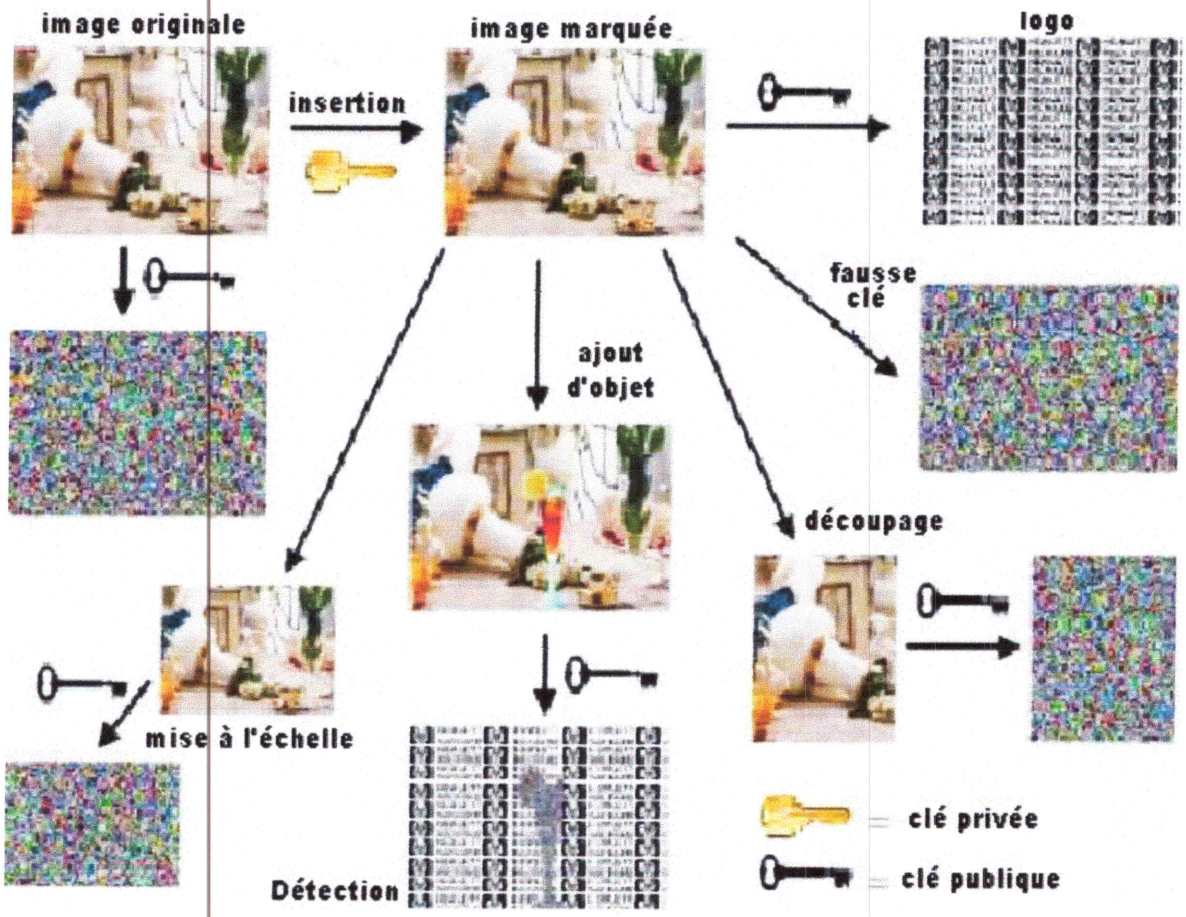

Figure II.2 : *Fonctionnement de la méthode de Wong* **[26]**.

II.3.1.2. Insertion dans le domaine transformé

1. Zhu **[22]** insère la marque dans le domaine DCT (*Transformée en Cosinus Discrète*). La marque est constituée à partir d'un bruit blanc généré grâce à une clé. Cette clé est nécessaire à l'extracteur qui régénère le bruit blanc et le compare à la marque extraite. L'erreur ainsi calculée est comparée à des seuils pour déterminer l'authenticité de l'image. Si cette méthode ne permet pas la localisation des dégradations, elle peut par contre les quantifier, et repérer les fréquences les plus atteintes.
2. Kundur **[24]** utilise quant à lui la DWT (*Discret Wavelet Transform*) et insère les données en quantifiant certains coefficients des images détails de tous les niveaux. Le choix de ces coefficients est déterminé 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 suivant un pas de quantification. A chaque pas est associée, alternativement la valeur 0 ou 1. Ainsi, si au coefficient d'ondelettes correspond la valeur binaire à insérer, le coefficient n'est pas modifié. Par contre, si les valeurs ne correspondent pas, le coefficient est modifié.

II.3.2. Marquage semi-fragile

D'une manière générale, on peut légitimement se poser la question de l'intérêt des méthodes de marquages fragiles vis-à-vis des techniques cryptographiques classiques, dans la mesure où elles ne garantissent également qu'une l'authentification exacte. Face à ce constat de semi-échec, les recherches s'orientent actuellement vers des approches dites semi-fragiles.

Les méthodes ayant recours à un marquage semi-fragile se distinguent des méthodes fragiles dans la mesure où elles offrent une robustesse accrue face à certaines manipulations d'image. L'objectif recherché est de pouvoir discriminer des opérations malveillantes, comme par exemple l'ajout ou la suppression d'un élément important de l'image, des transformations globales " *raisonnables* " ne portant pas atteinte au contenu sémantique de l'image **[4]**.

II.3.2.1. Exemple de méthode transparente à la compression Jpeg

Lin et Chang **[21]** proposent un algorithme d'authentification robuste à la compression Jpeg. Les composantes significatives d'une image de façon perceptuelle correspondent en général aux basses et moyen fréquences. Si l'on modifie les basses fréquences, l'impact visuel est important. Les hauts fréquences (*représentatives des détails*) sont enlevées par la compression Jpeg. Il s'avère donc judicieux de marquer un bit dans les moyennes fréquences du bloc donné. Dans leur article, les auteures ont mis en évidence et ont démontré deux propriétés d'invariance des coefficients DCT vis-à-vis de la compression Jpeg.

La première propriété énonce que si on donne à un coefficient DCT, quel qu'il soit, une valeur entière multiple d'un pas de quantification prédéfini Qm supérieur à tous les pas de quantification possible d'une compression Jpeg acceptable (*facteur de qualité 50% environ*), alors cette valeur peut être recalculé exactement après une compression Jpeg acceptable.

La deuxième propriété définit une règle d'invariance de la relation d'ordre entre les coefficients homologues de deux blocs DCT vis-à-vis la compression Jpeg.

En effet, lors de la compression, les différents blocs DCT d'une image sont tous divisés par la même table de quantification, de ce fait, la relation qui lie les coefficients de mêmes coordonnées de deux blocs reste inchangée après le processus de quantification. La seule exception est que dans certains cas, des inégalités strictes peuvent devenir de simples égalités, par le biais de la quantification. Le système d'authentification proposé par Lin et Chang repose donc sur ces deux propriétés. La première est utilisée pour définir un support de

marquage robuste à la compression Jpeg, tandis que la seconde sert à générer les données d'authentification proprement dites **[4]**.

II.3.2.2. Marquage par région

Le marquage par région consiste à découper l'image que l'on souhaite protéger en blocs relativement grands (*de l'ordre de 64×64 pixels*) et d'insérer, dans chacun d'eux, une marque " *relativement robuste* ". Lorsque l'on souhaite vérifier l'authenticité de l'image, on teste la présence de la marque dans les différents blocs. Dans le cas où la marque est présente avec une probabilité élevée dans chacun des blocs, on peut affirmer que l'image testée est intègre **[4]**.

II.3.2.3. Marquage dans le domaine des ondelettes

Les techniques basées sur les ondelettes sont actuellement de plus en plus fréquentes ou en cours d'investigation. Parmi celles-ci on peut citer celle de Kundur et Hatzinakos **[24]** et celle de Lin et Chang **[21]**. Le principe de la méthode proposée par Lin et Chang est de choisir, tout d'abord, un bruit pseudo-aléatoire et une ondelette de base, qui constituent le secret du système d'authentification. Puis, de décomposer l'image en 4 sous-bandes en fonction de l'ondelette de base choisie au départ. L'étape suivante revient à substituer la sous-bande HH par le bruit pseudo-aléatoire et à effectuer ensuite la transformation en ondelettes inverse afin d'obtenir l'image marquée. Il est intéressant de noter que le fait de modifier uniquement la sous-bande HH (*haute fréquences*) n'entraîne pas de dégradations visibles.

Le processus d'authentification consiste alors à effectuer la même décomposition que lors de la phase d'insertion, puis à corréler la sous-bande HH obtenue avec le bruit pseudo-aléatoire. Si l'image n'a subi aucune manipulation, le résultat du test ressemblera à une matrice de points uniformément répartis. Dans le cas contraire, la distribution perdra son caractère uniforme dans les régions ou l'image a été manipulée. Une autre solution reposant sur la transformée en ondelettes est présentée dans **[25]**, et on trouve dans **[26]** la description d'un système récent dédié aux images codées au format JPEG2000.

II.3.2.4. Marquage d'image basé sur le contenu

L'authentification basée sur le contenu (*Marquage de caractéristiques*) est utilisée pour authentifier un ensemble de caractéristiques perceptuelles de l'image, appelé "*contenu*". Le contenu détermine comment l'être humain interprète la signification sémantique de l'image.

L'idée de base dans cette méthode, consiste à extraire certaines caractéristiques de l'image originale (*couleur, formes, contours, texture*) et à les cacher ensuite dans l'image sous la forme d'un marquage robuste et invisible.

En général, le contenu est représenté par un vecteur appelé " *vecteur de caractéristiques* ", et l'authentification est jaugée à travers une distance d, entre le vecteur de caractéristiques de l'image originale I et celui de l'image à authentifier I' :

Exemple : $d = || \text{vecteur}(I) - \text{vecteur}(I') ||$

Si la distance d est inférieur à un seuil S prédéfini de l'application ($d<S$), le contenu est jugé authentique, sinon, l'image est considérée comme étant manipulée.

Différents schémas d'authentification basée sur le contenu peuvent être envisagés, suivant la mise en œuvre de l'extraction de caractéristiques et la comparaison correspondante montrée dans la figure.

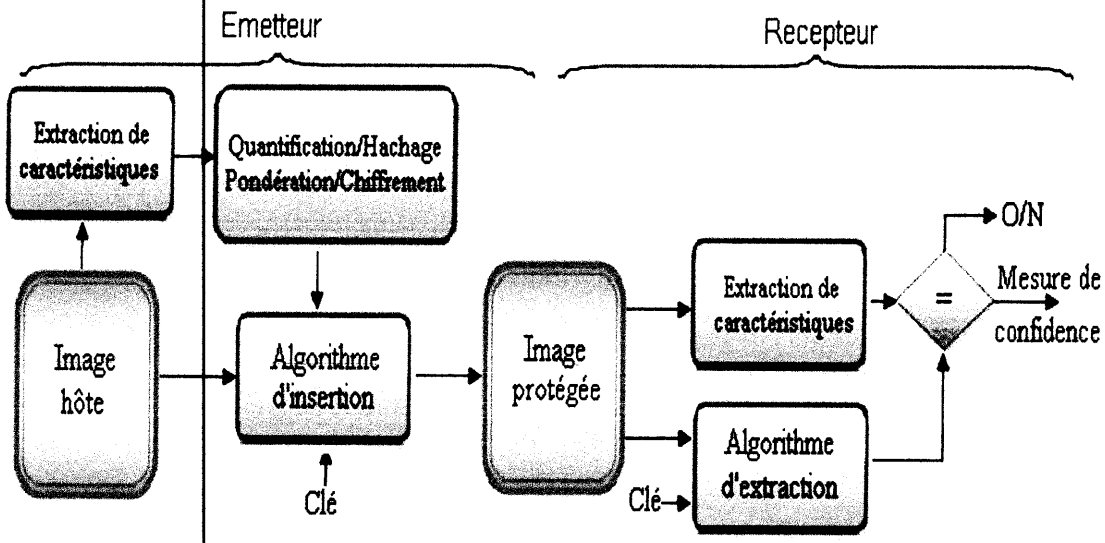

Figure II.3 : *Marquage de caractéristiques* **[4]**.

Les caractéristiques utilisées dans un tel schéma doivent satisfaire les exigences suivantes :

1. Identifier l'image de manière univoque.
2. Etre invariantes à des manipulations modérées qui préservent la qualité perceptuelle de l'image, telles la compression, le débruitage...

3. Etre hautement sensibles aux modifications qui affectent le contenu.
4. La localisation des modifications est une fonctionnalité supplémentaire très souhaitable.
5. La taille des données représentant ces caractéristiques doit être suffisamment faible pour faciliter la comparaison.
6. La complexité de calcul doit être raisonnable pour permettre des applications effectives.

Le choix des caractéristiques de l'image est primordial dans la mesure où il va conditionner les manipulations que l'on pourra détecter et celles qu'on laissera passer. De plus, ce choix dépend également du type d'image considéré (*image satellite, image médicale, photo, etc.*), ainsi que de l'application visée. D'une manière générale, on sélectionne les caractéristiques de l'image en fonction de leur stabilité face aux différentes attaques.

Typiquement, on recherchera des caractéristiques qui sont invariantes face à une compression Jpeg, à de faibles transformations géométriques, à un filtrage/débruitage, mais sensibles à des retouches locales de l'image. Cette technique impose également de nouvelles contraintes, principalement en termes de robustesse et de capacité d'insertion. Une des difficultés de dissimuler les attributs caractéristiques de l'image sous la forme d'un marquage réside dans le fait que l'image marquée est légèrement modifiée par l'insertion de la marque elle-même. Bien que ces variations soient imperceptibles à l'œil, elles affectent légèrement les caractéristiques intrinsèques de l'image. De ce fait, les caractéristiques de l'image originale et celles de l'image marquée ne sont plus exactement les mêmes, et on risque alors de détecter des régions altérées alors que l'image n'a pas été manipulée. Ce risque est plus ou moins important en fonction du type des caractéristiques choisi et de l'algorithme d'insertion utilisé. Ce problème a été résolu dans **[27]** grâce à un processus de marquage itératif. Ce processus est initialisé en marquant une première fois l'image originale avec ses propres caractéristiques, puis, de manière itérative, on extrait les nouvelles caractéristiques de l'image marquée que l'on insère à nouveau dans l'image originale sous la forme d'un nouveau marquage. Seule l'image originale est marquée pour éviter d'accumuler des distorsions liées au processus de marquage. De cette manière, grâce à ce processus itératif, les caractéristiques contenues dans le marquage coïncident quasi parfaitement avec celles de l'image une fois marquée.

II.3.3. Marquage réversible

Une limite évidente à l'utilisation de l'authentification par marquage numérique est la distorsion infligée à l'image hôte par le processus d'insertion. Même si cette distorsion est souvent minime, elle peut ne pas être acceptable dans certaines applications, particulièrement dans les domaines militaire et médical. Il est donc souhaitable de disposer de schémas d'authentification capables de supprimer toute distorsion de l'image après une vérification positive de la marque. Les schémas offrant cette possibilité sont qualifiés de réversibles (*ou inversibles*). Il est à noter cependant, que la moindre attaque ne permet plus d'assurer la réversibilité du système **[4]**.

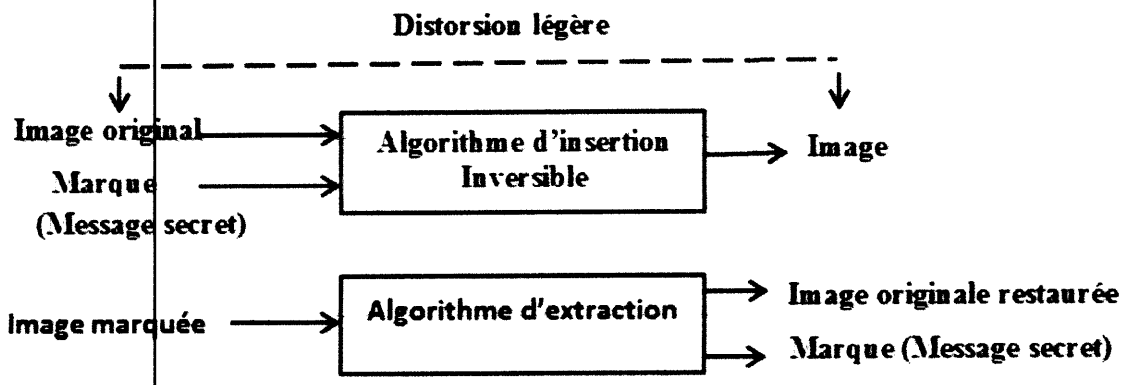

Figure II.4 : *Schéma bloc du marquage réversible.*

On peut classer les schémas réversibles en deux classes :

II.3.3.1 Les schémas basés compression

L'approche généralement suivie dans de tels algorithmes, est d'utiliser une certaine forme de compression sans perte sur certaines caractéristiques extraites de l'image, pour libérer de l'espace dans l'image hôte, destiné à contenir les données compressées ainsi que les données d'authentification (*MAC ou signature*). Pour authentifier l'image reçue, ces données sont décompressées et les données d'authentification sont extraites pour révéler l'image présumée originale. A nouveau, des données d'authentification sont extraites de l'image présumée originale puis comparées à celles extraites. Si elles correspondent, ceci signifie que l'image est authentique **[4]**.

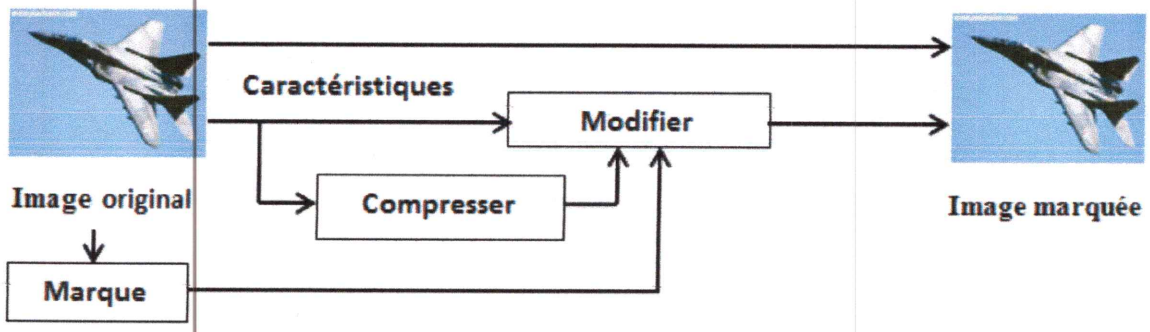

Figure II.5 : *Marquage réversible basé compression.*

II.3.3.2. Les schémas utilisant l'expansion de la différence

Le deuxième type de schémas réversibles, est celui utilisant l'expansion de la différence entre pixels adjacents pour insérer l'information d'authentification secrète. Ces schémas opèrent généralement en générant certaines valeurs représentant les caractéristiques de l'image, puis ces valeurs sont " *élargies* " de telle sorte à insérer les bits de la marque **[4]**.

II.4. Les type d'authentification

Les systèmes d'authentification des images peuvent être regroupés de plusieurs manières suivant qu'ils assurent un service d'intégrité stricte ou bien une intégrité en termes de contenu, suivant le mode de stockage des données d'authentification ou bien encore selon la nature des informations qu'ils enfouissent dans l'image à protéger.

II.4.1. Authentification exacte

La tâche la plus fondamentale est de vérifier qu'un travail n'a pas été changé du tout, depuis qu'il est devenu une partie de confiance. Au moindre changement d'un seul bit, le travail serait considéré comme inauthentique. En insistant sur une copie parfaite, nous évitons n'importe quel besoin de concevoir les algorithmes qui peuvent différencier entre les changements acceptables. Chaque travail est juste une collection de bits d'égale importance.

II.4.2. Authentification du contenu

Il est devenu de plus en plus facile de trifouiller les images numériques d'une façon où il est difficile de s'en apercevoir. Par exemple, les deux figures II.6 et II.7 montre une modification faite à une image en utilisant Adobe Photoshop. Du côté gauche : l'image originale et droite sa version modifiée. Si de telles images étaient des pièces à convection dans un procès, cette forme de manipulation peut poser des problèmes sérieux. On utilise la méthode de l'ajoutassions d'une signature cryptographique au document jugé important **[16]**.

Figure II.6: *Bill Clinton & Hillary.*

Figure II.7: *Bill Clinton & Monica.*

Dans ce type d'authentification en utilise la méthode de tatouage pour vérifier et maintenir l'intégrité du contenu.

II. 4.3. L'authentification sélective

L'authentification exacte est appropriée dans beaucoup d'applications. Par exemple, juste un changement d'un ou deux caractères dans un message texte peut avoir comme conséquence une signification essentiellement différente. Cependant, dans une image ou un clip audio, un changement de certains couples de bits fait rarement une différence de n'importe quelle importance. Les deux images de la figure II.8 semblent identiques, (a) est une version Jpeg compressée de (b).

(a)

(b)

Figure II.8 : *Deux images presque identiques. Image (a) est l'originale, image (b) a subi une compression JPEG avec un facteur de qualité de 90%.*

La méthode utilisée dans ce type c'est le tatouage semi-fragile, cette méthode décrit un tatouage qui est inchangé par des déformations légitimes (figure II.8), mais détruit par des déformations illégitimes (figure II.7) **[28]**.

II.5. Les attaques contre les systèmes d'authentification

Deux catégories d'attaques principales doivent être prises en considération lors de l'élaboration de tout système d'authentification: les attaques ciblant l'image et les attaques ciblant le système d'authentification.

- **les attaques ciblant le contenu de l'image**: ont pour but de manipuler l'image sans tenir compte des mesures de protection de l'algorithme d'authentification. Ces attaques peuvent à leur tour être classées en deux types :
    1. Les manipulations locales, telles l'ajout ou la suppression d'objets dans l'image.
    2. Les manipulations globales, comme le changement d'échelle, le découpage... etc.
- **Les attaques ciblant le système d'authentification** : Suivant le type du marquage (*fragile/semi-fragile*) et le type du système (*symétrique/asymétrique*) différentes attaques peuvent être montées :
    1. Une des attaques les plus courantes contre les systèmes à base de marquage fragile, consiste à tenter de modifier une image protégée sans affecter la marque qu'elle contient, ou bien encore à tenter de créer une nouvelle marque que le détecteur considérera comme authentique. Prenons par exemple le cas volontairement simplifié où l'intégrité d'une image est assurée par une marque fragile, indépendante du contenu, insérée dans les LSB des pixels. Il est clair que si on modifie l'image sans se préoccuper de savoir quels sont les bits affectés par la manipulation, on a toutes les chances pour que la marque soit dégradée et l'attaque détectée. Par contre, si on prend soin de modifier l'image sans toucher aux LSB, la marque restera intacte et le système ne décèlera aucune falsification **[28]**.
    1. D'un point de vue plus général, dès lors que l'intégrité est assurée par une marque indépendante du contenu de l'image à protéger il est possible d'imaginer une attaque qui recopie une marque valide d'une image dans une autre. De cette manière la deuxième image se retrouve alors protégée. Cette attaque peut très bien être appliquée sur la même image. Dans ce cas, la marque est dans un premier temps retirée de l'image, l'image est ensuite manipulée, et enfin la marque est réinsérée dans l'image manipulée, trompant ainsi le système d'authentification.

Chapitre III

Détection et Extraction de caractéristiques

Résumé :

Ce chapitre passe en revue les différentes méthodes de détection des points d'intérêt du contenu d'une image, ainsi que les méthodes d'extraction de leurs caractéristiques et de mesure de correspondance.

III.1. Introduction

Cette partie concerne les outils et les méthodes permettant la recherche d'images par le contenu, qui suscite actuellement un intérêt et une attention considérables et cela de la part de nombreuses communautés: celle de la recherche d'information, qui étend son périmètre au-delà du texte vers les autres médias telle que l'image, celle du traitement et de l'analyse de l'image qui met ainsi en œuvre ses compétences dans un domaine où la demande est forte, celle de l'intelligence artificielle et de l'extraction de connaissances.

Dans notre cas particulier, on s'intéressera à l'extraction de caractéristiques du contenu des images permettant la mesure de correspondance ou d'authentification.

Dans la suite de ce chapitre, une fois le mot "*contenu*" de l'image défini, nous présentons "*l'approche de conception de systèmes d'authentification et de recherche d'images par le contenu*" ainsi que les méthodes d'indexation utilisées. Nous terminons par une conclusion dans laquelle les principaux résultats obtenus sont exposés ainsi que les perspectives envisagées.

Notre but étant de réaliser un système d'authentification d'image numérique simple et efficace, il est nécessaire de travailler à tous les niveaux du système (*détection, extraction de caractéristiques et mesure de correspondance des ces dernière).*

III.2. Généralités

La recherche d'images par le contenu, est une des applications de la vision par ordinateur permettant de rechercher des images dans de grandes bases de données à partir de leurs caractéristiques visuelles. Dans ce contexte, le terme " *contenu* " de l'image doit être compris comme l'ensemble des caractéristiques de l'image.

III.2.1. Région d'intérêt

Nous utilisons la locution région d'intérêt pour traduire dans ce contexte précis le terme Feature. La définition dépend plutôt de la famille de problèmes que l'on cherche à traiter.

Comme expliqué plus haut, une région d'intérêt est une région " *intéressante* " d'une image, et peut être utilisée comme point de départ de nombreux algorithmes de traitement d'images. De ce fait, la qualité de l'algorithme utilisé pour détecter les régions d'intérêt conditionne souvent la qualité du résultat de la chaîne de traitement entière que l'on souhaite appliquer à une image. Aussi, la répétabilité, c'est-à-dire le fait que les mêmes régions d'intérêt (*ou à peu près*) puissent être détectées sur deux images (*numériquement*) différentes (*angle de vue, d'éclairage*...) mais représentant la même scène, est une propriété importante et généralement exigée pour tous les algorithmes de détection de régions d'intérêt **[29]**.

Après la détection, on applique souvent un algorithme de description qui va se concentrer sur chaque région d'intérêt détectée pour calculer ses caractéristiques qui sont principalement celles de l'image.

III.2.2. Points d'intérêt

La région d'intérêt est une partie de l'image qui représente une propriété intéressante. Le point est un cas particulier des régions d'intérêt. En remarquant que dans l'image ils existent plusieurs points qui ont des caractéristiques plus significatives que d'autres. H. Morave, 1977 a introduit la notion de points d'intérêts. Il utilise la fonction d'auto-corrélation afin de déterminer la meilleure position du point saillant, de façon à ce que toute position voisine contienne moins d'informations **[29]**.

III.3. Les détecteurs et descripteurs de points d'intérêt

Les détecteurs et descripteurs de caractéristiques sont conçus pour extraire des points spécifiques d'images. L'égalité des points est une tâche essentielle dans le processus pour trouver le point correspondant dans deux images de la même scène.

Les détecteurs de point d'intérêt local sont conçus pour localiser des points qui contiennent de l'information distinctive dans leur région **[30]**. Ces points sont des points caractéristiques dans l'image. Les détecteurs locaux de point d'intérêt ont besoin de spécifier automatiquement une région autour du point caractéristique qui aura un certain montant d'invariance aux transformations de l'image. Le détecteur sera capable d'extraire des points locaux et région dans les deux images qui correspondent au même point sur la surface de l'objet.

Les descripteurs locaux sont des vecteurs de caractéristiques compacts et distincts, extraits de régions d'intérêt locales. Les descripteurs locaux sont conçus pour capturer une

description compacte et complète de la région locale pour tenir compte de l'égalité entre les points d'intérêt de deux images [30]. Chaque point d'intérêt local est comparé avec plusieurs autres points d'intérêt locaux de l'autre image pour établir une mesure de ressemblance entre un grand nombre possible de points.

III.3.1. Les détecteurs

III.3.1.1. Détecteurs des points d'intérêt

L'efficacité des points d'intérêt a été prouvée pour la reconnaissance d'objets dans des images. La problématique essentielle en détection de points d'intérêt est de trouver des points d'une façon automatisée et suffisante pour représenter l'objet. Pour ce faire on doit respecter les étapes suivantes :

- La répétitivité des points sous plusieurs conditions de prise de vue.
- Définir un voisinage autour de chaque point après son extraction.
- Les représentations des modèles extraies sont comparées avec celles de la base en se référant à des techniques comme le calcul de la distance Euclidienne ou de Hamming.

Les détecteurs de points d'intérêts ont commencés par la détection de coins et de contours comme Harris et le détecteur de régions comme le SIFT " *Scale Unvariant Feature Transform* " qui est invariant au changement d'échelle [31].

III.3.1.1.1. Détecteurs de coins

Ces détecteurs localisent les points et les régions d'intérêt, qui présentent une structure importante dans l'image. Les primitives des coins ont été utilisées dans plusieurs travaux dans la reconnaissance d'objets [32].

❖ **Détecteur basé sur la matrice de Harris**

Ce détecteur est défini par Harris et Stephens. En se basant sur le calcul de la fonction d'auto-corrélation, Harris et Stephens se ramenaient à l'étude de valeurs propres de la matrice de Harris. Trois cas peuvent se présenter :

- Région homogène, si les deux valeurs propres sont faibles.
- Un contour (*transition*) si l'une des valeurs propres est très grande par rapport à l'autre.
- Un coin (point d'intérêt), si les deux valeurs propres sont élevées.

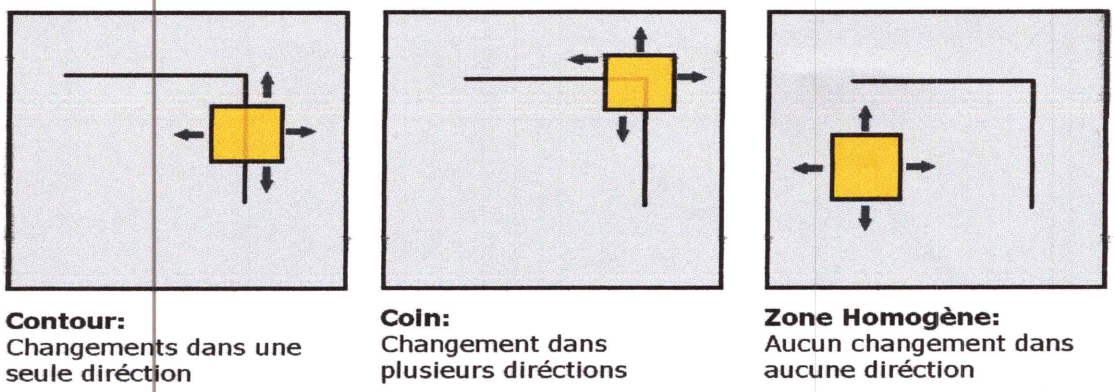

Figure III.1: *Les 3 cas de changements d'intensité considérés* **[32]**.

Donc, le calcul des valeurs propres nous permet de ne garder que les structures en coins, c'est à dire de courbure suffisamment grande (*la figure III.2 est un exemple de détection des coins par Harris*).

- **Exemple**

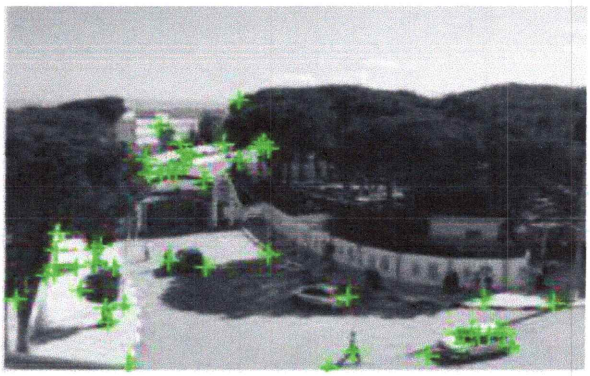

Figure III.2 : *Détection de points d'intérêt par la méthode de Harris.*

- **Détecteurs FAST**

FAST " *Features from Accelerated Segment Test* " est un algorithme proposé originairement par Rosten et Drummond **[33]** pour identifier les points d'intérêt dans une image. Un point d'intérêt dans une image est un pixel ayant une position bien définie et qui peut être détecté avec robustesse. Les points d'intérêt possèdent un grand contenu d'information locale et ils devraient être idéalement répétables entre images différentes. Il est conçu pour être très effectif et convenable pour les applications temps réel de n'importe quelle complexité.

Le critère " segment test " opère par considération d'un cercle de seize pixels autour du candidat 'p' de coin. Le détecteur original classe 'p' comme un coin s'il y a un ensemble de 'n' pixels contigus dans le cercle qui sont tous plus lumineux par rapport à l'intensité du candidat I_p plus un seuil t, ou tous plus sombres que $I_p - t$, comme illustré ci-dessous.

FAST est seulement un détecteur, mais il a prouvé être assez fiable et utilisé par beaucoup de descripteurs. La démarche de l'algorithme FAST est expliquée ci-dessous **[34]**:

1. Sélectionnez un pixel 'p' dans l'image. Assumez l'intensité de ce pixel pour être 'I_P'. C'est le pixel qui sera identifiée comme un point d'intérêt ou pas *(figure III.3)*
2. Définir une valeur de seuil t de l'intensité lumineuse.
3. Considérez un cercle de 16 pixels qui entourent le pixel 'p'.
4. "N" pixels contigus parmi les 16 ont besoin d'être au-dessous ou au-dessus d'I_P par la valeur t, si le pixel a besoin d'être détecté comme un point de l'intérêt.
5. Répétez la procédure pour tous les pixels dans l'image.

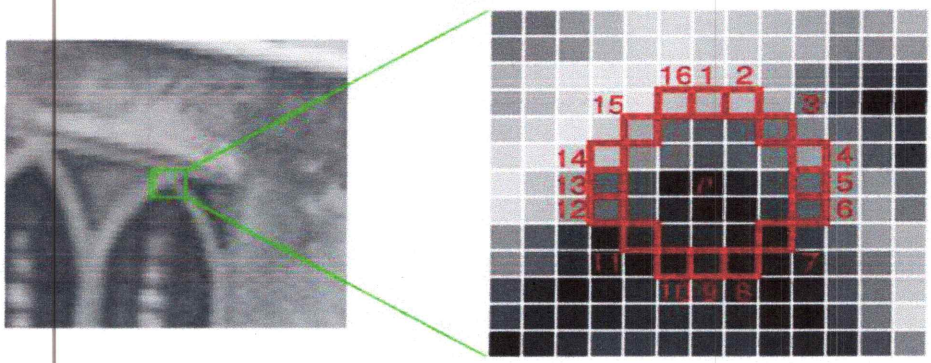

Figure III.3 : *Image qui montre le point d'intérêt sous épreuve et les 16 pixels sur le cercle* **[34]**.

➢ **Remarque**

Pour le calcul plus rapide, utilisez la méthode FAST (*Comparaison de l'Intensité Locale*). Pour l'exactitude de calcul, utilisez la méthode de Harris.

III.3.1.1.2. Détecteurs de régions

Ces détecteurs permettent de remédier aux lacunes du détecteur de coins concernant les zones uniformes. Ce détecteur extrait les régions de l'image qui sont des zones homogènes en termes d'intensité.

❖ **Détecteur SIFT**

La méthode SIFT **[32]** est très utilisée pour la reconnaissance visuelle dans le domaine de la vision par ordinateur. Cette méthode utilise des descripteurs haut-niveau de points d'intérêt des images pour la mise en correspondance. La force de l'algorithme est la stabilité des descripteurs, invariants à la rotation, translation, changement d'échelle et partiellement invariants aux changements d'illumination.

L'algorithme comporte 5 étapes **[35]**.

1. Extraction des points d'intérêt dans l'espace échelle.
2. Calcul de l'orientation des points.
3. Calcul des descripteurs.
4. Mise en correspondance.
5. Calcul de l'orientation relative entre images.

Figure III.4 : *Exemple de points d'intérêt détectés par SIFT.*

❖ **Détecteur MSER**

D'autres approches ont été envisagées pour fournir des détecteurs invariants à l'échelle. Matas et al. J. introduisent la détection MSER qui s'appuie sur un algorithme de segmentation de type " *watershed* ". Kadir *et al.* Mesurent l'entropie des histogrammes d'intensité des pixels pour chercher les maxima locaux.

➢ **Exemple**

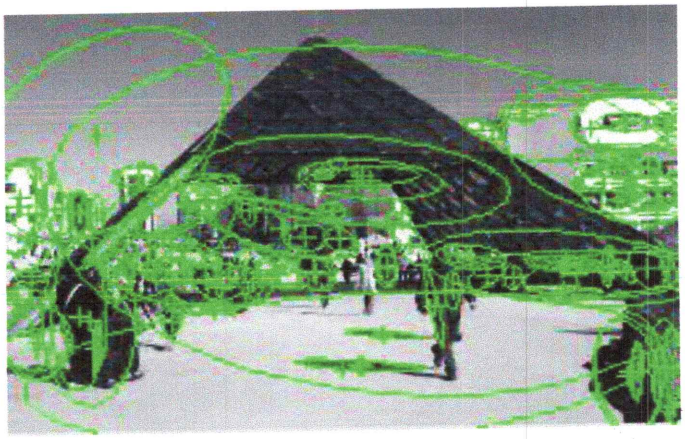

Figure III.5: *Détection de points d'intérêt par la méthode de MSER.*

❖ **Détecteurs SURF**

La détection des points SURF est basée sur la construction d'images intégrales qui permettent de gagner largement en temps de calcul. Les zones de fort changement d'intensité des pixels sont recherchées dans l'image. La matrice Hessienne, basée sur le calcul des dérivées partielles d'ordre deux, est utilisée pour cela. Les points d'intérêt seront donc localisés là où le déterminant de la matrice Hessienne est maximal. Le taux de répétabilité de SURF est directement lié au seuillage du maximum local de la matrice Hessienne. Des études comparatives montrent que ce taux, par défaut, est déjà bon. Parce que nous travaillons sur des images de documents en niveau de gris, la binarisation des documents permet de rendre le taux de répétabilité moins sensible à ce seuillage car les transitions entre les lettres et le fond sont binaires **[36]**.

➢ **Exemple**

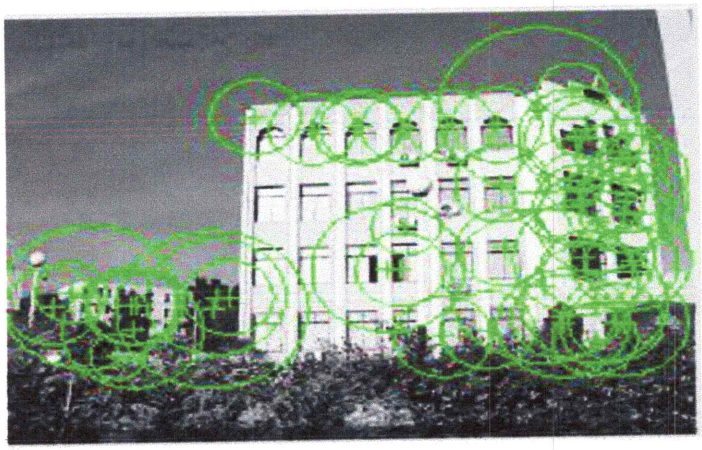

Figure III.6 : *Détection de points d'intérêt par la méthode de SURF.*

❖ **Détecteurs BRISK**

Inspiré par le descripteur effectif BRIEF, les auteurs du détecteur BRISK ont proposé un descripteur binaire associé **[37]**. La description est aussi un signe binaire de différences entre paires d'emplacements. La différence principale avec BRIEF est qu'il est invariable au changement d'échelle et de rotation. La figure III.7 montre le modèle d'échantillonnage BRISK.

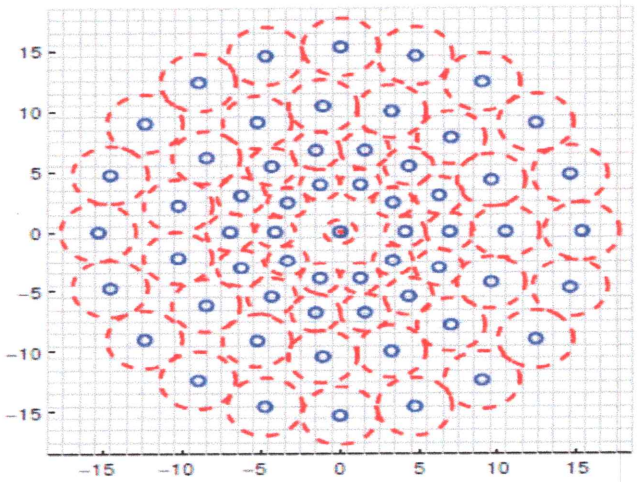

Figure III.7 : *Modèle d'échantillonnage BRISK* **[37]**.

On considère chaque point de l'échantillonnage, nous prenons autour de petite pièce une application lissage Gaussian. Le cercle rouge dans la figure III.7 illustre la dimension de la déviation standard du filtre Gaussian a appliqué à chaque point de l'échantillonnage.

L'algorithme pour l'extraction du descripteur est le suivant:

1. Un modèle d'échantillonnage concentrique est créé.
2. Un ensemble de longues paires de la gamme et un ensemble de paires de la gamme courtes est créé.
3. l'orientation globale est estimée utiliser l'ensemble de longues paires de la gamme.
4. le modèle d'échantillonnage est tourné dans la direction de l'orientation calculée.

BRISK est équipé avec un mécanisme pour compensation de l'orientation, en essayant d'estimer l'orientation du point d'intérêt et rotation. Le modèle d'échantillonnage par cette orientation BRISK devient quelque peu invariant à rotation.

➢ **Exemple**

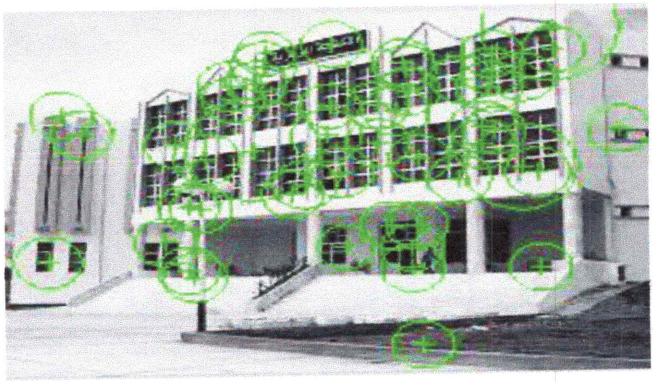

Figure III.8 : *Détection de points d'intérêt par la méthode BRISK.*

III.3.2. Comparaison entre les détecteurs

Pour faciliter l'identification de chaque méthode on résume les principales informations pour chaque détecteur.

Détecteur	**Catégorie**	**Invariance**	**Niveau de détection**
Harris	Coins	Rotation	Important
FAST	Coins	Echelle	Moyen
SIFT	Régions	Echelle et Rotation	Important
SURF	Points	Echelle et Rotation	Important
BRISK	Points	Rotation	Important
MSER	Régions	Echelle	Moyen

Tableau III.1 : *Tableau comparatif de différents détecteurs.*

III.3.2. Les descripteurs

Une fois les points d'intérêt détectés, l'étape suivante est de calculer un descripteur pour chaque point. Le descripteur est une empreinte qui va identifier le point et va servir pour le mettre en correspondance avec les points extraits sur l'autre image.

III.3.2.1. Descripteurs de texture

La texture est une caractéristique fondamentale des images, car elle concerne un élément important de la vision humaine. Elle traduit donc l'aspect homogène d'une zone, et peut être décrite selon ses propriétés spatiales et fréquentielles. L'approche basée sur la configuration spatiale de l'image consiste à représenter la texture sous forme d'un histogramme en niveau de gris. Les méthodes de description de la texture les plus utilisée se

basent sur les propriétés fréquentielles et s'appuient sur la transformée de Fourier, et en ondelettes [38].

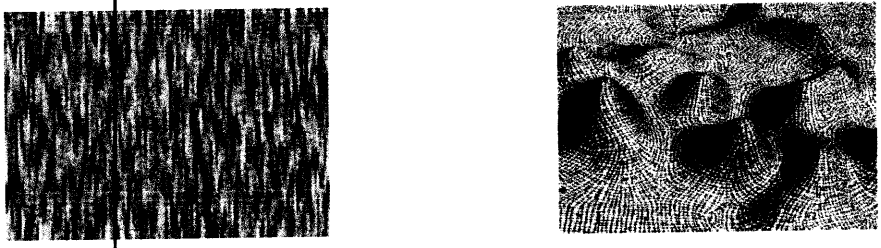

Figure III.9: *Deux images de texture* **[38]**.

III.3.2.2. Descripteurs de forme

La forme est généralement une description très riche d'un objet. De nombreuses solutions ont été proposées pour représenter une forme. Nous distinguons deux catégories de descripteurs de forme :

- **Les descripteurs basés sur les régions :**

Ces descripteurs font référence aux moments invariants et sont utilisés pour caractériser l'intégralité de la forme d'une région. Ces attributs sont robustes aux transformations géométriques comme la translation, la rotation et le changement d'échelle.

- **Les descripteurs basés sur les frontières :**

Ces descripteurs font référence aux descripteurs de Fourier et porte une caractérisation des contours de la forme **[30]**.

III.4. L'extraction de caractéristiques

Le bloc de l'extraction de caractéristiques consiste d'algorithmes responsables pour chiffrer le contenu de l'image dans un concis (*d'une façon compacte*). Les caractéristiques typiques incluent des mesures de : couleur (*ou intensité*), distribution, texture et des forme du plus pertinent objet dans l'image. Ces caractéristiques sont groupées habituellement dans un vecteur de caractère qui peut être alors utilisé comme un indicateur numérique de l'image (*objet*) destiné pour l'étape subséquente, où de tel contenu sera reconnu. **[39]**

III.4.1. Extraction de caractéristiques localisée :

Deux régions principales sont couvertes ici. Les approches traditionnelles ont l'intention de dériver des caractères locaux en mesurant des propriétés spécifiques de l'image.

Les coins: les sommets de courbure locale sont des coins, et analyser une image par ses coins convient surtout aux images d'objets artificiels (*ex : image satellite d'une ville, d'une construction, etc.*)

Les régions : inclut des approches plus modernes qui améliorent la performance en employant la région.

Les algorithmes basés-régions tels que SIFT et SURF comprennent à la fois une phase de détection et une phase d'extraction, alors que pour le cas de la détection MSER c'est l'algorithme SURF qui est généralement utilisé pour l'extraction des caractéristiques.

Les algorithmes d'extraction basés-coins tels que, BRISK et FREAK utilisent les coins détectés par Harris, FAST ou BRISK.

Le vecteur de caractéristiques contient parfois des données issues directement de la détection, telles que l'orientation du point d'intérêt. Les vecteurs de caractéristiques constituent une façon de décrire numériquement le contenu d'une image. De ce fait, ils sont souvent utilisés par des algorithmes plus globaux tels que la comparaison d'images ou la recherche d'images par le contenu.

III.5. Conclusion

L'extraction de structures d'une image s'avère être une tâche complexe, mais en contrepartie, présente de nombreuses applications pratiques. Pour aboutir dans l'extraction de caractéristiques, il faut utiliser des méthodes qui permettent d'extraire toute primitives d'une image (*texture, conteur, couleur, etc.*).

La prise de décisions sur des images approximatives s'est avérée nettement sensible aux conditions d'illumination, au point que deux images très semblables pourraient être extrêmement différentes si elles sont comparées pixel par pixel. Il est donc nécessaire d'extraire les caractéristiques appropriées et discriminantes à partir des deux images et de comparer ces caractéristiques au lieu de comparer des images. Naturellement, les caractéristiques sont plus discriminantes, donc l'authentification sera plus facile **[39]**.

Chapitre IV

Résultat et simulation

Résumé :

L'objectif de ce chapitre, est de dresser un panorama de deux méthodes de détection des points d'intérêt Harris et SURF, alors que l'extraction de caractéristiques est réalisée par FREAK et SURF respectivement. Ensuite après manipulation (compression JPEG), une mise en correspondance est réalisée.

IV.1. Introduction

L'authentification de données dans les images numériques connait un intérêt croissant. Dans notre travail, on décidera que le contenu sémantique (*structurel*) de deux images est authentique si les caractéristiques extraites à partir de deux images différentes passe le teste de mise en correspondance.

IV.2. La méthode proposée

Ayant deux images originales prises du site de l'université de Jijel, le travail réalisé dans ce chapitre est le suivant *(on va appliquer le même enchainement d'étapes sur les deux)* :

1. Prendre l'image originale et faire une copie compressée en utilisant le standard de compression JPEG avec perte. La copie compressée est numériquement différente de l'originale.
2. La détection des points d'intérêt dans les deux images (*originale et compressée*) est réalisée par deux méthodes différentes (*Harris et SURF*) pour la détection des coins et régions, respectivement.
3. L'extraction de caractéristiques est réalisée par l'algorithme FREAK et SURF respectivement.
4. La mise en correspondance (*matching*) est réalisée en calculant une métrique distance entre les caractéristiques extraites des deux images. Si la distance est inferieur à un certain seuil fixé, les caractéristiques sont acceptées semblables. Le pourcentage de caractéristiques acceptées sur le nombre total de caractéristiques comparées permet de décider sur l'authenticité sémantique du contenu des deux images.

IV.3. Description des étapes

Apres compression de l'image originale, vient la phase de détection. Cette détection des points d'intérêt sélectionne une région d'une image qui a le contenu unique, tel que les contours ou les coins. L'avantage de la détection de caractéristiques est de trouver celles qui restent localement invariantes, même dans certains cas en présence de changement d'échelle et même de rotation.

Au niveau de la phase d'extraction, on extrait les caractéristiques (*descripteurs*) des points d'intérêt calculés précédemment. Le descripteur est une empreinte qui va identifier le point d'intérêt et va servir pour le mettre en correspondance avec tous les points extraits sur l'autre image.

Au niveau de la mise en correspondance on va visualiser les points correspondants des deux images en les reliant par un trait.

L'organigramme suivant résume les phases précédentes

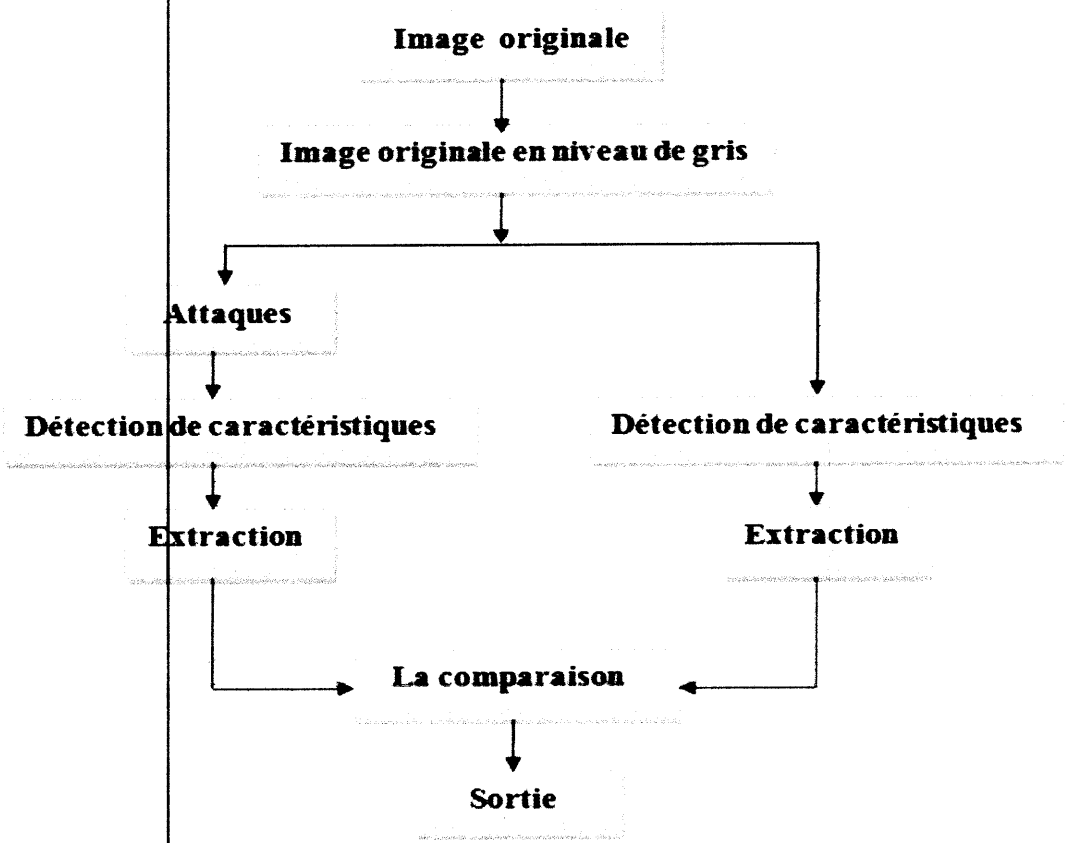

***Figure IV.1** : Schéma synoptique de la démarche.*

IV.4. Résultats de simulation

On teste les algorithmes de Harris et SURF sur les deux images.

IV.4.1. Détection de caractéristique de Harris

La méthode de Harris, consiste à détecter des points d'intérêt qui représente ici des coins dans le contenu de l'image. Cette méthode utilise l'algorithme de Harris-Stephens comme détecteur. Les paramètres qualité minimum 'MinQuality' de Matlab est prise '0.01' valeur par default de Matlab et la taille du filtre 'Filtresize' de Matlab est gardée la même que la valeur par default de Matlab '5'. Les points d'intérêt (*coins*) qui se trouve près des bords de l'image, et qui donc ne peuvent pas être le centre du filtre de 5 pixels sont exclus de la phase d'extraction des caractéristiques.

Les détails des différents algorithmes sortent du cadre de notre projet.

IV.4.1.1 Détecteur Harris appliqué à l'image la fontaine

On a pris pour premier essai l'image qu'on a appelé fontaine située face du hall de technologie et on a effectué une compression JPEG, pour voir si la compression influe sur la correspondance des caractéristiques.

Figure IV.2 : *Image originale*

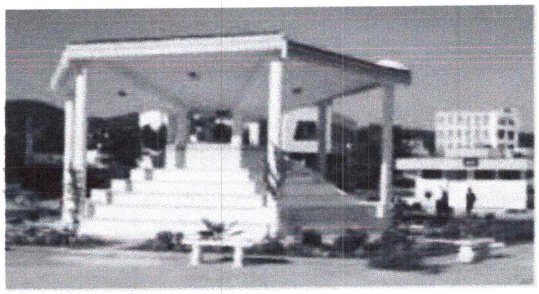

Figure IV.3 : *Image originale grisé*

La détection des points d'intérêt (coins)

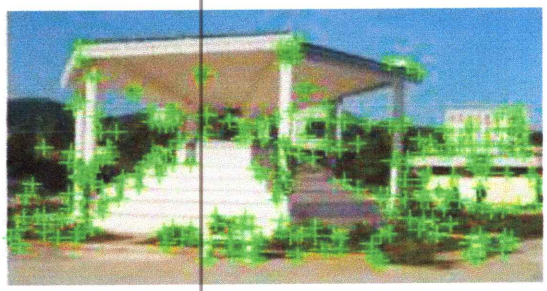

Figure IV.4*: Coins image originale.*

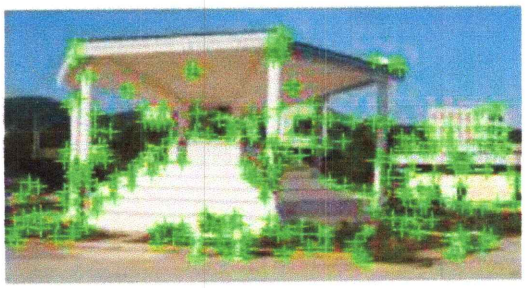

Figure IV.5: *Coins image compressée.*

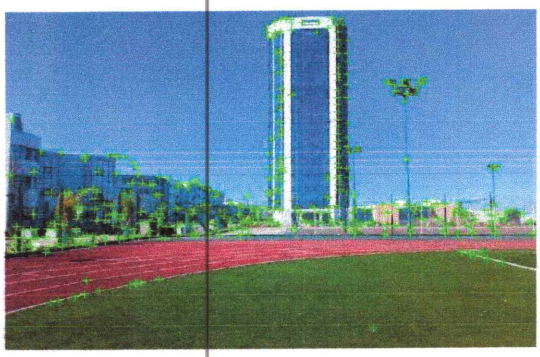

Figure IV.10: *Coins détectés (Image originale).*

Figure IV.11 : *Coins détectés (Image compressée)*

L'extraction de caractéristiques et la mise en correspondance des celles-ci dans l'image originale et l'image compressée.

Figure IV.12*: Les plus importants coins qui correspondent des deux images originale et compressée.*

On remarque que l'influence de la compression JPEG à un facteur de qualité de 80est imperceptible, alors que le pourcentage des caractéristiques trouvées similaires a encore diminué et devient 61,44%.

IV.4.2. Détection SURF

La méthode SURF, s'intéresse à la détection des points d'intérêt qui sont des régions (*plobs / régions*) dans ce cas plutôt que des coins. Cette méthode utilise l'algorithme SURF comme un détecteur de régions d'intérêt et aussi pour extraire les caractéristiques de ceux-ci.

IV.4.2.1 Détecteur SURF appliqué à l'image fontaine

Le même traitement est refait encore une fois, mais cette fois-ci en utilisant l'algorithme de SURF à la détection au lieu de Harris et SURF (*qui détecteur/extracteur*) aussi à l'extraction au lieu de FREAK. La deuxième image est toujours une copie JPEG compressée de l'image originale avec un facteur de qualité de 80.

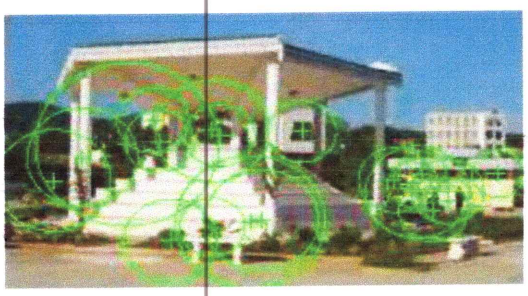

Figure IV.13: *Image originale détecté.*

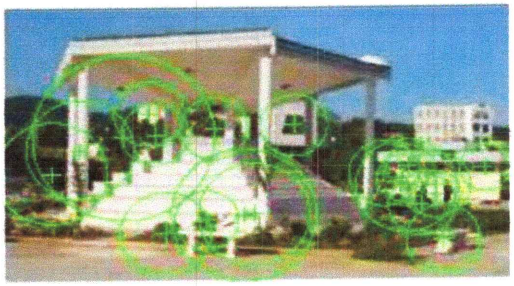

Figure IV.14: *Image originale extraie.*

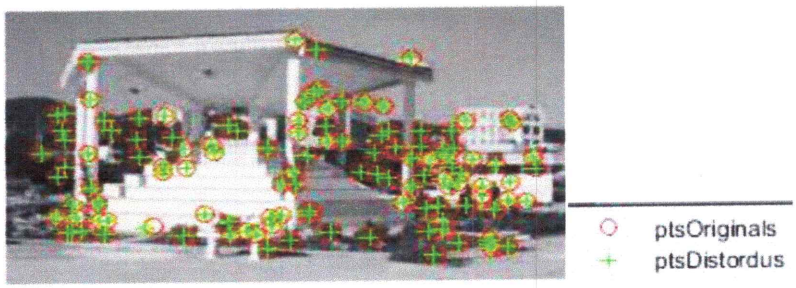

Figure IV.15: *La comparaison des deux images l'originale et le compressé.*

On trouve dans ce cas un taux de correspondance de 95.27% ; une augmentation considérable de pouvoir détecter et extraire les caractéristiques pertinentes.

IV.4.2.2. Détecteur SURF appliqué à l'image rectorat de Tassoust

Le même test de la méthode SURF est refait une autre fois cette fois-ci sur l'image rectorat de Tassoust.

Correspondance de 86,13% est retrouvée dans ce cas.

On a récapitulé les résultats dans le tableau suivant :

Image	Correspondance Harris (%)	Correspondance SURF (%)
Fontaine	84,32	95,27
Rectorat	61,44	86,13

IV.1 : *Résultats de simulation.*

On remarque que le détecteur/extracteur SURF qui opère non-plus sur des coins isolés, mais sur des régions qui sont généralement plus grandes et donc décrivent plus efficacement le contenu de l'image. De ce fait SURF est comme on pouvait le prédire est plus robuste et le pourcentage de correspondance de l'image originale avec l'image attaquée par la compression JPEG est supérieur.

IV.5. Conclusion

On a testé dans ce chapitre deux méthodes différentes de détection et d'extraction des caractéristiques sur deux images numériques. La méthode de détection de Harris (***utilisant l'algorithme FREAK pour l'extraction des caractéristiques***) est basée sur la détection des coins, et qui est ni invariante au changement d'échelle ni à la rotation, alors que la deuxième (*SURF détecteur et extracteur en même temps*) basée sur l'approche régions est invariante aux deux.

Ni changement d'échelle ni rotation n'ont été appliqués à l'image, mais seulement une compression JPEG (*facteur de qualité 80*) qui numériquement change considérablement les valeurs des pixels alors que du point de vue sémantique (*contenu*) l'image reste visuellement inchangée.

Les résultats de la mise en correspondance montrent que la méthode SURF donne un plus grand nombre de caractéristiques classées semblables. Cela montre que SURF est plus robuste face à la compression JPEG avec pertes.

Références Bibliographiques

[1] Afaf Afer, *"Transfert sécurisé d'image par combinaison des techniques de compression, de cryptage et de marquage,"* Mémoire de Master, Université de Jijel, Algérie, 2012.

[2] Mohammed Bouab et Mourad Chebbat, *"Proposition d'une Méthode d'Authentification des Images Numériques,"* Mémoire de Licence, Université de Jijel, Algérie, 2002-2003.

[3] R. Achary, D. Anand, S. Bhat and U.C. Niranjan, ''Compact torage of medical images with patient information,'' *IEEE Transactions on Information technology in Biomedicine*. Vol. 5, 2001, pp. 320-323.

[4] Samia Chikhi, " *Contribution à l'authentification souple d'images digitales par des techniques de marquage numérique Application aux images médicales,"* Thèse de Doctorat, Université Mentouri de Constantine, Algérie, Octobre 2008.

[5] www.cgi..ca/cgi/pdf /cgi_whpr_35_pki_f.pdf
Croupe CGI, "*cryptographie clé publique et signature numérique principe de fonctionnement,*" 2002.

[6] G. Coatrieux, H. Maitre, "Image médicales, sécurité et tatouage, "*Annales des Télécommunications, Numéro Spécial Santé,* vol.58, pp.782-800, 2003.

[7] G. Dubertret, " *Initiation à la cryptographie,* " Vuibert, 1998.

[8] Abdelhakim Frites, " *Dissimulation des Images dans la Transformée en Ondelettes,* " Mémoire de Master, Université de Jijel, Algérie, 2014.

[9] Patrik Bas, " *Méthodes de tatouage d'image fondées sur le contenu,* " Thèse de Doctorat de l'INPG, Grenoble, 6 Octobre 2000.

[10] http://www.reuters.com.

[11] A. P. Petitcolas, R. J. Anderson and M. G. Kunh, "Information hiding-a survery," *Proceedings ofthe IEEE*, 87(7): 1 062-1 078.

[12] "*Security and Watermarking of Multimedia Contents II de SPIE Electronices Imaging,*" 2328 Jan 2000-San Jose CAL. http://www.spie.org/info/ei

[13] http://www.intelligenceonline.fr/: Les efforts de la NSA vis-à-vis la stéganographie.

[14] "*IEEE Colloquium on Secure Image and Image Authentication,*" 10 April 2000 at IEEE Savoy place in London-(GB). http://www.iee.org.uklEvents/elOaprOO.htm

[15] M. Barni, F. bartoloni, V. sappellini, A. llippi, and A. Piva, "A dwt-based technique for spatio-frequency masking of digital signatures," *In Ping Wah Wong and Edward J. delp, editors, ISBT/SPIE's 11th annual symposium, Electronic Imaging* , 99: "security and watermarking of multimedia centents," *volume 3657 of spie proceedings* , pp.31-39 san Jose, California USA, 23-29 January 1999.

[16] Samira Bouchama, "*Le tatouage des images appliqué à l'imagerie médicale,*" Mémoire de Magister en Électronique, École Nationale Polytechnique, 2007.

[17] 1. J. Cox, M. L. Miller & J. A. BIoom, "*Digital watermarking,*" Morgan Kaufmann, edition académique, New York, 2002.

[18] M. Nishio, Y. Kawashima, S. Nakamuar & N. Tsukamoto, (2002), "*Development of a digital watermark method suitable for medical images with error correction,*" RSNA'02, Archive Site: http://archive.rsna.org/index.cfm.

[19] Understanding and Intergrating KODAK Picture Authentication Cameras. http://www.kodak.com/US/en/digital/software/imageAuthentication/ .

[20] M. Wu & B. Liu, 1998, "Watermarking for image authentication," *Proceeding of the IEEE International Conference on Image Processing*, II, 437-441.

[21] C.-Y. Lin & S.-F. Chang, 2000, "Semi-Fragile Watermarking for Authenticating JPEG Visual Content," *SPIE International Conference on Security and Watermarking of Multimedia Contents, San Jos, USA,* vol. 3971, No. 13, pp.140–151.

[22] S. Walton, 1995, "Information Authentication for a Slippery New Age," *Dr. Dobbs Journal*, vol. 20, No. 4, pp. 18-26.

[23] P.-W. Wong, 1998, "A public key watermark for image verification and authentication," Proceeding of the IEEE International Conference on Image Processing, pp. 455-459.

[24] D. Kundur & D. Hatzinkos, 1999, "Digital watermarking for telltale tamper proofing and authentication," *Proceedings of IEEE*, 87(7), pp. 1167-1180.

[25] A. Van Leest, M. Van der Veen, & F. Bruekers, (2003), "*Reversible image watermarking,*" Proceedings of the IEEE International Conference on Image Processing, II.

[26] S. Yang & & C. Chen, 2005, "Robust image hashing based on SPIHT," *In Proc IEEE Information Technology: Research and Education* – ITRE,05, pp. 110-114.

[27] C. Rey & -J. L. Dugelay, (2000), "*Blind Detection of Malicious Alterations on Still Images Using Robust Watermarks*," IEE Secure Images and Image Authentication colloquium, London, UK.

[28] "*Information Security and Multimedia Content Workshop*," March 10-11 2000, Seoul, Korea. http://multimedia.kangwon.ac.kr/ismc/ismc 2 000 _1.html.

[29] D. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *IJCV*, vol. 2, No. 60, pp. 91-110, 2004.

[30] K. Grauman, B. Leibe, "*Visual Object Recognition,*" 5(2):23-39, 2011.

[31] D. Lowe, "*Distinctive Image Features from Scale-Invariant Keypoints,*" IJCV, vol. 2, no. 60, pp. 91-110, 2004.

[32] G. David Lowe, "*Distinctive image features from scale-invariant keypoints,*" 2003.

[33] E. Rosten and T. Drummond, "*Machine learning for high speed corner detection,*" in 9th European Conference on Computer Vision, 1:430–443, 2006.

[34] Vis. Wanathan, D. Geetha, "*Features from Accelerated Segment Test (FAST),*" (n.d.).

[35] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, 60(2):91–110, 2004.

[36] http://www.google.com/insidesearch/features/images/searchbyimage.

[37] S. Leutenegger, M. Chli and R. Siegwart, "*BRISK: Binary Robust Invariant Scalable Keypoints,*" in IEEE International Conference on Computer Vision (ICCV), 2011.

[38] http://www.xbox.com/en-US/community/events/e3/kinect.htm.

[39] https://support.google.com/websearch/answer .