UNIVERSITE ELHADJ LAKHDER - BATNA
FACULTE DES SCIENCES DE L'INGENIEUR
DEPARTEMENT D'INFORMATIQUE

Mémoire

présenté en vue de l'obtention du diplôme

Magister en Informatique

Spécialité : Ingénierie des Systèmes Informatiques
présenté et soutenu publiquement par

Nour El-Houda GOLEA

Titre :

Tatouage numérique des images couleurs RGB.

JURY

M.	AMMAR LAHLOUHI	Président
M.	MOHAMED CHAOUKI BABAHENINI	Examinateur
M.	ABDELKADER GASMI	Examinateur
M.	REDHA BENZID	Rapporteur
M.	RACHID SEGHIR	Co-Rapporteur

Remerciements

Je tiens tout d'abord à exprimer mes sincères remerciements à mes encadreurs Mr. Redha BENZID et Mr. Rachid SEGHIR qui ont assumé la direction de ce travail. Leur dévouement, leur disponibilité et leurs conseils m'ont permis d'accomplir ce travail dans les meilleures conditions. Merci de m'avoir fait découvrir le plaisir de la recherche et de m'avoir soutenue jusqu'au bout.

Je remercie les membres de jury qui ont accepté de juger ce travail :

Dr. Ammar LAHLOUHI, maître de conférences à l'université de Batna, qui me fait le grand honneur d'accepter la présidence du jury.

Dr. Mohamed Chaouki BABAHNINI, maître de conférences à l'université de Biskra et Dr. Abdel-kader GASMI, maître de conférences a l'université de M'sila pour l'honneur qu'ils me font en acceptant de participer à ce jury.

Je suis très reconnaissante à mes enseignants durant les années de cette formation. J'adresse un remerciement particulier a Dr. Ali BEHLOUL.

Je tiens egalement à remercier tous mes collègues à l école doctorale STIC (ISI).

Je réserve un remerciement chaleureux à mes chères amies : Lemya, Nabila et Leila.

Un grand merci à mes très chers parents qui m'ont toujours aidé, soutenu et encouragé au cours de mes études.

Je remercie aussi mes sœurs et frères : Affaf, Farouk, Asma, Nour El-Imen et mon petit frère adorable Mohamed Akram.

Merci à ma grande mère, merci pour son encouragement et ses prières.

Merci à tous ceux qui ont su me donner le goût pour la science et la recherche.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Les réseaux numériques sont tellement développés qu'ils sont devenus un mécanisme primordial de communication. Ils permettent de transmettre toute sorte d'informations : textuelles, sonores, et principalement des images. L'utilisation accrue de ces dernières est renforcée par l'apparition des caméras, appareils photos numériques et des téléphones mobiles.

Le grand développement des technologies de communication et des outils de traitement d'images soulève un nombre important de problèmes : la distribution illégale, la duplication, la falsification et l'authentification. 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 droit d'auteurs.

En outre, le développement des systèmes multimédia distribués, en particulier sur les réseaux ouverts comme l'Internet, est conditionné par le développement de méthodes efficaces pour protéger les propriétaires de données contre la copie non autorisée et la redistribution du matériel mis sur le réseau.

Depuis l'antiquité, il y a eu des méthodes d'établir l'identité du propriétaire d'un objet en cas de conflit comme l'inscription du nom du propriétaire sur l'objet (exemple : tatouage du papier).

Cependant, dans le monde numérique, des techniques plus sophistiquées sont exigées afin d'assurer la même chose, depuis que la reproduction des travaux des autres est devenue extrêmement facile et le travail reproduit s'étend à la vitesse de la lumière à travers le globe.

La cryptographie constitue la première solution pour sécuriser le transfert des données numériques. Elle répond aux besoins des utilisateurs en matière de sécurité comme la confidentialité, l'intégrité, et l'identification. Néanmoins, une fois le document est décrypté, il n'est plus protégé, et il peut être distribué malhonnêtement (il n'y a plus de contrôle sur la diffusion des données).

Dans les dernières décennies, le concept de tatouage numérique a été connu comme un moyen utile pour faire face à ce type de problème. Cette nouvelle technologie consiste à insérer dans une image une marque (watermark), qui peut être le logo d'une société, le nom du propriétaire, etc.

Le watermark inséré doit être entièrement invisible par l'observateur humain. L'opération d'insertion ne doit pas détériorer l'image hôte de façon perceptible, c'est à dire l'image tatouée doit être visuellement équivalente à l'image originale.

Autres conditions que doit remplir un algorithme de tatouage dépendant du problème traité :

- Un algorithme de tatouage, peut être un problème de copyright. Dans ce cas, le watermark doit être *robuste*, i.e., il doit être suffisamment résistant à certains types d'attaques.
- Un algorithme de tatouage, peut avoir aussi l'objectif de repérer toute manipulation non autorisée de l'image. Dans ce cas, le watermark doit être *fragile* de sorte que n'importe quel

changement de l'image entraîne une modification du watermark, et soit donc détecté.

En plus des critères précédents, d'autres aspects sont possibles :

– Le besoin ou non de l'information originale à l'extraction : L'extraction la plus intéressante mais aussi la plus difficile est l'extraction *aveugle* (blind extraction). Dans ce mode, l'image tatouée et la clé sont utilisées pour détecter le watermark.
– L'information secrète : La méthode de tatouage doit respecter le principe suivant énoncé par Kerckhoff [21] : "l'algorithme lui-même doit pouvoir être rendu public, la sécurité ne dépendant pas de son caractère secret".
– Domaine d'insertion du watermark : les techniques courantes décrites dans la littérature peuvent être regroupées en deux principales classes : techniques travaillant dans le domaine *spatial* et techniques travaillant dans le domaine *transformé* (ou fréquentiel). Dans les techniques spatiales, le watermark est inséré en modifiant directement les valeurs de pixels de l'image hôte. Ce sont des méthodes simples et peu coûteuses en temps de calcul. Tandis que dans le domaine fréquentiel, le watermark est inséré en modifiant les coefficients de la transformée utilisée. Des schémas de tatouage peuvent effectuer l'insertion du watermark dans des espaces transformés. Un espace transformé est obtenu après l'emploi d'une transformée telle que : DCT, DFT, DWT, SVD, etc. Cette stratégie rend le watermark plus robuste à la compression, puisqu'elle utilise le même espace qui sert au codage de l'image.

Contribution

Bien que, le tatouage numérique est un nouvel axe de recherche, il a gagné beaucoup d'attention et a évolué très rapidement. Dans la littérature, plusieurs méthodes efficaces sont développées et satisfont certains conditions selon le problème traité, mais la majorité des contributions ont été apportées aux images aux niveaux de gris.

Dans les dernières années, la couleur est devenue un élément clé pour les systèmes de traitement d'images et de vidéos. Il est bien connu que la couleur joue un rôle central dans le cinéma numérique, l'électronique, les systèmes photographiques comme les caméras numériques, les lecteurs vidéo, les téléphones cellulaires et les imprimantes. Pour cette raison, nous avons orienté notre attention vers le tatouage d'images couleurs. Notre contribution se place dans le cadre de proposer des nouveaux schémas de tatouage d'images couleurs RGB. Nous avons travaillé sur différents critères : robuste/fragile, domaine spatial/domaine transformé.

Nos objectifs sont centrés sur deux grands axes de recherche dans le domaine du tatouage numérique : le premier axe concerne le tatouage *robuste* qui a pour but de protéger les droits d'auteurs, tandis que, le deuxième axe concerne le tatouage *fragile* qui a pour objectif de garantir un service d'intégrité et d'authentification. Nous nous sommes aussi intéressés au mode d'extraction aveugle, car le caractère aveugle constitue un enjeu majeur dans les applications réelles. Cela permet de ne pas diffuser les données originales qui peuvent être détruites après tatouage.

Outre un état de l'art, nous allons présenter dans ce mémoire deux méthodes que nous avons développées.

La première méthode :

Nous avons proposé un nouveau schéma du tatouage robuste d'images couleurs RGB, qui est caractérisé par les points suivants :

– L'algorithme du tatouage est robuste ;

– La phase de détection est aveugle ;
– Le watermark est inséré dans le domaine transformé, en utilisant la transformé SVD ;
– Le watermark inséré est une image couleur RGB ;
– L'algorithme de tatouage est publique : la sécurité dépend d'une clé secrète.

Les résultats expérimentaux effectués montrent que notre méthode est maintien une haute qualité d'images tatouées et une robustesse contre plusieurs attaques conventionnels.

La deuxième méthode :

Nous avons aussi proposé un schéma du tatouage fragile. Ce schéma est caractérisé par les points suivants :

– L'algorithme de tatouage est fragile ;
– La phase de détection est aveugle ;
– Le watermark est inséré dans l'image, sans aucune décomposition ;
– Le watermark est inséré dans le domaine spatial, en utilisant le code détecteur d'erreurs CRC ;
– Le watermark est généré en utilisant une clé secrète, et il dépend des données à protéger ;
– L'algorithme de tatouage est publique : la sécurité dépend d'une clé secrète.

Cette nouvelle méthode est efficace en termes d'imperceptibilité et fragilité par rapport aux divers types d'attaques standards et conventionnelles.

Organisation du mémoire

Ce manuscrit est composé de deux parties et est organisé comme suit :

– La première partie établit un état de l'art des différentes terminologies dans lesquelles s'inscrivent nos travaux de mémoire. Cette première partie se décompose en quatre chapitres :
  – Le chapitre 1 présente une introduction aux images numériques. Plus précisément, nous présentons quelques terminologies et quelques notions pertinentes dans le domaine des images numériques telles que la numérisation, le codage et le stockage. Nous présentons aussi quelques aspects du traitement d'images, tels que le filtrage, la compression et le tatouage.
  – Le chapitre 2 décrit les aspects principaux et les terminologies liés aux évolutions des technologies du tatouage invisible des images numériques. Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle. Nous présenterons aussi une taxonomie des techniques de tatouage selon différents critères et quelques métriques pour l'évaluation de la qualité perceptuelle des images.
  – Le chapitre 3 expose le principe du tatouage d'images utilisant la transformée SVD. En particulier, nous présentons quelques algorithmes très connus qui utilisent cette transformée pour insérer des watermarks numériques.
  – Le chapitre 4 présente l'efficacité des techniques du tatouage fragile pour assurer des services d'intégrité et d'authentification.
– La seconde partie est composée de deux chapitres et présente les deux méthodes développées durant ce mémoire.
  – Le chapitre 5 présente la méthode proposée pour le tatouage robuste d'images couleurs RGB.
  – Le chapitre 6 décrit la méthode proposée pour le tatouage fragile d'images couleurs RGB.

Dans les deux chapitres de la seconde partie, nous présentons des exemples et des résultats expérimentaux afin d'évaluer l'efficacité des méthodes proposées.

Première partie

État de l’art

Chapitre 1

Introduction aux images numériques

Résumé : ***« Une image vaut mille mots. »***[1]***, est un adage bien connu qui signifie que les images ont tendance à avoir plus d'impact que le texte, car il est plus facile de faire abstraction du contenu des informations textuelles que s'interroger sur l'origine et l'authenticité d'une photo.***

Depuis quelques années, avec l'explosion d'Internet et aussi le développement à grande échelle de la photographie numérique, le domaine de l'image numérique est devenu un domaine en pleine expansion. Ce chapitre constitue une introduction aux images numériques.

1.1 Introduction

Récemment, l'amélioration sans cesse du facteur puissance/coût des systèmes d'acquisition d'images a permis un formidable essor de l'utilisation de l'image numérique. Cette dernière est utilisée dans divers disciplines scientifiques, comme les disciplines biomédicales. Le biologiste et le médecin peuvent en effet être amenés quotidiennement à créer, visualiser, échanger et archiver des images, et à les insérer dans des rapports ; il a été également constaté qu'ils peuvent en extraire des mesures, d'une façon moins subjective que par la simple perception visuelle, et que la puissance de calcul des systèmes informatiques peut leur fournir, par le traitement automatique de grandes séries d'images, des données pertinentes et statistiquement significatives qui leur seraient inaccessibles directement. Ces nouvelles situations nécessitent l'utilisation des méthodes de traitement et d'analyse d'images.

Le traitement et l'analyse d'images trouvent leurs applications dans des domaines extrêmement variés de l'industrie et de la recherche. Ces méthodes sont utilisées dans de nombreuses disciplines scientifiques, citons en particulier les sciences des matériaux (céramurgie, matériaux pour l'électronique, etc.), les sciences de la terre, la géographie (dont la cartographie et la géomorphologie), la robotique (pour le tri et la vérification de pièces électroniques) ou bien encore dans des domaines aussi variés tels que ceux qui ont trait à l'astronomie, l'identification, la pharmacologie[77]..

Le traitement numérique d'images n'est pas un nouveau phénomène. Des techniques pour la

[1] Proverbe chinois : "an image is worth a thousand Words."

manipulation, la correction et le rehaussement d'images numériques sont utilisées depuis plus de trente ans. Sans traitement numérique approprié, une grande partie des images reproduites ou retransmises seraient de piètre qualité.

l'objectif de ce chapitre est d'introduire le domaine des images numériques. Nous découvrons ce domaine depuis la phase d'acquisition, numérisation, représentation des couleurs, jusqu'au stockage dans les différents formats possibles.

1.2 Les images numériques et le système visuel humain

L'étude de la perception visuelle est intéressante pour le traitement d'images pour deux raisons principales. La première est qu'elle peut nous mettre sur la voie de nouveaux algorithmes reflétant les mécanismes naturels. Et la seconde est qu'elle nous permet de connaître les limites de notre perceptions. Ainsi, il est par exemple inutile de représenter plus de couleurs que nous pouvons en percevoir lors d'une application de visualisation.

Dans un système d'analyse d'images, on distingue la lumière captée par un récepteur (caméra), transmise par des transmetteurs (câbles ou autres) à l'analyseur (l'ordinateur). On peut effectuer la même décomposition avec la perception visuelle. La lumière est captée par l'œil, l'information visuelle est transmise via les nerfs optiques vers l'analyseur qui est le cerveau [61].

La perception visuelle est un mécanisme complexe qui met en jeu plusieurs structures : l'œil, la rétine et le cerveau. La compréhension de ce mécanisme repose sur la modélisation du SVH (Système Visuel Humain) en vue d'en simuler son fonctionnement.

Le SVH est un système sophistiqué qui détecte et agit sur des stimuli visuels. Intuitivement, la vision par ordinateur et la vision humaine semblent avoir la même fonction. Le but des deux systèmes est d'interpréter des données spatiales. Même si l'ordinateur et la vision de l'homme sont fonctionnellement similaires, on ne peut pas s'attendre à un système de vision par ordinateur pour reproduire exactement la fonction de l'œil humain. Cela s'explique en partie parce que nous ne comprenons pas entièrement comment l'oeil fonctionne. En fait, certaines des propriétés de l'œil humain sont utiles pour élaborer des techniques de vision par ordinateur, alors que d'autres sont en fait pas souhaitables dans un système de vision par ordinateur. Mais il existe des techniques de vision par ordinateur qui peuvent être reproduites dans une certaine mesure et, dans certains cas, améliorées même sur le SVH. Pour mieux comprendre ce qu'est une image numérique, voyons d'abord ce qu'est une image et comment fonctionne le SVH.

Dans le SVH, l'élément sensible est l'œil à partir duquel les images sont transmises via le nerf optique au cerveau, pour un traitement ultérieur. Le nerf optique a une capacité insuffisante pour transporter toutes les informations perçues par l'œil. En conséquence, il doit y avoir de prétraitement avant que l'image ne soit transmise par le nerf optique.

Le SVH peut être modélisé en trois parties :

1. *L'œil* : il s'agit d'un modèle physique puisqu'une grande partie de sa fonction peut être déterminée par pathologie ;
2. *Le système nerveux* : il s'agit d'un modèle expérimental, puisque sa fonction peut être modélisée, mais ne peut pas être déterminée avec précision ;

3. *Le traitement par le cerveau* : c'est un modèle psychologique puisque nous ne pouvons pas modéliser le traitement directement, mais nous pouvons seulement déterminer le comportement par l'expérience et la déduction [77].

Tout d'abord, pour obtenir une image, il faut de la lumière. Cette dernière est émise d'une ou plusieurs sources telles que le soleil, des spots, des néons, etc. Cette lumière est représentée par des rayons qui partent de la source dans toutes les directions.

Généralement, lorsqu'un rayon de lumière rencontre un objet, ce dernier en absorbe une partie correspondant à sa couleur, et disperse le reste en une infinité de rayons qui peuvent éventuellement être captés par un oeil annonçant la présence de l'objet ainsi que sa couleur. Pour recevoir ces rayons, l'oeil est équipé d'un appareil optique complet illustré par la Figure 1.1 :

– l'*Iris* sert de diaphragme il s'ouvre et se ferme pour accepter plus ou moins de lumière.
– Le *Cristallin* fait la mise au point en fonction de la distance de l'objet[61].

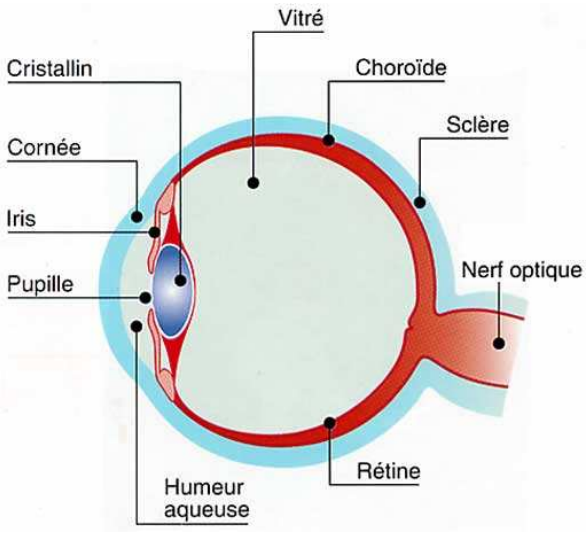


FIG. 1.1 – L'œil, notre capteur.

Finalement, cette lumière arrive sur des capteurs placés sur la rétine appelés cellules à cônes et cellules à bâtonnets du fait de leur forme. Les cellules à bâtonnets, plus sensibles, sont spécialisées dans la vision nocturne. Les cellules à cônes, plus précises, sont séparées en trois types, chacun étant plus sensible à une couleur qu'aux autres. C'est ce découpage de l'image en trois couleurs primaires que vient la vision des couleurs.

Ces informations sont ensuite transmises au cerveau par le nerf optique. C'est le cerveau qui réalise ensuite la partie la plus complexe de regroupement de toutes ces informations pour former une image mentale en couleur de notre environnement [5].

Du point de vue fonctionnel, l'œil peut être comparé à un appareil photo et la rétine à la pellicule photographique (Figure 1.2). En effet, le rôle de l'appareil photo est de concentrer sur le film une image nette ni trop sombre ni trop lumineuse. On y parvient grâce à la bague de mise au point qui met l'objet au foyer et au diaphragme qui s'ouvre et se ferme pour laisser passer juste la bonne quantité de lumière pour la sensibilité du film [36].

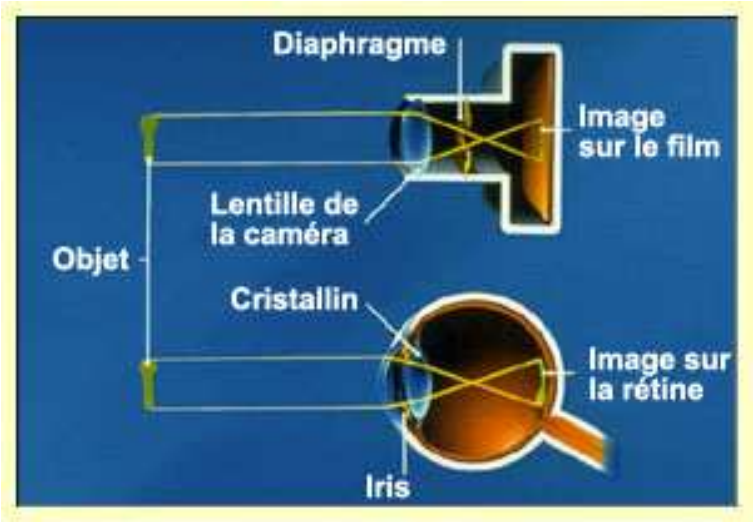


FIG. 1.2 – Analogie entre l'œil et l'appareil photo.

L'animation des images est basée sur le phénomène suivant : Lorsqu'une cellule capte de la lumière, l'impression lumineuse persiste pendant environ 1/50s. En effet, quand l'image change rapidement, l'oeil n'est pas assez rapide pour percevoir une succession d'images fixes et croit voir un mouvement continu [77].

Image réelle/image numérique

Voyons maintenant comment transformer une image réelle en une suite de chiffres compréhensible par un ordinateur.

En fait, il suffit de s'inspirer de l'oeil humain avec ses cellules à bâtonnets et ses cellules à cônes. L'image ne pouvant être analysée de façon continue, son intensité est analysée à intervalles réguliers. Plus il y a de capteurs, plus l'image est précise.

L'image numérique fonctionne sur ce principe. Elle est découpée en de nombreux petits points appelés pixels[2]. Pour chaque élément, on attribue une intensité lumineuse. La qualité de l'image dépend d'une part du nombre de pixels, et d'autre part du nombre de valeurs possibles pour l'intensité [37].

1.3 Numérisation des images

Le terme d'image numérique désigne, dans son sens le plus général, toute image qui a été acquise, traitée et sauvegardée sous une forme codée représentable par des valeurs numériques. La numérisation est le processus qui permet le passage de l'état d'image réelle qui est caractérisée par l'aspect continu du signal qu'elle représente, à l'état d'image numérique qui est caractérisée par l'aspect discret, .i .e, l'intensité lumineuse ne peut prendre que des valeurs quantifiées en un nombre fini de points distincts. C'est cette forme numérique qui permet une exploitation ultérieure

[2]Abréviation de "picture element" qui signifie "élément d'image".

par des outils logiciels sur ordinateur. Du point de vue mathématique, une image réelle est généralement représentée par une fonction bidimensionnelle représentant des caractéristiques particulières du signal lumineux de l'image en chaque point de son espace (intensité, couleur, etc.).

Représentation mathématique sous forme matricielle :

Une image numérique 2D est représentée par un tableau f de n lignes et m colonnes. Le pixel est désigné par un couple (i, j) où j est l'indice de colonne $j \in \{0, m-1\}$, et i est l'indice de ligne $i \in \{0, n-1\}$, m est la largeur, n est l'hauteur de l'image f. Par convention le pixel d'origine (0,0) est en général en haut à gauche (Figure 1.3). Le nombre $f(i, j)$ est la valeur du pixel (i, j), $f(i, j) \in \{0, N_{max} - 1\}$, N_{max} est le nombre de niveaux de gris. On appelle dynamique de l'image le logarithme en base de N_{max}, .i .e, le nombre de bits utilisés pour coder l'ensemble des valeurs possibles [6].

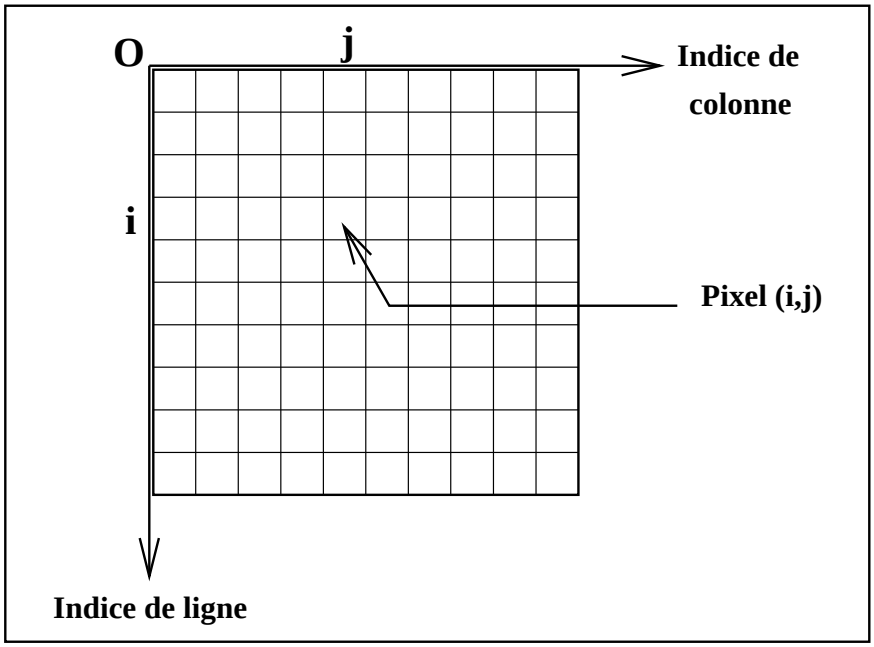


FIG. 1.3 – Représentation mathématique sous forme matricielle d'une image.

1.3.1 Processus de numérisation

La représentation informatique d'une image est nécessairement discrète, alors que l'image est de nature continue : le monde est continue. Si on regarde un peu près, la transformation d'un signal analogique 2D nécessite à la fois une discrètisation de l'espace : c'est l'échantillonage, et une discrètisation des couleurs : c'est la quantification.

Le processus de numérisation d'une image suit les étapes suivantes :

– **Échantillonnage :** l'échantillonnage est le procédé de discrétisation spatiale d'une image consistant à associer à chaque pixel R(x,y) une valeur unique I(x,y) (Figure 1.4). On parle

de sous échantillonnage lorsque l'image est déjà discrétisée et qu'on diminue le nombre de pixels [6].

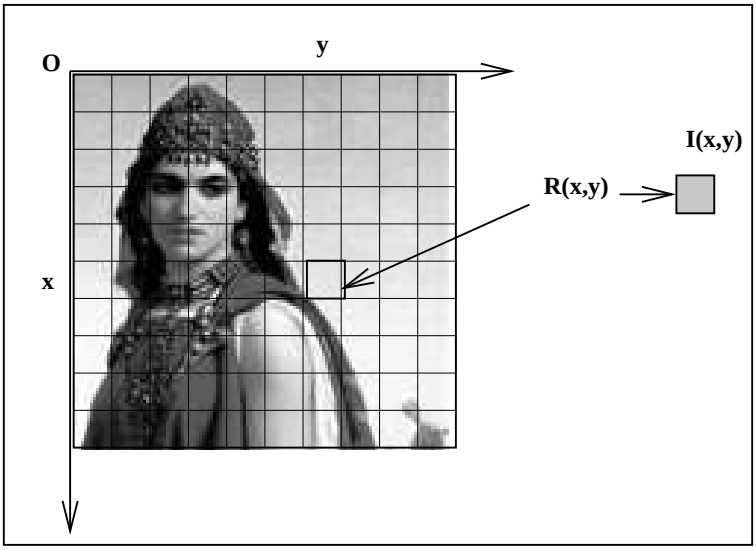


FIG. 1.4 – Échantillonnage, discrétisation spatiale.

– **Quantification :** la quantification désigne la discrétisation tonale correspondant à la limitation du nombre de valeurs différentes que peut prendre chaque pixel.
Idéalement, le nombre de valeurs différentes devrait dépendre de l'amplitude des grandeurs observées (réflectance de la lumière visible, luminance infrarouge, ...) dans la scène. Mais en pratique, le nombre de valeurs utilisées pour coder une image lors de son acquisition dépend de la capacité effective du capteur à observer des signaux de grandeurs différentes, qui s'assimile à un rapport signal sur bruit [77, 61].

1.3.2 Fidélité de la numérisation

La fidélité de la représentation fournie par l'image numérique par rapport à l'image modèle analogique dépend de nombreux paramètres très liés entre eux : la résolution, la définition (dimension de l'image), l'échantillonnage et la qualité de stockage [42].

1.3.2.1 Résolution

La résolution est le nombre de pixels par unité de longueur dans cette image. Plus la résolution est élevée (plus le pas de discrétisation est faible), mieux les détails seront représentés. A titre indicatif, le théorème de Shannon indique qu'il est nécessaire d'utiliser une fréquence d'échantillonnage deux fois plus élevée que celle du signal à représenter. Ce paramètre dépend principalement des caractéristiques du matériel utilisé lors de la numérisation. La résolution d'image se mesure en *dpi*[3].

[3]"dots per inch" équivalent à "pixels par pouce" (ppp).

La résolution standard pour l'affichage Web est de 72 dpi : c'est la résolution maximale supportée par un écran jusqu'à maintenant. A titre informatif, la résolution des images destinées à l'impression est de 150 dpi pour l'impression qualité journal. Cette résolution peut facilement monter jusqu'à 1200 dpi pour une impression en qualité photo [6, 42].

1.3.2.2 Dimension (la définition) de l'image

La définition de l'image est le nombre fixe de pixels qui est utilisé pour représenter l'image dans ses deux dimensions. Pour une image analogique donnée, plus la définition est grande, plus la précision des détails sera élevée. Ce nombre de pixels détermine directement la taille des informations nécessaire au stockage de l'image (du fichier numérique brut). La dimension, en pixels, détermine le format d'affichage à l'écran (la taille des pixels de l'écran étant fixe) [41].

1.3.2.3 Échantillonnage

La quantification détermine la qualité de l'échantillonnage du signal. Celui-ci se mesure en nombre de bits par pixel de l'image (bpp). La précision du rendu colorimétrique de l'image dépend du nombre de niveaux du signal pouvant être codés pour chaque pixel. Les valeurs les plus courantes sont 8 bits/pixel pour les images en niveaux de gris (256 niveaux de gris) et 24 bits/pixels, c'est à dire 8 bits par composante primaire, pour les images en couleur (plus de 16 millions de couleurs distinctes)[42].

1.3.2.4 Qualité de stockage

Le volume des informations qu'il est nécessaire pour stocker une image peut être très important, surtout dans le cas de l'utilisation d'images en haute résolution. Des techniques de compression doivent souvent être mises en place pour diminuer ce volume tout en conservant une certaine qualité de représentation.

Il existe des techniques de compression non destructives (basées sur des compressions de données sans perte d'informations et qui conservent l'intégralité du signal) et des techniques destructives qui augmentent le taux de compression au prix d'une dégradation (généralement paramétrable) de la qualité de l'image. Un exemple de technique de compression destructive couramment utilisée est la compression JPEG [42].

1.4 Codage des images numériques

1.4.1 Codage en noir et blanc

Pour ce type de codage, chaque pixel est soit noir, soit blanc. Il faut un bit pour coder un pixel (0 pour noir, 1 pour blanc). Ce type de codage peut convenir pour un plan ou un texte mais on voit ses limites lorsqu'il s'agit d'une photographie.

La figure 1.5 représente l'image Fatma Nessoumer codée en noir et blanc.

FIG. 1.5 – Image codée en noir et blanc.

1.4.2 Codage en niveaux de gris

Si on code chaque pixel sur 2 bits on aura 4 possibilités (noir, gris foncé, gris clair, blanc). L'image codée sera très peu nuancée.

En général, les images en niveaux de gris renferment 256 teintes de gris. Par convention la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur 255 le blanc (intensité lumineuse maximale). Le nombre 256 est lié à la quantification de l'image. En effet chaque entier représentant un niveau de gris est codé sur 8 bits. Il est donc compris entre 0 et $2^8 - 1$. C'est la quantification la plus courante. On peut coder une image en niveaux de gris sur 16 bits ou sur 1 bit : dans ce dernier cas le «niveau de gris» vaut 0 ou 1 : il s'agit alors d'une image binaire (Noir et Blanc) [6].

La Figure 1.6 illustre l'image Fatma Nessoumer codée en niveaux de gris.

FIG. 1.6 – Image codée en niveaux de gris.

1.4.3 Codage en couleurs 24 bits

Il existe plusieurs modes de codage de la couleur. Le plus utilisé est le codage RGB[4]. Chaque couleur est codée sur 1 octet = 8 bits. Chaque pixel sur 3 octets c'est à dire 24 bits : le rouge de

[4]*Red Green Blue*, également appelé RVB en français (*Rouge Vert Bleu*)

0 à 255 , le vert de 0 à 255, le Bleu de 0 à 255. Le principe repose sur la synthèse additive des couleurs : on peut obtenir une couleur quelconque par addition de ces trois couleurs primaires en proportions convenables. On obtient ainsi 256 x 256 x 256 = 16777216 (plus de 16 millions de couleurs différentes) [67].

C'est ce codage de la couleur qui est utilisé par la plupart des écrans d'ordinateurs actuellement. On constate qu'il est très gourmand en mémoire (Figure 1.7).

FIG. 1.7 – Image codée en couleurs 24 bits.

1.4.4 Codage en couleurs 8 bits

Dans ce cas on attache une palette de 256 couleurs à l'image. Ces 256 couleurs sont choisies parmi les 16 millions de couleurs de la palette RGB. Pour chaque image le programme recherche les 256 couleurs les plus pertinentes. Chaque code (de 0 à 255) désigne une couleur. L'image occupe 3 fois moins de place en mémoire qu'avec un codage 24bits. L'image est moins nuancée : sa qualité est bonne mais moindre [67].

1.5 Représentation de la couleur

L'espace des couleurs primaires RGB est calqué sur notre perception visuelle. Il utilise trois couleurs de base : le rouge ($\lambda = 700nm$), le vert ($\lambda = 546nm$) et le blue ($\lambda = 435,8nm$) ; où λ est la longueur de l'onde.

1.5.1 Synthèse additive de la lumière (mode RGB)

L'image est obtenue par superposition de trois rayonnements lumineux : le rouge (R), le vert (G) et le bleu (B). Dans le cas d'un écran cathodique, ces trois rayonnements sont obtenus en bombardant les luminophores photosensibles de l'écran.

Une image RGB est composée de la somme de trois rayonnements lumineux rouge, vert, et bleu dont les faisceaux sont superposés. A l'intensité maximale, ils produisent un rai de lumière blanche, et à l'extinction une zone aussi noire que l'éclairage ambiant le permet [61, 67].

1.5.2 Synthèse soustractive de la lumière (mode CMJN)

La synthèse soustractive permet de restituer une couleur par soustraction, à partir d'une source de lumière blanche, avec des filtres correspondant aux couleurs complémentaires : Cyan (C), Magenta (M), Jaune (J). Ce procédé est utilisé en photographie et pour l'impression des couleurs.

Si on soustrait la lumière Magenta de la lumière blanche (par exemple par un filtre), on obtient de la lumière verte. Si on soustrait la lumière Cyan, on obtient de la lumière rouge et si on soustrait la lumière jaune, on obtient de la lumière bleue. Si on soustrait à la fois la lumière magenta, Cyan et jaune (par exemple en superposant trois filtres), on n'obtient plus de lumière, donc du noir (que l'on note donc en toute logique :"N", comme Noir) [61, 67].

La gamme des couleurs reproductibles par le mode CMJN est plus restrictive que celle de la gamme RGB. Elle est, de surcroît, particulièrement sensible aux variations inévitables dues aux conditions mécaniques et physiques de l'impression en machine.

1.6 Stockage des images

Il existe de nombreux formats plus ou moins performants et ne permettant pas de faire les mêmes choses. Par ailleurs, certains éditeurs de logiciel créent leur format propriétaire, l'interopérabilité n'étant souvent pas assurée.

Techniquement, on peut distinguer les images matricielles (bitmap) et les images vectorielles. Les premières sont composées d'une matrice de points à plusieurs dimensions. En deux dimensions, cas le plus fréquent, les points sont nommés des pixels tout comme sur un moniteur d'ordinateur.

Les images vectorielles de leur côté utilisent des formules géométriques décrivant le contenu de l'image à afficher. Ainsi au lieu de mémoriser un ensemble de points comme c'est le cas pour l'image matricielle, seront mémorisées les opérations conduisant au résultat. Si cette méthode présente de nombreux avantages, il n'en faut pas moins passer par une conversion de l'image vectorielle en représentation matricielle pour l'afficher sur les moniteurs d'ordinateur actuels [67].

Les applications des images vectorielles sont multiples. Elles sont en effet très utilisées pour des applications de visualisation scientifique ainsi que pour la création Web (format flash), la PAO (Publication Assistée par Ordinateur) et surtout l'illustration. Ceci est en effet dû à plusieurs raisons. La première vient de la taille des fichiers. Ceux-ci sont en effet très peu volumineux en comparaison des images bitmap. La seconde vient de la qualité et de la précision des images. Cela vient de la manière dont sont crées ces images. Comme son nom l'indique une image vectorielle est faite de vecteurs. Ainsi, pour créer une droite, il suffit de déterminer les coordonnées d'un des points de la droite ainsi que son orientation. Pour créer un segment, les coordonnées de début et de fin de segment suffisent. Un cercle sera défini par son centre et son rayon, etc. De même, les couleurs sont réparties en fonction d'équations mathématiques. Si l'on veut faire un dégradé, le principe est le même. Une autre chose très intéressante en dessin vectoriel, c'est que les objets ne s'écrasent pas entre eux. Chaque objet créé existe. Il faut alors définir pour chaque objet sur quelle couche il se situe, les zones dessinées des couches les plus élevées masquant les zones des couches les plus basses. Ceci a comme énorme avantage que si l'on veut modifier des objets ou modifier

la taille de l'image, la qualité restera la même. En effet, il suffit de recalculer les dimensions de chaque objet et les zones de couleur. Ainsi, il n'y a pas de perte d'information [38].

Nous détaillerons dans une première partie les formats d'image matricielle avant d'aborder les formats d'image vectorielle.

1.6.1 Formats d'image matricielle

1.6.1.1 JPEG

Ce format est l'un des plus complexes, son étude complète nécessite de solides bases mathématiques, cependant malgré une certaine dégradation il offre des taux de compressions plus qu'intéressants.

JPEG est la norme internationale (ISO 10918-1) relative à la compression d'images fixes, notamment aux images photographiques. La méthode de compression est "avec pertes" et s'appuie sur l'algorithme de transformée en cosinus discrète DCT. Un mode "sans perte" a ensuite été développé mais n'a jamais été vraiment utilisé. Cette norme de compression a été développée par le comité JPEG (*Joint Photographic Experts Group*) et normalisée par l'ISO/JTC1 SC29. Ce type de compression est très utilisé pour les photographies, car il est inspiré des caractéristiques de perception visuelles de l'œil humain.

Le JPEG2000 est la norme internationale (ISO 15444-1). Elle apporte quelques améliorations au JPEG classique et notamment permet un réglage autorisant une compression sans perte ou encore la résistance aux erreurs de transmission. JPEG 2000 est relative à la compression d'images qui s'appuie sur un mécanisme de compression par ondelettes [40].

1.6.1.2 GIF

Le format GIF pour *Graphical Interchange Format* été créé en 1987 par Compuserve pour que les utilisateurs puissent s'échanger des images de façon efficace et moins onéreuse. Ce format a permet une compression sans perte (algorithme LZW[5]).

Quelques problèmes juridiques avec la société Unisys détenant un brevet sur le LZW et donc revendiquant des royalties sur le GIF ont favorisés le développement de nouveau format a l'instar du PNG. Ces brevets ont aujourd'hui expiré faisant tomber le GIF dans le domaine public.

Ce format fonctionne sur la base d'une palette de 256 couleurs indexées (8 bits), le GIF est de fait limité à seulement 256 couleurs. Il autorise une bonne compression et une décompression très rapide grâce à la méthode LZW. Cette compression est plus efficace pour les dessins et graphiques que pour les photographies numériques [61, 40].

1.6.1.3 PNG et MNG

Le PNG pour *Portable Network Graphic* (ISO 15948) a été développé par le W3C pour remplacer le GIF. Il surpasse ce dernier en ce qu'il n'est notamment pas limité à 256 couleurs. De même,

[5]Lempel-Ziv-Welch

le format est ouvert et permet une bonne compression sans perte. Son utilisation est recommandée à l'instar du GIF pour les petits logos.

Côté photo, s'il permet une compression sans perte, le poids de la photo n'est pas compétitif avec les formats JPEG. Précisons que le PNG ne gère pas l'animation mais un format dérivé, le MNG, y est destiné. Ces formats ne sont pas encore démocratisés, et le MNG notamment nécessite l'adjonction de plugins [40].

1.6.1.4 TIFF

Le TIFF pour *Tagged Image File* a été mis au point en 1987 par la société Aldus (appartenant désormais à Adobe). Les dernières spécifications (Revision 6.0) ont été publiées en 1992.

Le format TIFF est un ancien format graphique, permettant de stocker des images bitmap (raster) de taille importante (plus de 4 Go compressées), sans perdition de qualité et indépendamment des plates formes ou des périphériques utilisés (Device-Independant Bitmap, noté DIB). Il supporte différents types de compression autant avec que sans perte de données.

Le format TIFF permet de stocker des images en noir et blanc, en couleurs réelles (True color, jusqu'à 32 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de couleurs [37].

1.6.1.5 BMP

Le BMP est un des formats les plus simples développé conjointement par Microsoft et IBM, ce qui explique qu'il soit particulièrement répandu sur les plates formes Windows et OS/2.

C'est un format ouvert et non compressé. Sa taille rédhibitoire rend son utilisation en ligne difficile, mais sa grande compatibilité en fait un format de travail efficace. En BMP la couleur est codée en RGB (synthèse additive), le format lui-même supportant la palette 256 couleurs que le « true color » [61, 40].

1.6.1.6 PSD

Le format PSD pour *Photoshop document* (Adobe) est pour sa part très complet mais la taille des fichiers produits rend son utilisation en ligne difficile. Il est donc limité à la retouche d'images et au développement. Il est reconnu par plusieurs logiciels de traitement d'images, du fait de la grande diffusion des produits Adobe dans le domaine d'images numériques. Ce format peut coder la couleur sur 2, 8, 16, 24 et 32 bits, utilisant le mode RGB ou CMJN [40].

1.6.2 Formats d'image vectorielle

1.6.2.1 PICT

PICT pour *Picture* de Apple est obsolète comparé aux autres formats disponibles. Le format PICT est le format standard d'images du monde Macintosh, toutes les applications de dessin sous cet environnement sont généralement capables d'exporter des images dans ce format. Les fichiers

PICT peuvent provenir directement du Macintosh, ou encore être générés par des applications de dessin Windows comme Photoshop ou CorelDraw. L'utilisation du format PICT à l'intérieur de la base de données permet de visualiser ces images à la fois sur Macintosh et sur PC. L'extension des fichiers PICT sous Windows peut être soit PIC, soit PCT, suivant le logiciel ayant généré l'image. Les fichiers PICT sont compressés ou non par QuickTime.

1.6.2.2 PS

PS pour *PostScript* utilisé avec la majorité des applications d'aujourd'hui, autant les logiciels de mise en pages, de traitement de textes et autres, il est possible d'exporter un document en format PS (PostScript) lequel pourra être acheminé vers un périphérique d'impression. Ce format est également une façon sûre de rendre disponible un document seulement pour impression sans droit de modification. Il s'agit toutefois d'un format très lourd à éviter lorsqu'il doit être transféré par Internet sur des liens à basse vitesse.

1.6.2.3 DXF

Le format DXF est un format créé par la compagnie AutoDesk pour son logiciel de CAO AUTOCAD. Bien qu'étant un format très répandu dans le monde de la conception et du dessin assisté par ordinateur, le format DXF est très peu répandu en d'autres domaines.

1.6.2.4 WPG

Le format WPG est un format utilisé par les logiciels de la gamme de WordPerfect (WordPerfect, DrawPerfect, WP Presentations et autres) sous DOS, Windows ou Macintosh. Ce format donne un résultat acceptable lors de l'impression, mais qui doit surtout être utilisé en tant que format de travail. D'autant plus que ce n'est pas un format qui est reconnu par tous les logiciels [61, 40].

1.7 Aspects du traitement d'images

Dans cette section, nous présentons les trois aspects du traitement d'images qui nous intéresses : filtrage, compression et tatouage.

1.7.1 Filtrage

Pour améliorer la qualité visuelle de l'image, on doit éliminer les effets des *bruits* (parasites) en lui faisant subir un traitement appelé *filtrage*.

Le filtrage consiste à appliquer une transformation (appelée *filtre*) à tout ou à une partie d'une image numérique en appliquant un opérateur [41].

Définition 1 ***Filtre***

Un filtre est une transformation mathématique permettant, pour chaque pixel de la zone à laquelle il s'applique, de modifier sa valeur en fonction des valeurs des pixels avoisinants, affectées de coefficients [39].

Le filtre est représenté par un tableau (matrice), caractérisé par ses dimensions et ses coefficients, dont le centre correspond au pixel concerné. Les coefficients du tableau déterminent les propriétés du filtre.

Définition 2 ***Bruit***

Le bruit caractérise les parasites ou interférences d'un signal, c'est-à-dire les parties du signal déformées localement. Ainsi le bruit d'une image désigne les pixels de l'image dont l'intensité est très différente de celles des pixels voisins [39] .

Le bruit peut provenir de différentes causes :
- Environnement lors de l'acquisition ;
- Qualité du capteur ;
- Qualité de l'échantillonnage.

1.7.1.1 Filtre passe-bas (lissage)

Un filtre passe-bas accentue les éléments qui ont une basse fréquence spatiale tout en atténuant les éléments à haute fréquence spatiale (pixels foncés). Il en résulte une image qui apparaît plus homogène (un peu floue) particulièrement en présence d'arêtes. Ce type de filtrage est généralement utilisé pour atténuer le bruit de l'image, c'est la raison pour laquelle on parle habituellement de lissage.

Lors de l'application du filtre, une nouvelle valeur de pixel est générée en tenant compte du voisinage de chaque pixel de l'image originale. Une fenêtre de 3 pixels sur 3 ou plus, sert à prélever les pixels du voisinage dont on utilisera les statistiques. Plus la fenêtre est grande, plus le lissage sera important (ce qui produira une image très floue). En appliquant une pondération aux éléments de la fenêtre, il est possible d'accentuer certains éléments directionnels de l'image. Parce qu'un filtre passe-bas tend à rendre une image plus lisse, les plages de l'image apparaissent plus homogènes. Les filtres passe-bas sont donc très utiles pour réduire le bruit d'une image [6].

Parmi les filtres passe-bas, on cite : les filtres moyenneur, médian et gaussien .

Filtre moyenneur

Ce filtre très simple préserve la radiométrie mais tend à brouiller les parties texturées de l'image. Ce lissage de l'image est souhaitable lorsque l'on applique le filtre en tant que filtre spatial. Les fenêtres de grande dimension reflètent les fréquences spatiales les plus basses alors que les fenêtres plus petites reflètent les fréquences spatiales basses et intermédiaires [35].

Filtre médian

Le filtre médian préserve l'information texturale plus efficacement que le filtre moyenneur. Toutefois, le filtre modifie l'information radiométrique et ne préserve pas la signature des cibles ponctuelles. Lorsqu'on se sert de ce filtre comme filtre spatial, il préserve bien les arêtes tout en lissant des données [35].

Filtre gaussien

Un filtre où tous les éléments du filtre sont pondérés selon une distribution gaussienne (distribution normale). Selon la dimension du filtre, la convolution de ce filtre avec une image donne une image plus ou moins lissée (une petite dimension de filtre donne une image peu lissée) [35].

En pratique, il faut choisir un compromis entre l'atténuation du bruit et la conservation des détails et contours significatifs [41].

1.7.1.2 Filtre passe-haut (accentuation)

Les filtres passe-haut atténuent les composantes de basse fréquence de l'image et permettent notamment d'accentuer les détails et le contraste, c'est la raison pour laquelle le terme de "filtre d'accentuation" est parfois utilisé [39]. Ce filtre n'affecte pas les composantes de haute fréquence d'un signal, mais doit atténuer les composantes de basse fréquence .

Un filtre passe haut favorise les hautes fréquences spatiales, comme les détails, et de ce fait, il améliore le contraste. Toutefois, il produit des effets secondaires [6] :

- Augmentation du bruit : dans les images avec un rapport Signal/Bruit faible, le filtre augmente le bruit granuleux dans l'image.
- Effet de bord : il est possible que sur les bords de l'image apparaisse un cadre. Mais cet effet est souvent négligeable et peut s'éliminer en tronquant les bords de l'image [6].

1.7.1.3 Filtre passe-bande (différentiation)

Cette opération est une dérivée du filtre passe-bas. Elle consiste à éliminer la redondance d'information entre l'image originale et l'image obtenue par filtrage passe-bas. Seule la différence entre l'image source et l'image traitée est conservée [41]. Les filtres différentiels permettent de mettre en évidence certaines variations spatiales de l'image. Ils sont utilisés comme traitements de base dans de nombreuses opérations comme le rehaussement de contraste ou la détection de contours [6].

1.7.1.4 Filtre directionnel

Dans certains cas, on cherche à faire apparaître des détails de l'image dans une direction bien déterminée. Pour cela, on utilise des filtres qui opèrent suivant des directions (horizontales, verticales et diagonales) [41].

1.7.2 Compression

Certes, les capacités de disques durs de nos ordinateurs et le débit des réseaux ne cessent d'augmenter. Mais notre utilisation de l'image et les capacités d'acquisition des capteurs numériques s'accroissent tout autant.

De nombreux autres appareils numériques ont fais leurs apparitions. Il ne faut pas parler uniquement de mémoire pour un ordinateur mais également pour un assistant personnel (PDA), pour un téléphone portable, un GPS, un appareil photo numérique, etc., et les applications actuelles

n'envisagent plus de se passer de l'image. Une page web sans image, l'imaginez-vous encore ? A quand la disparition du SMS pour le MMS ? Acceptez-vous d'attendre avant de commencer à visualiser un film acheté sur un service de vidéo à la demande sur Internet ?

Dans d'autres domaines professionnels tels que l'imagerie médicale, des masses gigantesques de données sont acquises chaque jour. On chiffre à environ dix téraoctets la masse de données produites annuellement dans un service radiologique d'un hôpital dans un pays industrialisé. La compression d'images est donc encore plus d'actualité aujourd'hui [61].

1.7.2.1 Objectif de la compression

En fonction de l'application recherchée, différentes qualités vont être demandées à un algorithme de compression. Parmi elles, on cite la rapidité de la compression et de la décompression. En effet, il serait dommage, dans une application de transmission, que le temps gagné par une réduction de la taille des données à transmettre soit inférieur au temps passé à la compression ou décompression. Cette qualité sera cependant moins cruciale dans des applications visant à l'archivage de données.

Viennent ensuite deux qualités antagonistes : le taux de compression et la qualité de l'image après un cycle de compression/décompression. Il existe des algorithmes de compression sans pertes mais dont le taux de compression est limité. Les algorithmes avec perte d'informations peuvent obtenir de meilleurs taux de compression mais en jouant sur les dégradations. Selon l'application visée, on voudra obtenir une qualité suffisante pour distinguer certaines informations, ou bien une qualité visuelle parfaite du point de vue d'un humain, ou bien encore conserver la qualité la meilleure possible afin de pouvoir effectuer des traitements ultérieurs sur l'image et éviter des artefacts dûs à la compression [61].

1.7.2.2 Notions générales

Définition 3 ***Histogramme***

Dans une image en niveaux de gris, l'histogramme comptabilise le nombre d'occurrences de chacune des valeurs. En couleur, l'histogramme peut être réalisé sur les indices de couleurs dans des systèmes de couleurs indexées ou bien nécessite plusieurs histogrammes sur chacune des composantes du système de représentation de couleur [41, 61].

Un histogramme permet d'obtenir des informations sur la répartition des intensités comme la moyenne ou la variance . Par contre, un histogramme ne fournit aucune information de répartition spatiale. Ainsi, deux images peuvent posséder le même histogramme sans pour autant se ressembler. De même, un histogramme est invariant aux transformations réarrangeant les pixels (par exemple les symétries).

Définition 4 ***Taux de compression***

Le taux de compression est défini comme le rapport du nombre de bits utilisés par l'image originale et du nombre de bits utilisés par l'image compressée. Les méthodes réversibles ont un taux de compression entre 1 et 2.5, tandis que les méthodes irréversibles prouvent voir de bien meilleurs taux de compression mais avec une distorsion [61].

1.7.2.3 Quelques idées pour la compression

Les principales idées pour la compression sont basées sur :

- La quantification des niveaux de gris ou composantes couleurs ou bien des coefficients dans les images transformées ;
- La mémorisation des occurrences (on remplace la chaîne 00000 par 5 0) ;
- Le codage des valeurs avec un code de longueur inversement propositionnelle aux occurrences [61].

On cite deux algorithmes de codage largement utilisés : codage d'Huffman et le codage LZW.

Codage d'Huffman

Le Codage de Huffman est basé sur le principe suivant : coder ce qui est fréquent sur moins de bits que ce qui n'est pas fréquent. Les pixels sont regroupés par blocs de L pixels puis, la probabilité des différentes niveaux de gris du bloc est estimée.

A un niveau donnée m, on combine deux symboles de probabilités minimales. On obtient alors un ensemble de niveau $m-1$ comportant un élément de moins.

Le code de chaque élément est identique, sauf pour les combinaisons. Les codes associés aux deux caractères combinés à un niveau m sont obtenus à partir de leur code au niveau inférieur $(m-1)$ auquel on joute 0 et 1 [61].

Codge LZW (Lempel-Ziv-Welch)

En 1977, Lempel et Ziv créèrent l'algorithme de compression LZ77, évoluant l'année d'après en LZ78. Welch, de la société Unisys, modifia l'implémentation de ce codage LZW. Autant les précédentes peuvent être utilisées librement, autant le LZW fait l'objet de plusieurs brevets dont certains pourraient le bientôt expirer.

Le principe de codage est similaire pour LZ77, LZ78 et LZW. Il s'agit d'une compression sans pertes qui fonctionne bien pour les images de grandes zones homogènes. Considérant les pixels comme un tableau mono dimensionnel, l'algorithme est basé sur le découpage de l'ensemble des pixels en mots les plus longs possibles. Chaque mot, quelque soit sa longueur, se voit attribuer un code de taille fixe. Le tableau étant mono dimensionnel, les redondances verticales ne sont pas prises en compte.

L'algorithme d'Huffman attribue des codes de longueurs variables en fonction de l'occurrence des éléments. L'algorithme de LZW, quant à lui, attribue des codes de longueur fixe à des chaînes d'éléments de taille variables [61].

1.7.3 Tatouage numérique

L'idée de base du tatouage numérique est de cacher dans un document numérique une information subliminale (i.e. invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, traçabilité, non répudiation, etc.) ou à but d'information [84]. Le principe et les notions liées à ce traitement sont bien détaillés dans le chapitre suivant.

1.8 Conclusion

Dans ce chapitre, nous avons présenté les images numériques d'une manière générale. Nous nous sommes intéressés aux terminologies et aux notions pertinentes dans le domaine des images numériques telles que la numérisation, le codage, le stockage. Nous avons également présenté quelques aspects du traitement d'image, tels que le filtrage, la compression et le tatouage, et c'est ce dernier qui est présenté le long de ce mémoire.

Chapitre 2

Tatouage numérique, concepts de base et terminologies

Résumé : Le « digital watermarking » ou tatouage numérique a connu, ces dernières années, un essor spectaculaire. Initialement développé pour renforcer la protection des droits d'auteur des documents multimédia, il tend de plus en plus a être utilisé pour remplir d'autres fonctions de sécurité, notamment des fonctions d'intégrité, ou des services d'information.

L'objectif de ce chapitre est de présenter les aspects principaux et les méthodes liées aux évolutions des technologies traitées dans le contexte de ce mémoire. Mais en se concentrant principalement sur le tatouage invisible des images numériques.

2.1 Introduction

La révolution numérique, l'explosion des réseaux de communication et l'engouement sans cesse grandissant du grand public pour les nouvelles technologies de l'information entrainent une circulation accrue des documents multimèdia (images, vidéos, textes, sons, etc.). L'ampleur de ce phènoméne est telle que des questions essentielles se posent désormais quant à la protection et au contrôle des données échangées. En effet, de par leur nature numérique, les documents multimédia peuvent être dupliqués, modifiés, transformés et diffusés très facilement. Dans ces conditions, il devient donc nécessaire de mettre en oeuvre des systèmes permettant de faire respecter les droits d'auteur, de contrôler les copies et de protéger l'intégrité des documents.

La cryptographie a été une première proposition pour sécuriser des transferts de documents numériques. Aujourd'hui les algorithmes de cryptage modernes, avec des clés de longueur importante, permettent d'assurer la confidentialité. Néanmoins, une fois décrypté, le document n'est plus protégé et il peut être distribué ou modifié malhonnêtement. La dissimulation d'information, et plus particulièrement l'insertion de données cachées peut être une réponse à ce problème. En effet, l'insertion d'un watremark dans un document permet de l'authentifier et de garantir son intégrité [85].

Dans ce contexte, plusieurs techniques de dissimulation d'information ont été proposées dans la littérature. Les techniques les plus connues sont la stéganographie et le tatouage.

La stéganographie cherche à cacher un message secret dans un médium de sorte que personne ne puisse distinguer un médium vierge d'un stégo-médium. La nature de l'information dissimulée ne revêt pas d'importance : il peut tout aussi bien s'agir d'un texte en clair que de sa version chiffrée. Ce message n'a priori aucun lien avec le stégo-médium qui le transporte.

Le tatouage cherche à répondre au problème de la protection des droits d'auteur.Il s'agit bien de dissimulation d'information puisque, pour y parvenir, on insère un watermark dans le médium spécifique au propriétaire. Comme celui-ci souhaite protéger son médium et non une version trop déformée, l'insertion doit minimiser les modifications subies par le médium afin d'être imperceptible. Ici, la dissimulation ne signifie pas la même chose qu'en stéganographie : un attaquant sait qu'un tatouage est présent dans le document tatouée, mais cette connaissance ne doit cependant pas lui permettre de le retirer.

Parmi les applications s'intéressant à l'art de dissimulation d'information, on peut citer :

- Les agences militaire qui exigent des communications secrètes. Par exemple, même si le contenu est chiffré, la détection d'un signal sur un champ de bataille moderne peut conduire rapidement à une attaque sur le signaleur. Pour cette raison, les communications militaires utilisent des techniques telles que la modulation d'étalement de spectre pour rendre difficile à l'ennemi de détecter ou modifier les signaux.
- Les criminels imposent une grande importance à la discrétion des communications. Leurs technologies préférées comprennent entre autres les téléphones mobiles prépayées, les téléphones mobiles qui ont été modifiés pour changer fréquemment leur identité et le piratage des tableaux de distribution d'entreprise par lesquels les appels peuvent être déroutés.
- Les agences d'application de la loi et de renseignement sont intéressées à la compréhension de ces technologies et leurs faiblesses, afin de détecter et de tracer des messages cachés.
- Les schémas numériques pour les élections et le paiement numériques font usage des techniques de communication anonyme [79].

Dans le contexte de notre travail on s'intéresse au tatouage numérique (digital watermarking en Anglais). Cette technologie est très rapidement apparue comme la solution « alternative » pour renforcer la sécurité des documents multimédia. L'idée de base du « watermarking » est de cacher dans un document numérique une information invisible ou inaudible suivant la nature du document permettant d'assurer un service de sécurité (copyright, intégrité, traçabilité, non répudiation, etc.) ou à but d'information.

Dans ce qui suit, des concepts de base liés à cette nouvelle technologie seront présentés.

2.2 Historique et Terminologies

2.2.1 Historique

Les tatouages du papier sont apparus dans l'art de la fabrication du papier il y a presque 700 ans. Le plus ancien document tatoué trouvé dans les archives remonte à 1292 et a son origine dans la ville de Fabriano en Italie qui a joué un rôle important dans l'évolution de l'industrie papetière.

A la fin du troisiéme siècle, environ 40 fabricants du papier partageaient le marché du papier. La concurrence entre ces fabricants était très élevée et il était difficile que n'importe quelle partie

maintienne une trace de la provenance du papier et ainsi que son format et sa qualité. L'introduction des tatouages était la méthode parfaite pour éviter n'importe quelle possibilité de confusion.

Après leur invention, les tatouages se sont rapidement étendus en Italie et puis en'Europe et bien qu'au commencement utilisé pour indiquer la marque ou le fabricant du papier, ils ont servi plus tard pour indiquer le format, la qualité, et la force du papier, et ont été également employés comme une base pour dater et authentifier le papier [89, 79].

L'analogie entre le tatouage du papier et le tatouage numérique[1] est évidente : les tatouages du papier des billets de banque et de timbres ont inspiré la premiére utilisation du terme «Marque d'eau»[2] dans le contexte de données numériques. Les premiéres publications portant sur le tatouage d'images numériques ont été publiés par Tanaka et al. [95] en 1990 et par Tirkel et al. [96] en 1993.

En 1995, le temps est évidemment bien de prendre ce sujet, et il a commencé à stimuler l'augmentation des activités de recherche. Depuis 1995, le tatouage numérique a gagné beaucoup d'attention et a évolué très rapidement et alors qu'il y a beaucoup de sujets ouverts pour davantage de recherches, des méthodes de travail et des systèmes pratiques ont été développés, dont certains sont présentés dans le Chapitre 3 et 4.

2.2.2 Terminologies

2.2.2.1 Tatouage visible et invisible

On distingue généralement deux classes du tatouage : visible et invisible.

L'idée derrière le tatouage visible est très simple. Il est équivalent à l'estampage d'un watremark sur le papier, et pour cette raison il est appelé parfois estampage numérique. Le tatouage visible altère le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre). Il est fréquent que les agences de photo ajoutent un watermark visible en forme de copyright (©) aux versions de pré-visualisation (basse résolution) de leurs photos. Ceci afin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watremark est visible, alors elle peut être facilement attaquée. Néanmoins, nous trouvons des applications qui demandent que le watremark soit visible, c'est le cas du logo des sociétés dans les programmes télévisuels. Dans la catégorie du tatouage visible, nous distinguons les travaux [75, 43, 74, 46].

En revanche, le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le signal d'une manière imperceptible par l'utilisateur final. Pour reprendre l'exemple de l'agence de photo, les photos hautes résolutions vendues par l'agence possèdent elles au contraire un watermark invisible, qui ne dégrade donc pas le contenu visuel, mais qui permet de détecter

[1] Le terme tatouage numérique est originaire du Japon : denshi sukashi qui se traduit en anglais par electronic watermark.

[2] Les fibres sont marquées au moment de la sortie du bain d'eau, ce qui est à l'origine du terme anglais water mark.

l'éventuelle source d'un vol. Le message caché par le tatouage peut être un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur [89, 47].

Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs [109, 108, 71]. La majorité des techniques concernant la protection de propriété intellectuelle suit la branche du tatouage invisible.

Dans ce qui se suit, nous nous concentrons sur cette dernière catégorie, et le mot "Tatouage" est pris au sens du tatouage invisible.

2.2.2.2 Définitions

Le tatouage numérique est l'un des concepts techniques qui soulève la problématique et permet à chacun de donner sa définition, et en raison de l'absence d'une définition normalisée, nous présentons quelques définitions parmi plusieurs, proposées par différents auteurs du domaine informatique, électronique ou autre.

Définition Miller et Cox 1997

Le tatouage numérique signifie l'incorporation d'une information numérique dans un contenu multimédia, comme une vidéo, un audio ou une image de telle manière que l'information insérée doit être imperceptible pour un observateur humain, puis à tenter de la récupérer aprés que le document tatoué ait éventuellement subi des manipulations de nature variée [15].

Définition Kundur et Hatzinakos 1998

Le processus du tatouage numérique implique la modification des données multimédia originales pour insérer un watremark contenant des informations clés telles que le codes d'authentification ou de droit d'auteur. La méthode d'insertion doit conserver les données originales visuellement inchangés, mais d'imposer des modifications qui peuvent être détectés à l'aide d'un algorithme d'extraction. Les types de signaux à tatouer sont des images, le son, vidéo et le texte [51].

Définition Petitcolas, Anderson et Kuhn 1999

Le tatouage numérique signifie l'intégration d'une information dans un document numérique de façon à ce que cette information soit imperceptible pour un observateur humain, mais facilement détectée par l'ordinateur . Le watremark est une information transparente, invisible qui est inséré dans un document source en utilisant un algorithme informatique [79].

Définition Christian REY et Jean-Luc DUGELAY 2001

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (i. e, invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc.) ou à but d'information. Une des particularités du tatouage numérique par rapport à d'autres techniques, comme par exemple un stockage simple de l'information dans l'en-tête du fichier, est que le watremark est lié de manière intime et résistante aux données. De ce fait, le tatouage est théoriquement indépendant du format de fichier et il peut être détecté ou extrait même si le document a subi des modifications ou s'il est incomplet [84].

Définition Chun-Shien Lu 2004

Le tatouage numérique est un signal intégré de façon permanente dans des données numériques

(audio, image, vidéo et texte) qui peut être détecté ou extrait plus tard par l'execution d'un algorithme informatique afin de faire des affirmations sur les données. Le tatouage est caché dans le document hôte de telle manière qu'il est inséparable des données et qu'il est résistant à de nombreuses opérations, sans dégrader la qualité du document hôte. Ainsi, par le biais du tatouage, le travail est encore accessible, mais définitivement marqué [66].

Quelque soit la manière d'exprimer la définition de la technique du tatouage, son principe et ses exigences restent les mêmes. Dans les sections suivantes, nous présentons ce principe (à travers un modèle générique) et les exigences d'une technique du tatouage invisible.

2.3 Modèle générique du tatouage

Le schéma du tatouage numérique est résumé dans la figure 2.1 . Le système typique du tatouage numérique comprend deux sous-systèmes : le sous-système d'insertion du watermark (appelé aussi la phase de codage) et le sous-système de détection/extraction (appelé aussi la phase de décodage).

Le sous-système d'insertion (Embedding) comprend en entrée un watermark W, un document hôte (porteur) I et une clé secrète K spécifique au tatoueur. Cette dernière est utilisée pour renforcer la sécurité de tout le système.

La phase d'insertion génère en sortie un document tatoué I_w. Cette phase est modèlisée par la fonction suivante :

$$I_w = E(I, W, K). \tag{2.1}$$

Le document tatoué I_w est en suite copié et attaqué, ce qui est modèlisé par la transmission dans un canal soumis à bruit. Le document reçu est appelé I_w^*. La réception du document consiste en deux parties : d'une part la détection du watermark et d'autre part, s'il est présent son décodage (extraction).

La phase de détection/extraction prend en entrée le document tatoué et éventuellement attaqué I_w^* et la clé K et éventuellement (dépend de la méthode utilisée) le document original I et/ou le watermark originel W.

La phase de détection consiste à prouver la présence d'un watermark en utilisant une mesure de confidentialité ρ. Elle est modélisée par la fonction :

$$\rho = D(I_w^*, K, ..). \tag{2.2}$$

La phase d'extraction consiste à calculer une estimation $W^{'}$ de W. Elle est modélisée par la fonction :

$$W^{'} = D(I_w^*, K, ..). \tag{2.3}$$

I et W sont des paramètres optionnels pour la fonction D [79, 114].

Pour un système de tatouage typique, plusieurs conditions doivent être satisfaites :

– Le watremark $W^{'}$ doit être détecté à partir de I_w avec/ou sans la connaissance explicite du I.
– Si I_w n'est pas modifié (attaqué) , alors $W^{'}$ correspond exactement à W .

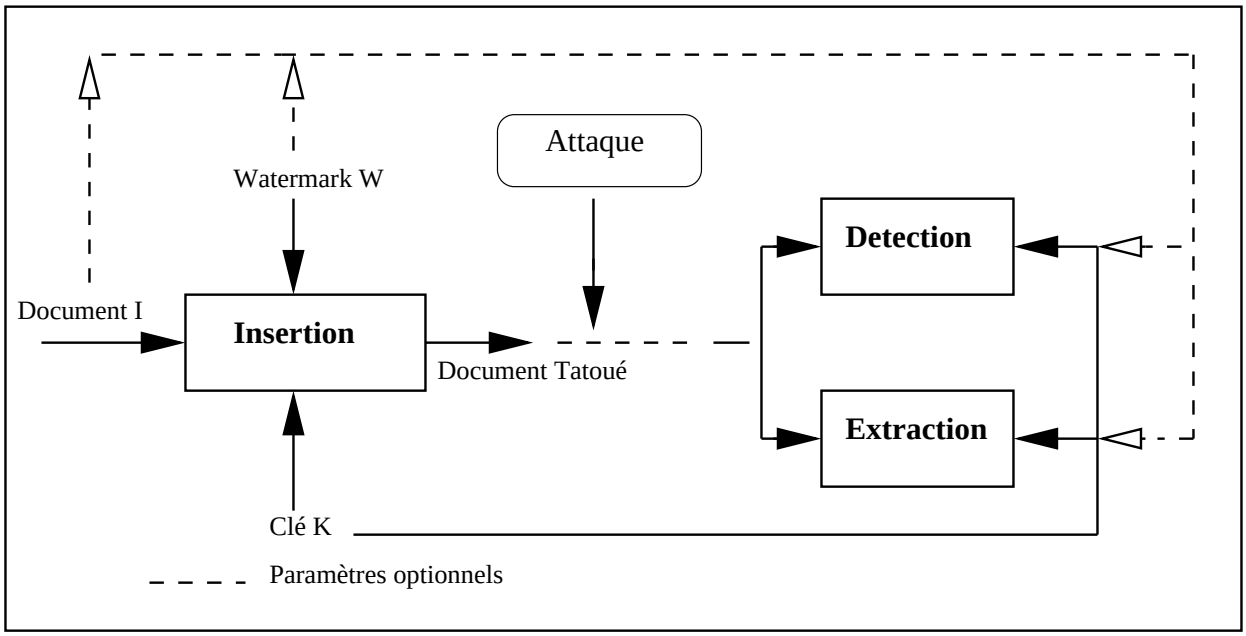


FIG. 2.1 – Modèle générique d'un système du tatouage.

– Pour un tatouage *robuste*, si I_w est attaqué, $W^{'}$ doit correspondre à W, pour donner un jugement clair de l'existence du watremark.
– Pour un tatouage *fragile*, $W^{'}$ doit être significativement ou totalement différente à W, après des petites modifications de I_w.

Zheng et al. [114] classent le tatouage numérique en différentes classes selon le document hôte utilisé pour insérer le watremark.

– **Tatouage numérique d'images :** La plupart des recherches sur le tatouage numérique sont sur les images numériques. Cela peut être dû au fait qu'il y a autant d'images disponibles sur le World Wide Web gratuit et sans aucune protection du droit d'auteur.
– **Tatouage numérique de la Vidéo :** Une séquence vidéo comprend des images fixes. Par conséquent, toutes les méthodes de tatouage sur l'image peuvent être appliquées sur la vidéo. Toutefois, le tatouage numérique de la Vidéo a d'autres problèmes. Par exemple, Zhao et al.[113] ont fait remarquer qu'il est dangereux d'utiliser la même clé du tatouage pour l'ensemble des images de la vidéo. Si la même clé est utilisée pour toutes les images dans une séquence vidéo, l'algorithme du tatouage serait vulnérable aux attaques.
– **Tatouage numérique du son :** Dans le cas des signaux audio, le terme "Tatouage" peut être défini comme la transmission robuste et inaudible de données supplémentaires avec les signaux audio. Le tatouage audio est basé sur l'approche psycho-acoustique des techniques de codage audio.

Dans le reste de ce mémoire, nous nous focalisant sur le tatouage d'images numériques.

2.4 Conditions requises pour les techniques du tatouage d'images numériques

Les méthodes du tatouage requirent différentes propriétés selon leurs domaines d'application et leurs finalités. Le watermark caché dans une image doit remplir certaines conditions essentielles :

2.4.1 Imperceptibilité

Le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée. Cox et al. [17] définissent l'imperceptibilité[3] en tant que similitude visuelle entre la version originale et les versions tatouées.

Le watermark inséré doit être entiérement invisible par le système visuel humain (SVH). L'opération d'insertion ne doit pas détériorer l'image hôte de façon perceptible, c'est à dire l'image tatouée doit être visuellement équivalente à l'image originale. Non seulement, il ne faut pas dénaturer l'image, mais en plus si le watermark est visible, il pourrait être facilement éliminé.

2.4.2 Robustesse et fragilité

L'image tatouée pourrait être modifiée, elle peut être attaquée, dans le but de corrompre ou de supprimer le watermark, mais des opérations usuelles telles que la compression, l'impression, la dégradent également. Le watermark doit être suffisamment résistant à ces attaques pour rester lisible. Cox et al. [17] définissent la robustesse comme capacité de détecter le watermark après des opérations de traitement des signaux.

D'une autre façon, la robustesse est l'aptitude à préserver le watermark face aux attaques. Le tatouage est même modélisé comme un jeux entre le tatoueur et l'attaquant.

La robustesse correspond donc à la quantité d'énergie que possède le watermark insérée. Un watermark de forte énergie est robuste. Cette exigence est fortement attachée à la plupart des types du tatouages, particulièrement ceux pour la protection des droits d'auteur. Mais elle n'existe bien sûr pas dans le cas où l'on veut un watermark fragile pour vérifier que l'image n'a pas été modifiée.

Il est neanmoins interessant de remarquer qu'il peux être utile, dans certain cas, de favoriser une fragilité plutot qu'une robustesse. Pour s'assurer par exemple de l'integrité d'un document, le fait de tatouer avec un algorithme fragile permettra, par la suite de verifier si l'information tatouée est toujours presente, ce qui sous entends donc qu'elle n'a subit aucune modification malveillante.

2.4.3 Sécurité

La sécurité constitue une troisième contrainte indépendante des deux premières. Elle concerne par exemple la génération de la clé secréte, ainsi que le protocole d'échange général. La méthode du tatouage doit également respecter le principe suivant énoncé par Kerckhoff : "l'algorithme lui-même doit pouvoir être rendu public, la sécurité ne dépendant pas de son caractère secret". Cela

[3]Dans certaines références on trouve les termes : Invisibilité, Transparence ou fidélité.

signifie que l'efficacité d'un algorithme du tatouage ne peut pas être fondée sur l'hypothèse que les attaque possibles ne savent pas le processus du tatouage [94].

2.5 Taxonomie des techniques du tatouage numérique

Cette section n'a pas pour objectif de dresser une revue exhaustive de toutes les techniques disponibles dans la littérature. Néanmoins, nous décrivons les grandes lignes de certaines catégories du tatouage numérique dans le but de montrer à quel point le sujet est vaste. Pour plus de détails sur les techniques du tatouage, le lecteur peut se référer à : [44, 47, 15, 27, 89, 47, 66].

Une taxinomie des techniques de tatouage est présentée sur la base de plusieurs publications récentes. La raison de cet arrangement est de fournir une vue générale de plusieurs principaux domaines du tatouage. Nous avons choisit trois critères pour regrouper les techniques du tatouage : le *type de l'algorithme*, le *domaine d'insertion* et le *champ d'application* (voir la figure 2.2).

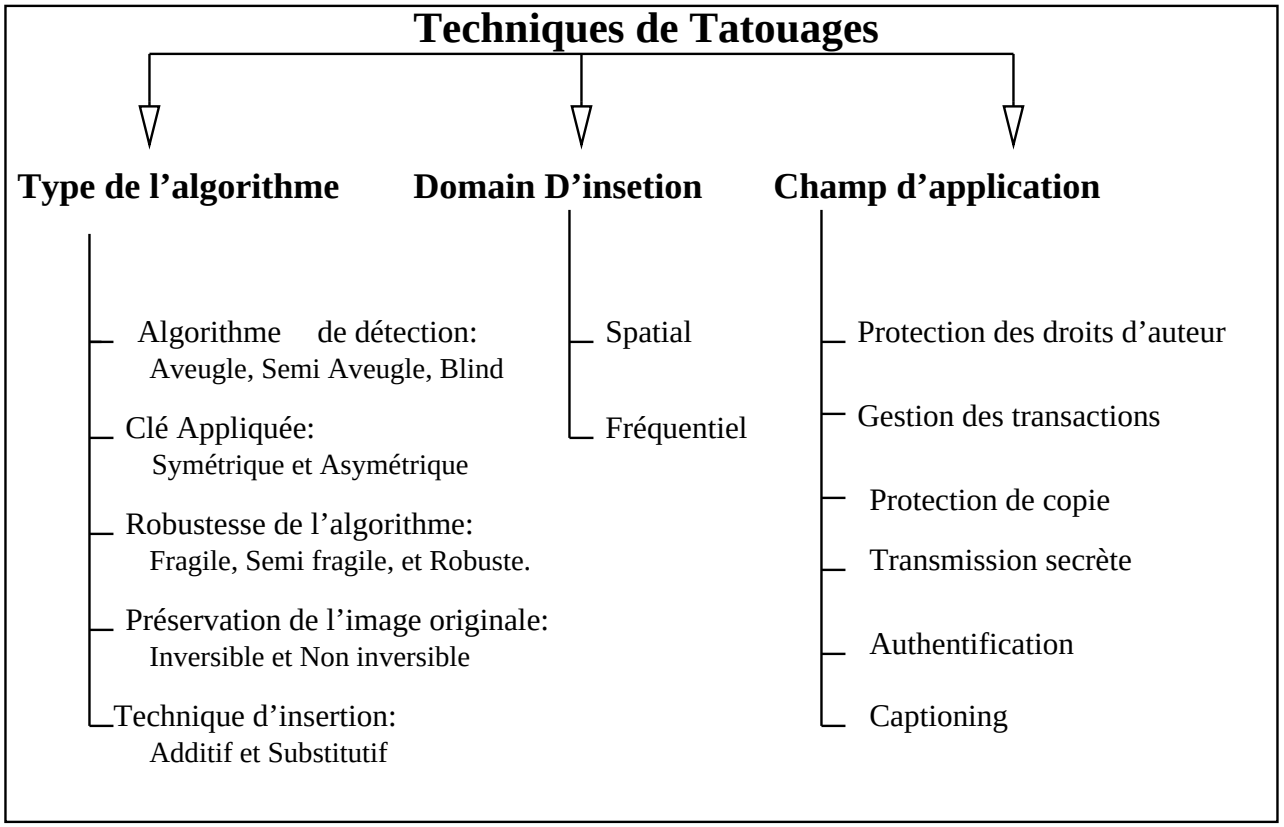


FIG. 2.2 – Taxonomie des techniques du tatouage numérique.

2.5.1 Classification selon le type de l'algorithme

Il est aussi possible de grouper les techniques du tatouage selon différents critères : conformément au type de clé appliquée (asymétrique et symétrique) ; selon l'information nécessaire à l'extraction (aveugle, semi-aveugle et non-aveugle) ; conformément à la robustesse (fragile, semi-fragile et robuste) ; selon la préservation de l'image originale (inversible et non-inversible) et conformément à la technique d'insertion (additive et substitutive). [17, 20] ont bien détaillé dans leurs livres ces types de classifications.

2.5.1.1 L'algorithme de détection : Aveugle, Semi-aveugle et Non aveugle

Le tatouage aveugle est la plus ancienne forme du tatouage. Il n'oblige pas l'extracteur d'avoir connaissance de l'image originale, ni du watermark. Seule l'image tatouée et la clé secréte doivent être disponibles au moment de l'extraction. En se basant sur le modèle générique présenté dans la section 2.3, la fonction d'extraction est modélisée comme suit :

$$W^{'} = D(I_w^*, K). \tag{2.4}$$

Dans cette catégorie de techniques, on peut citer les travaux : [110, 9].

Dans le cadre d'un système semi-aveugle, nous avons besoin d'informations supplémentaires pour aider la détection ou l'extraction. Cette demande est dûe à la perte de synchronisation à cause de canal bruité ou de la technique d'insertion. La phase d'extraction peut require le watermark ou l'image tatouée (l'image originale juste après l'incrustation du watermark). En se basant sur le modèle générique présenté dans la section 2.3, la fonction d'extraction est modélisée comme suit :

$$W^{'} = D(I_w^*, K, W, I_w). \tag{2.5}$$

Dans cette catégorie de techniques, nous pouvons citer les travaux [24, 64].

Au contraire du tatouage aveugle, les algorithmes de marquage non-aveugle nécessitent toujours l'image originale. En se basant sur le modèle générique presenté dans la section 2.3, la fonction d'extraction est modélisée comme suit :

$$W^{'} = D(I_w^*, K, I). \tag{2.6}$$

Dans cette catégorie de techniques, on peut citer les travaux : [23, 87].

Le nombre d'algorithmes non-aveugle n'est pas important par rapport aux nombreux algorithmes semi-aveugles et aveugles. Ceci est dû au fait que la disponibilité des données originales au moment de l'extraction du watermark, ne peut pas toujours être garantie.

Les termes tatouage aveugle, semi aveugle et non aveugle peuvent être désignés respectivement par tatouage publique, semi-privé et privé dans certains articles [79, 53].

2.5.1.2 La clé appliquée : Asymétrique et Symétrique

Le tatouage asymétrique repose sur l'utilisation de deux clés : une clé K_s privée pour l'insertion et une clé K_p publique pour la détection. K_p est issue de K_s par une transformation non inversible.

N'importe quel utilisateur peut détecter le watermark en connaissant K_p, mais seul la connaissance de K_s permet d'enlever ou modifier le watermark[102, 48].

Dans le tatouage symétrique les paramètres utilisés pour insérer le watermark sont les mêmes que pour l'extraire. Le rôle de clé-privée et clé-publique n'existe pas, l'insertion et l'extraction sont faites à l'aide de la même clé et procédure [91].

Les termes tatouage asymétrique et symétrique peuvent être nommés respectivement tatouage à clé publique, et à clé privée dans certains articles [79, 53].

2.5.1.3 La robustesse de l'algorithme : Fragile, Semi-fragile et Robuste

Dans le tatouage fragile, le watermark est fortement sensible aux modifications de l'image tatouée. Cette approche sert à prouver l'authenticité et l'intégrité d'un fichier tatoué [105, 111] .

Le tatouage semi-fragile a pour objectif de reconnaître les perturbations mal intentionnées et de rester robuste à certaines classes de dégradations légères de l'image, comme la compression avec pertes par exemple. Diverses méthodes d'authentification d'images par tatouage semi-fragile ont été proposées [68].

Le tatouage robuste dispose d'un large champ de théories et de résultats. Celui-ci cherche à préserver les données cachées face aux attaques. Le watermark doit donc être suffisamment résistant aux attaques afin de rester identifiable [33, 57, 72, 92].

2.5.1.4 La préservation de l'image originale : Inversible et Non-inversible

Le tatouage inversible permet de récupérer toutes les propriétés originales de l'image hôte après l'extraction du watermark [112, 56].

Dans le tatouage non-inversible, l'image originale est définitivement altérée par le mécanisme d'insertion du watermark. La matrice originale de pixels est irrécupérable. La plupart des méthodes citées jusqu'ici sont non-inversibles.

2.5.1.5 La technique d'insertion : Additif et Substitutif

Dans le tatouage additif, le message à ajouter n'est pas corrélé à l'image hôte. La plupart des techniques du tatouage aveugle sont basées sur une insertion additive [2, 3].

Le tatouuage substitutif modifie les bits de l'image hôte afin de les faire correspondre au watermark. Ce type de marquage est connu comme tatouage par contrainte, parce qu'il force l'image hôte à respecter certaines propriétés qui déterminent le watermark [45, 22].

2.5.2 Classification selon le domaine d'insertion

Les techniques courantes décrites dans la littérature peuvent être regroupées en deux principales classes : techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

2.5.2.1 Domaine Spatial

Dans les techniques spatiales, le watermark est inséré en modifiant directement les valeurs de pixels de l'image hôte. Ce sont des méthodes simples et peu couteuses en temps de calcul. Elles sont consacrées aux tatouages en temps réel demandés dans des environnements de faible puissance. Certaines techniques dans le domaine spatial peuvent être robustes aux attaques de type transformations géométriques [19, 78, 100].

La plus part des techniques spatials sont basées sur l'addition d'une séquence pseudo-bruit (PN) d'amplitude fixe. Dans ce cas les fonctions D et E (introduites dans la section 2.3) sont simplement des opérations d'addition et de soustraction, respectivement.

Plusieurs méthodes, proposées dans la littérature, modifient les bits de poids faible LSB de l'image hôte. L'invisibilité du watermark est obtenu par l'hypothèse que les données contenus dans les bits LSB sont visuellement insignifiantes. Le watermark est généralement inséré en utilisant la connaissance de la séquence PN (et peut être la connaissance d'une clé secrète, comme la location du watermark).

Deux techniques LSB sont proposées par Schyndel et al. [88]. La première remplace les LSB de l'image hôte par la séuennce PN, et la deuxième ajoute la séquence PN aux bits LSB.

Brassil et al. [8] marquent des images contenant du texte en modifiant très légèrement l'espacement vertical entre deux phrases, l'espacement horizontal entre deux mots, et la forme de certains caractères du texte. Ils incluent un message dans le texte, pour empêcher la copie ; ce message peut être retrouvé par comparaison avec le document original. Cependant, il est assez facile de détruire un tel watermark.

Bender et al. [4] proposent un algorithme du tatouage à réponse binaire. Le principe de cette méthode est de sélectionner, à l'aide d'une clé secrète K, une séquence S_a de n couples de pixels (A_i, B_i), puis de modifier très légèrement l'image en augmentant d'une unité le niveau de gris des pixels de type A_i et en diminuant d'un niveau de gris les pixels de type B_i. Considérons la somme S des différences de luminance des couples de pixels sélectionnés. Une personne ne disposant pas de la clé sera incapable de régénérer la bonne séquence S_a et obtiendra $S = 0$. Seule la personne disposant de la clé sera en mesure d'obtenir la bonne valeur de S, c'est-à-dire $2 * n$.

Cette méthode de base n'est bien sûr pas très robuste. Cependant, différentes extensions de cet algorithme ont vu le jour [81, 55].

Dans [52], Kutter et al. travaillent sur des images en couleurs, dans lesquelles ils veulent inclure un watermark binaire, composé de bits b_i qui valent 0 ou 1 : ils choisissent aléatoirement certains pixels colorés de l'image et pour coder un bit $b_i = 1$, ils en augmentent la composante bleue, et pour coder un 0 ils diminuent cette composante bleue (d'un facteur qui dépend de la luminance du pixel). Pour retrouver le watermark, ils estiment la valeur de la composante bleue du pixel avant l'insertion du watermark en faisant une moyenne sur les points voisins et la comparent à la valeur de la composante bleue du pixel après insertion du watermark. Pour que l'algorithme gagne en robustesse, on peut tatouer plusieurs pixels avec le même bit b_i.

2.5.2.2 Domaine Fréquentiel

Les méthodes présentées précédemment permettent en général de retrouver le watermark en faisant la différence entre l'image originale et l'image tatouée. Cela leur confére un sérieux désavantage : une personne qui voudrait attaquer ces images et qui se serait procurée une image originale, ou bien plusieurs personnes mettant en commun leurs images tatouées peuvent détruire le watermark. Des algorithmes incluant le watermark non pas directement dans l'image, mais dans une transformée de l'image seront à cet égard plus robustes, et permettent en plus de choisir les pixels qui seront plus résistants à certains types d'attaques.

Des schémas du tatouage peuvent effectuer l'insertion du watermark dans des espaces transformés. Un espace transformé est obtenu après l'emploi d'une transformée telle que : DCT, DFT,DWT, SVD,etc. Cette stratégie rend le watermark plus robuste à la compression, puisqu'elle utilise le même espace qui sert au codage de l'image. Contrairement au domaine spatial, le watermark inséré dans le domaine fréquentiel est très sensible aux transformations géméométriques parce que ce genre de transformations modifient considérablement les valeurs des coefficients transformés [51, 50].

Transformée en Cosinus Discrtète (DCT)

De nombreuses méthodes ont été développées à partir des connaissances acquises auparavant en codage de source. Les auteurs de ces méthodes espèrent ainsi en travaillant dans le domaine DCT, anticiper et prévenir au moins les attaques liées à une compression JPEG. Ils espèrent également pouvoir travailler plus rapidement en couplant le tatouage d'images avec le codage de source. En d'autres termes, le tatouage est réalisé directement sur le flux compressé. Le dernier point opérant en faveur d'un tatouage dans le domaine DCT est qu'il est possible de bénéficier, au moins en partie, des études psycho-visuelles déjà menées en codage de source pour gérer les problèmes de visibilité. Parmi les techniques les plus connus on cite [49, 19].

Zhao et Koch [49], proposent d'insérer un watermark binaire $w \in (1, 0)$. Ils découpent l'image en bloc de taille 8 x 8 ; on fait ensuite la transformée DCT de chacun des blocs. Pour chaque bloc B_i, on choisit aléatoirement deux coefficients $f_{B_i}(m_1, n_1)$ et $f_{B_i}(m_2, n_2)$ parmi les fréquences moyennes. Chaque bloc est ensuite quantifié en utilisant la matrice de quantification JPEG et un facteur de quantification Q, la différence absolue entre les deux coefficients selectionnés est représenté par :

$$\Delta_{B_i} = |f_{B_i}(m_1, n_1)| - |f_{B_i}(m_2, n_2)|. \tag{2.7}$$

Un bit du watermark est inséré dans le bloc B_i, en modifiant la paire des coefficients $f_{B_i}(m_1, n_1)$ et $f_{B_i}(m_2, n_2)$ tels que la distance devienne :

$$\Delta_{B_i} = \begin{cases} \geq q \text{ si } w_i = 1 \\ \leq -q \text{ si } w_i = 0 \end{cases} \tag{2.8}$$

Où q est un paramètre qui contrôle la quantité d'information insérée. Cette méthode est bien adaptée à la compression JPEG, mais le watermark s'avère facilement détectable dans le cas d'une collusion de personnes mettant en commun leurs images tatouées.

Cox et al.[19] proposent également de faire une transformée DCT de toute l'image, pour tatouer les 1000 coefficients de plus grande amplitude, de façon à ce que le watermark soit inséré dans des zones visuellement significatives, où elle sera plus imperceptible. Le watermark est une séquence gaussienne de nombres réels pseudo-aléatoires d'une longueur 1000. Elle est ajoutée à ces coefficients selon une loi normale : ils montrent en effet qu'un tel watermark résistera mieux aux attaques par collusion (mise en commun de plusieurs documents tatoués). L'extraction du watermark se fait en soustrayant l'image originale à l'image tatouée : on obtient ainsi un watermark $W^{'}$ dont on calcule la corrélation avec le watermark original W pour décider si l'image avait bien été tatouée à l'aide du W.

Transformée en Ondelette Discrtète (DWT)

La recherche sur la perception humaine indique que la rétine de l'œil coupe l'image en plusieurs canaux de fréquence.Les signaux dans ces canaux sont traités indépendamment. De même, dans une décomposition de multi-résolution, l'image est séparée dans des bandes de largeur de bande approximativement égale sur une échelle logarithmique. On s'attend à ce donc que l'utilisation de la transformée en ondelette discrète qui permettra le traitement indépendant des composants résultants sans interaction perceptible significative entre eux, et par conséquent rend le processus d'insertion imperceptible plus efficace.

Pour cette raison, la décomposition en ondelette est généralement employée pour la fusion des images. Puisque le tatouage numérique comporte le fusionnement d'un watermark à un signal hôte, il suit que les ondelettes sont attrayantes pour le tatouage des images.

La théorie des ondelettes est commune à celle des bancs de filtres. L'idée est de séparer le signal original en plusieurs bandes de fréquences (basse-fréquence et haute-fréquence), pour mieux le compacter et le transmettre. La partie passe-bas donne une représentation compactée de l'image initiale. Cette partie passe-bas peut être décomposée plusieurs fois et ces décompositions successives correspondent aux échelles de décomposition. Pour reconstruire le signal, il faut rassembler ces diverses bandes.

La transformée en ondelettes utilise des filtres pour transformer l'image. Il y a beaucoup de filtres disponibles, les filtres les plus généralement utilisés pour le tatouage sont filtres ondelettes de Haar, filtres orthogonaux de Daubechies et filtres Bi-orthogonaux de Daubechies. Chacun de ces filtres décompose l'image en plusieurs fréquences.

La décomposition de niveau simple de l'image donne quatre représentations de fréquence . Ces quatre représentations s'appellent les sous-bandes LL, LH, HL, et HH comme montre la figure 2.3.

Kunder et Hatzinakos [50] proposent un algorithme du tatouage d'image, dans lequel le processus d'insertion utilise une technique de fusion multi-résolution et incorpore un modèle de système visuel humain SVH. Ils effectuent une transformée en ondelettes discrète de l'image et du watermark. Le watermark est une image (Logo) qui est 2^M plus petite que l'image hôte. La transformée en ondelettes du watermark est ajoutée dans la transformée en ondelettes de l'image. Afin de savoir dans quels points exactement ajouter le watermark, on calcule la *salience*, mesure donnant l'importance visuelle d'un pixel, et les coefficients d'ondelettes du watermark sont rajoutés dans les coefficients d'ondelettes correspondant aux points de plus forte salience. Les résultats expérimentaux

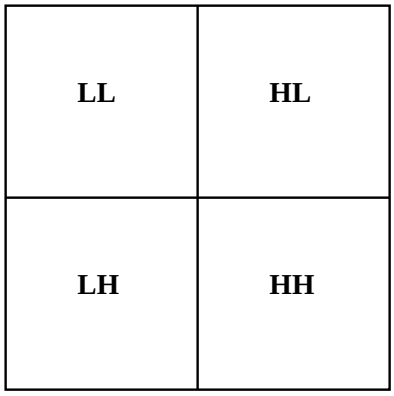


FIG. 2.3 – Un niveau de décomposition en utilisant la DWT.

montrent que cette méthode n'est pas robuste contre la rotation.

Kunder et Hatzinakos [51] proposent une technique du tatouage fragile. Le watermark est une sequence binaire. Il est inséré dans les coefficients des détails de l'image hôte avec l'utilisation d'une clé. Cette clé est générée aléatoirement et est employée pour choisir les endroits exacts dans le domaine de l'ondelette. Pour chaque coefficient, la clé a une valeur correspondante de 1 ou de 0 pour indiquer si le coefficient doit être marqué ou pas, respectivement. Le nombre de 1 dans la clé doit être plus grand ou égal à la taille du watermark.

Chen et Lin [12] proposent une technique de quantification pour le tatouage des images. Ils se sont basés sur la méthode proposée par Kundur et Hatzinakos [50] afin d'améliorer certains points faibles de cette dernière, tels que le choix du paramétre de quantification Q et la prise en compte des caractéristiques du Systéme Visuel Humain (SVH) pour maximiser l'imperceptibilité du watermark. Pour résoudre ces problèmes, les auteurs intègrent les points suivants pour atteindre un tatouage robuste :

- Chaque bit du tatouage est inséré par la modulation d'un ensemble de coefficients de l'ondelette.
- Utilisation d'un modèle visuel humain JND (voir 2.7.2.2) pour déterminer la quantité du signal tatoué qui peut être toléré à chaque localisation sans affecter la qualité visuelle de l'image.
- Deux watremarks identiques sont insérés dans la composante de basse fréquence et haute fréquence, pour augmanter la robustesse contre les différents types d'attaque.

La Décomposition en Valeurs Singulières (SVD)

La SVD est un outil mathématique très utilisé dans le traitement numérique d'images. Récemment, cette transformée est utilisée pour le tatouage numérique à cause de ses propriétés algébriques. Dans le chapitre suivant 3, nous détaillons le principe de cette décomposition, ainsi que les différents algorithmes fondés sur cette transformée.

2.5.3 Classification selon le champ d'application

Le champ d'application est la troisième métrique utilisée pour classer les techniques du tatouage. Le tatouage numérique a donc de nombreuses applications :

2.5.3.1 Protection des droits d'auteurs

La protection des droits d'auteur a été une des premières applications étudiée en tatouage d'images. Ce service reste cependant toujours d'actualité et concerne encore la majorité des publications. L'objectif est d'offrir, en cas de litige, la possibilité à l'auteur ou au propriétaire d'une image d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce même si l'image concernée a subi des modifications par rapport à l'original [16].

Identification du Propriétaire : (Owner identification)

La forme de l'avis de droit d'auteur (la notice copyright) est généralement " ©Propriétaire Date". Un inconvénient de ce texte de copyright est que les copyrights peuvent souvent être retiré du matériel (musique, film,livre,...) protégé [18, 66].

Le tatouage numérique peut être utilisé pour fournir des fonctionnalités de marquage des droits d'auteur, car il devient une partie intégrante du contenu, c'est-à-dire les informations de droit d'auteur sont intégrées dans le document.

Preuve de la propriété : (Proof of ownership)

Les propriétaires du multimédia utilisent les techniques du tatouage, non seulement pour identifier les droits d'auteur, mais en fait pour prouver la propriété.

Pour illustrer le problème, supposons Alice crée une image et la met sur son site, avec une copyright "©Alice 2000 ". Bob vole l'image, et utilise un programme de traitement d'images pour remplacer la copyright avec "©Bob 2000", puis prétend qu'il posséde le droit d'auteur . Comment peut régler le différend ?

La solution de ce problème consiste à déposer les droits d'un document auprès d'un tiers de confiance, qui délivre ensuite un identifiant. C'est cet identifiant qui sera tatoué dans le document [18].

La société Digimarc a commercialisé un système du tatouage conçu pour cette application. Leurs fonctions d'insertion et détection sont livrées avec le programme de traitement d'images, Photoshop. Lorsque le détecteur trouve un watermark, il contacte une base de données centrale pour identifier le propriétaire du watermark (qui doit payer un droit de garder l'information dans la base de données).

2.5.3.2 Gestion des transactions (transaction tracking)

Dans ce type d'application, on insére l'identité du vendeur et celle de l'acheteur. Les propriétaires successifs du document, et donc les sources de copie d'un document peuvent ainsi être identifiés. Un schéma du tatouage multiple est nécessaire.

Une application du tatouage transactionnel a été déployée par la société DiVX. L'une des mesures de sécurité mises en oeuvre dans le matériel DiVX est un tatouage qui pourrait être utilisé

pour identifier une tentative de piratage. Si des copies illégales d'un film DivX apparu sur le marché noir, DiVX pourrait utiliser le tatouage pour les suivre jusqu'à la source [18].

2.5.3.3 Protection de Copie (Copy protection)

On détecte la présence d'un copyright sur un document, dans le but d'empêcher sa manipulation par exemple. Cet enjeu est très important pour les maisons de disques regroupées dans le consortium SDMI[4] face à l'échange de mp3. Toutefois, il est également possible pour des dispositifs d'enregistrement et de lecture de réagir aux signaux tatoués. De cette façon, un dispositif d'enregistrement peut empêcher l'enregistrement d'un signal s'il détecte un watermark qui indique que l'enregistrement est interdit [18, 66].

En pratique, on peut par exemple imaginer un environnement logiciel et matériel totalement compatible avec le tatouage, qui empêche la copie d'un document tatoué [66].

2.5.3.4 Transmission secrète (Covert communication)

On peut aussi tatouer une image, de façon aussi discrète que possible, dans le but d'échanger des messages secrets. Ceux-ci sont cachés dans l'image, et nécessitent une clé secrète pour être décodés. Cette application a été formulée par Simmons [90] avec le problème du prisonnier, dans laquelle on suppose deux détenus dans des cellules séparées tentent de passer les messages secrèts.

Leur problème est qu'ils ne peuvent pas passer directement ces messages, mais plutôt, ces dernièrs doivent passer à travers le gardien de prison. Le gardien est prêt à transporter des messages inoffensifs entre eux, mais les punir s'il constate, par exemple, que leurs messages contiennent un plan pour s'enfuir.

La solution consiste à déguiser le plan d'évacuation dans les messages inoffensifs. Il existe plusieurs programmes commercialement disponibles conçus pour cette application, y compris StegoTools [5] [18].

2.5.3.5 Authentification

L'objectif est de détecter la manipulation des données originales. Ceci peut être fait en utilisant un tatouge fragile. Si le document original est modifié avec malveillance, le watermark sera détruit. Si le watermark peut être récupéré au destinataire, le travail est considéré authentique, autrement il devrait être considéré comme truqué. Un niveau bas de compression est habituellement autorisé mais pas le changement du contenu. Il y a plusieurs types du tatouages fragiles : certains nous permettent de détecter si l'image a été modifié et certains nous permettent de calculer une approximation de l'image originale dans les régions modifiées [18, 66].

[4] Le SDMI (Secure DigitalMusic Initiative) est un consortium de compagnies pour un projet du tatouage audio.

[5] http ://www.informatik.tu-muenchen.de/ stowasse/security.html.

2.5.3.6 Indexation (Captioning)

On peut enfin cacher des informations descriptives (méta-informations) dans une image ; par exemple, un médecin peut inclure dans une radiographie, de façon discrète afin de ne pas la dénaturer, le nom du patient traité, son diagnostic et ses observations. Ce cas est le plus simple, puisqu'une attaque visant à détruire le watermark ne présente aucun intérêt et n'est donc a priori pas à craindre.

Selon Vincent Martin [70], ce type de documents est appelé documents auto-indexé, car le watermark contient sa propre description, afin de permettre son stockage dans une base de données sans probléme de changement de format.

2.6 Classification des attaques

Pendant longtemps, les recherches dans le domaine du tatouage ont été focalisées sur la protection des droits d'auteur dont la robustesse est la propriété la plus importante. Le watermark doit être robust à certains types de manipulations habituellement utilisées dans l'imagerie numérique. S. Voloshynovskiy et al. [97] regroupent les attaques en trois catégories selon l'objectif de l'attaquant :

- Attaques géométriques : visant à déformer suffisamment le document tatoué.
- Attaques d'effacement : visant à supprimer le watremark.
- Attaques de cryptographie : visant à décrypter la clé secrète.
- Attaques de protocoles : visant à trouver une faille dans le protocole de gestion des droits d'auteurs.

Les deux premiers types d'attaques peuvent être considérés comme des attaques sur la robustesse, alors que les suivants sont des attaques sur la sécurité.

Attaques géométriques : Les attaques géométriques peuvent empêcher la détection du watermark. Parmi les transformations géométriques, les plus usuelles on cite :

- *Fliping (symétrie) :* Plusieurs images peuvent être retournées sans perdre aucune valeur. Bien que la résistance à ce type d'opérations est généralement simple à mettre en œuvre mais trés peu de systèmes survivre à ce type de transformation.
- *Rotation :* des petites angles de rotation, n'ont pas l'habitude de changer la valeur commerciale de l'image, mais peuvent faire le watermark non détectable.
- *Scaling (modification des dimensions)* : ce type d'opération est appliqué quand une image imprimée est scannée ou quand une image numérique de haute résolution est utilisée pour des applications électroniques, telles que la publication Web.
- *Le Cropping (rognage) :* Supprimer ou couper une partie d'une image qui s'étend au-delà d'une certaine limite, le bord de la fenêtre, par exemple. Certains programmes graphiques autorisent aussi le rognage comme moyen de tout masquer, sauf un objet donné, afin que les outils de dessin s'appliquent à l'objet seul.

Attaques d'effacement : Les attaques d'effacement les plus évolués sont :

- *Débruitage :* L'objectif de cette manipulation est d'approcher au mieux la forme d'onde du watermark pour pouvoir l'enlever. Le watermark peut étre estimé en utilisant le filtrage de

Wiener. Cette estimation est alors soustraite à l'image originale pour l'obtention d'une copie du message.

- *Compression JPEG :* La compression JPEG est une technique de compression avec pertes qui supprime les informations redondantes des images dont le but de diminuer la taille du fichier image. Comme le watermark est invisible, il peut donc être considéré comme non significatif et donc aussi être supprimé.
- *Modifications volumétriques :* Il existe une catégorie de traitement (étalement d'histogramme, égalisation d'histogramme, ou encore transformation Gamma) qui ne prend en compte que la luminance pour améliorer l'image. Comme le changement est fait sur la luminance, les informations tatouées sur la chrominance peuvent être désynchronisées.
- *Addition d'un bruit additif ou multiplicatif :* ont été largement abordés dans la théorie de la communication et de traitement du signal.
- *Filtage :* les filtre les plus utilisés sont : median filter, gausien filter, laplacien filter et average filter.
- *Rehaussement et lissage :* Le rehaussement correspond à l'augmentation des composantes hautes fréquences de l'image. L'image devient alors plus contrastée. Le lissage est l'opération contraire du rehaussement, il atténue les composantes hautes fréquences de l'image qui devient alors plus floue. Ces opérations peuvent modifier également les composantes hautes fréquences du message et leur faire perdre leurs particularités.
- *Gigue (Jittering) :* est un phénomène connu en télécommunications. Lorsque le délai de transmission du signal varie, il en résulte une réplication ou une suppression d'un morceau du signal. Ceci peut se produire dans le domaine spatial ou temporel sur les images, il peut y avoir un ajout ou une suppression de lignes ou de colonnes.

Petiscolas [80] donne un exemple de profit d'evaluation d'un algorithme du tatouage avec les paramètres d'attaques conseillés 2.1.

Niveau de l'attaque	Zéro	Faible	Modéré
Compression JPEG- Facteur de qaulité	100-90	90-75	75-50
Corrélation Gamma		0.7-1.2	0.5-1.5
Changement d'échelle		1/2-3/2	1/3-2
Filtre moyenne :			3x3

TAB. 2.1 – Exemple de profit d'evaluation d'un algorithme du tatouage proposé par Ptiscolas [80]

2.7 Mesures perceptuelles de la qualité visuelle des images

Dans les techniques du tatouage numérique la mesure de la qualité apportée sur le document hôte lors de l'insertion du watermark est importante. La qualité perceptuelle devrait être évaluée par des expériences subjectives avec des observateurs humain. Celles-ci sont cependant coûteuses

et rares. La contrainte d'imperceptibilité[6] conduit donc a construire des critères objectifs pour mesurer l'impact perceptuel d'un watermark : ce sont « les mesures perceptuelles ».

Dans le cadre du tatouage d'images, elles sont construites à partir d'études psycho-visuelles et modèle du SVH (Système Visuel Humain).

En générale deux types de métriques peuvent être utilisées pour l'évaluation de l'imperceptibilité : métriques basées pixel et métriques psycho-visuelles [53].

2.7.1 Métriques Basées Pixels

La table 2.2 représente les mesures de distortion les plus connues. Ces mesures sont basées sur le calcul de la différence entre l'image originale et tatouée (attaquée ou non attaquée).

La table 2.3 représente des mesures de distortion basées sur la corrélation entre l'image originale et tatouée [53].

Une étude comparative entre ces métriques est bien présentée par Eskicioglu et Fisher [25].

Maximum Difference	$MD = \max_{m,n} \lvert I_{m,n} - I^*_{m,n} \rvert$
Average Absolute Difference	$AD = \frac{1}{MN} \sum_{m,n} \lvert I_{m,n} - I^*_{m,n} \rvert$
Norm. Average Absolute Difference	$NAD = \sum_{m,n} \lvert I_{m,n} - I^*_{m,n} \rvert / \sum_{m,n} \lvert I_{m,n} \rvert$
Mean Square Error	$MSE = \frac{1}{MN} \sum_{m,n} (I_{m,n} - I^*_{m,n})^2$
Normalised Mean Square Error	$NMSE = \sum_{m,n} (I_{m,n} - I^*_{m,n})^2 / \sum_{m,n} I^2_{m,n}$
L^p-Norm	$L^p = (\frac{1}{MN} \sum_{m,n} \lvert I_{m,n} - I^*_{m,n} \rvert^p)^{1/p}$
Laplacian Mean Square Error	$LMSE = \sum_{m,n} (\nabla^2 I_{m,n} - \nabla^2 I^*_{m,n})^2 / \sum_{m,n} (\nabla^2 I_{m,n})^2$
Signal to Noise Ratio	$SNR = \sum_{m,n} I^2_{m,n} / \sum_{m,n} (I_{m,n} - I^*_{m,n})^2$
Peak Signal to Noise Ratio	$PSNR = MN \max_{m,n} I^2_{m,n} / \sum_{m,n} (I_{m,n} - I^*_{m,n})^2$
Image Fidelity	$IF = 1 - \sum_{m,n} (I_{m,n} - I^*_{m,n})^2 / \sum_{m,n} I^2_{m,n}$

TAB. 2.2 – Métriques de distortion basées sur la différence entre l'image originale et tatouée.

Le PSNR est la mesure de la distortion entre le signal tatoué et le signal original la plus utilisée. On considère généralement en tatouage d'images qu'un tatouage est imperceptible pour un PSNR

[6]Dans certaines références cette contrainte est désignée «fidélité» pour signifier qu'il y a peu de différences entre l'image originale et tatouée.

Normalised Cross-Correlation	$NC = \sum_{m,n} I_{m,n} I^*_{m,n} / \sum_{m,n} I^2_{m,n}$
Correlation Quality	$QC = \sum_{m,n} I_{m,n} I^*_{m,n} / \sum_{m,n} I_{m,n}$

TAB. 2.3 – Métriques de distortion basées sur la corrélation entre l'image originale et tatouée.

supérieur à 36 dB, et plus il est élevé, moins la distortion est importante.

Malgré l'utilisation courante du PSNR pour mesurer la qualité des images, celui-ci, n'est pas bien adapté au SVH. Le SVH ne perçoit pas tous les signaux de la même façon, comme la sensibilité au contraste par exemple. L'utilisation de PSNR seul ne peut donc pas être considérée comme une mesure objective de la qualité visuelle de l'image.

2.7.2 Métriques psycho-visuelles

D'autres métriques à prendre en compte sont les phénomènes de perception humaine. Des méthodes de mesures perceptuelles des distorsions qui prend en compte des éléments psychologiques et physiologiques de la perception humaine pour l'évaluation qualitative des images tatouées [76, 1]. Néanmoins, l'évaluation qualitative est encore d'actualité et il n'y a pas encore une métrique standard. Les approches les plus connues sont les métriques avec pondération perceptuelle et par seuil de perception présentées ci-dessous.

2.7.2.1 Pondération perceptuelle

L'approche la plus pratique est l'introduction d'une pondération perceptuelle w au sein de la mesure classique d'erreur quadratique moyenne. Le wPSNR - (weighted PSNR) est défini par :

$$wPSNR = 10 \log_{10}(\frac{\max^2}{wMSE}). \tag{2.9}$$

$$wMSE = \frac{1}{n} \sum_{i=1}^{n} \varphi_i^2 . (x_i - y_i)^2. \tag{2.10}$$

Où φ_i est une pondération représentant l'importance du i^{eme} échantillon. Plusieurs pondérations ont été proposées.La pondération la plus connue est celle de Watson [99] :

$$\varphi_i^2 = \frac{1}{\sigma_{b_i}^2 + V_i^2}. \tag{2.11}$$

$$V_i = \frac{1}{||\phi_i||} \sum |x_j|^\rho. \tag{2.12}$$

Dans ces formules, pour le i^{eme} coefficient, V_i est une mesure d'activité de voisinage, ϕ_i (de taille $||\phi_i||$) est l'ensemble qui représente les indices des voisins et enfin la variable $\sigma_{b_i}^2$ est un seuil

de visibilité qui dépend de la distance d'observation. Ce seuil est fixé à 10^2 pour JPEG2000. Les meilleurs résultats sont obtenus pour $\rho = 1/2$.

Le wPSNR de Watson a été conçu pour les images dans le domaine DCT notamment JPEG. Il utilise une table de niveau de sensibilité pour les 64 coefficients d'un bloc DCT. Ceci permet de prendre en compte la sensibilité fréquentielle et les phénomènes de masquage dûs à la luminance et au contraste. Une version plus simplifiée du wPSNR de Watson est utilisée dans JPEG2000 [53].

2.7.2.2 Seuils de perception

Contrairement aux critères de qualité sous forme de pondérations vus précédemment, ce type de seuil ne permet pas de quantifier la distorsion perceptuelle introduite. Néanmoins, il indique le niveau de distorsion maximal JND (*Just Noticeable Difference*) acceptable afin que le changement sur l'image ne soit pas visible. Au-dessous de ce seuil, la modification ne pourra pas être perçue, mais au-dessus elle pourra être remarquée.

Modèle JND de Watson :

Le modèle JND de Watson [99] est basé sur le calcule de l'erreur de quantification.

Compression JPEG et l'erreur de quantification :

Les étapes du processus de compression JPEG sont les suivantes :

– Décomposition de l'image originale I en blocs de taille 8x8,
– Application de la DCT à chaque bloc B_k. Soit c_{ijk} la fréquence DCT du bloc k.
– Quantification et arrondissement de chaque coefficient du bloc B_k en utilisant une matrice de quantification $Q = (q_{ij}, i, j = 1..8)$:

$$u_{ijk} = round[\frac{c_{ijk}}{q_{ij}}]. \tag{2.13}$$

L'erreur de quantification est calculée comme suit :

$$e_{ijk} = c_{ijk} - u_{ijk} \times q_{ij}. \tag{2.14}$$

La valeur maximale de e_{ijk} est $q_{ij}/2$.

On pose :

$$t_{ij} = q_{ij}/2. \tag{2.15}$$

Waston définit le seuil de masquage de la luminance comme suit :

$$t_{ijk} = t_{ij} \times (\frac{c_{00k}}{\bar{c}_{00}})^{a_T}, \tag{2.16}$$

où c_{00k} est le coefficient DC du bloc B_k, $\bar{c}_{00}$ est la moyenne des coefficients DC et a_T est un facteur qui contrôle le degré du masquage.

Cependant le modéle de seuil de masquage est définit par Watson comme suit :

$$m_{ijk} = \max[t_{ijk}, |c_{ijk}|^{w_i} \times t_{ijk}^{1-w_i}], \tag{2.17}$$

où w_i est un exposant $\in [0, 1]$.

2.7.2.3 Mesures d'imperceptibilité pour les images couleurs RGB basées SVH

Modèle JNCD (Just Noticeable Color Differences) :

La plus part des modèles perceptibles sont conçus pour des images niveau de gris. Le modèle JND de Watson est étendue pour l'évaluation de la qualité des images couleurs RGB. Ce modéle JNCD est proposé en 2007 par Yang et al. [106]. Dans ce cas, le JND de chaque composante $c \in \{R, G, B\}$ doit être calculé.

On pose m_{ijkc} le JND de la composante c calculé par la formule 2.17. Après plusieurs études expérimentales le modèle de JNCD pour les images couleurs RGB est définit comme suit :

$$cm_{ijkc} = \begin{cases} \frac{2}{7}m_{ijkc} & , c = R \\ \frac{1}{7}m_{ijkc} & , c = G \\ \frac{4}{7}m_{ijkc} & , c = B \end{cases} \tag{2.18}$$

Modèle CPSNR (Color image Peak Signal to Noise Ratio) :

Le PSNR peut être appilqué pour des images couleurs, en appliquant les formules suivantes :

$$PSNR = 10\log(\frac{255^2}{(MSE(R) + MSE(G) + MSE(B))/3}). \tag{2.19}$$

ou,

$$PSNR = (PSNR_R + PSNR_G + PSNR_B)/3. \tag{2.20}$$

En 2007, Yang et al.[106] ont proposé aussi un nouveau modèle PSNR pour l'evaluation de la qualité perceptuelle des images couleurs RGB. La contribution de ce nouveau modéle est l'incorporation du modèle JND de Watson dans le calcul de PSNR.

Ce processus se déroule suivant les étapes ci-dessous :

- Décomposition de l'image originale I en blocs B_k de taille 8x8.
- Décomposition de l'image tatouée I^* en blocs B_k^* de taille 8x8.
- Application de la DCT à chaque bloc B_k et B_k^*. soient c_{ijkc} la fréquence DCT du bloc B_k de la composante c et c_{ijkc}^* la fréquence DCT du bloc B_k^* de la composante c.
- Calcul de la fonction d'erreur :

$$e_{ijkc} = c_{ijkc}^* - c_{ijkc} \tag{2.21}$$

- Le CPSNR d'une image de taille $m \times n \times 3$ est donné par la formule :

$$CPSNR = 10\log(\frac{3 \times m \times n \times 255^2}{\sum_c \sum_k \sum_{ij}(p_{ijkc} \times e_{ijkc}^2)}) \tag{2.22}$$

p_{ijkc} est l'unité de masquage :

$$p_{ijkc} = \frac{1}{1 + cm_{ijkc}} \tag{2.23}$$

Où cm_{ijkc} est la valeur de JNCD calculée par la formule 2.18.

2.8 Conclusion

Dans ce chapitre, nous avons présenté la technologie du tatouage numérique d'une manière générale. Nous nous sommes intéressés aux terminologies et notions liées aux techniques du tatouage invisible des images numériques. Ces terminologies sont nécessaires pour les chapitres suivants telles que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle.

Nous avons présenté aussi une taxonomie des techniques du tatouage selon différents critères : type de l'algorithme, champ d'application et le domaine d'insertion. Selon le dernier critère les techniques du tatouage peuvent être regroupées en deux catégories : ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel . Dans cette dernière catégorie plusieurs transformées peuvent être utilisées telles que la DFT, DCT, DWT, et la SVD, et c'est cette dernière transformée qui est présentée dans le chapitre suivant.

Chapitre 3

Tatouage d'images numériques utilisant la SVD

Résumé : Généralement, le watermark n'est pas inséré directement dans l'image originale, mais dans une transformée de celle-ci. Le principe consiste à représenter les données initiales dans un domaine transformé. A cet égard, il existe un large éventail de solutions : DFT, DCT, DWT et SVD, etc.

L'objectif de ce chapitre est de jeter la lumière sur l'utilisation de la SVD dans le contexte du tatouage numérique des images, en présentant quelques algorithmes très connus qui utilisent cette transformée pour insérer des watermarks numériques.

3.1 Introduction

Historiquement, les premières techniques du tatouage d'images introduisaient le watermark directement dans les pixels. Partant d'une image à niveau de gris où chaque pixel est codé sur un octet, le dernier bit significatif est changé selon une règle pré-définie. Ces approches, peu robustes, ont été rapidement abandonnées. En fait, elles relèvent davantage de la stéganographie que du tatouage.

Comme indiqué précédemment, le watermark est aujourd'hui inséré dans une transformée des données. La transformée la plus populaire en traitement d'image est la DCT. Cela est dû sans doute au remarquable comportement théorique de la DCT ayant l'avantage d'optimalité au sens de compaction d'énergie, i.e. de la plus petite quantité d'information nécessaire pour approcher au sens des moindres carrés une image.

La représentation par ondelette (DWT) s'impose aujourd'hui comme une méthode incontournable en traitement d'images et de vidéo en raison de ses solides fondements théoriques, de son efficacité pratique et de son interprétation intuitive.

En dehors de la DCT et DWT, une nouvelle transformées SVD a été mise en ouvre.

La décomposition en valeurs singulières (SVD) et ses propriétés algébriques ont également été utilisées par certains chercheurs pour des applications de tatouage numérique d'images. Le

principe de cette décomposition et quelques techniques de tatouage utilisant cette technologie sont présentées dans les sections suivantes.

3.2 La décomposition en valeurs singulières SVD

Une matrice est un tableau de nombres dont il est difficile d'extraire les caractéristiques intéressantes pour résoudre un problème donné. Une stratégie efficace et générale pour mettre en évidence les propriétés d'une matrice est de la décomposer (ou "factoriser") en un produit de matrices plus simples et dont les caractéristiques sont clairement identifiables et interprétables. La factorisation la plus générale, et peut-être la plus utile, est *la Décomposition en Valeurs Singulières*[1].

La SVD s'avère être non seulement un outil puissant d'analyse de l'efficacité des méthodes numériques d'inversion mais permet également d'introduire la notion de pseudo-inverse. Cette notion sera en particulier utilisée pour les problèmes de reconstruction avec des données incomplètes ou encore de détermination dans le cas de problèmes sur-déterminés (comme par exemple l'interpolation polynomiale en deux dimensions et plus). Pour des raisons de simplicité, et parce que c'est le cas général en images numériques, nous allons définir la décomposition en valeurs singulières d'une matrice A en se limitant au cas où A est à valeurs réelles. Une extension au cas où A serait à valeurs complexes est présentée dans [14].

3.2.1 Définition

Toute matrice A, de taille $m \times n$, peut se décomposer en produit de trois matrices de la manière suivante :

$$A = USV^T = \sum_{i=1}^{r} \lambda_i U_i V_i^T. \tag{3.1}$$

Où U et V sont des matrices orthogonales, respectivement de dimensions $m \times m$ et $n \times n$. On a : $U^T U = I$ et $V^T V = I$.

S est une matrice diagonale de taille $n \times n$ composée des valeurs singulières λ_i, dans l'ordre décroissant, sur la diagonale et T est l'opérateur de transposition. On peut aussi écrire :

$S = diag(\lambda_1, \lambda_2, ..., \lambda_r)$, telles que $\lambda_1 \geq \lambda_2 \geq .... \geq \lambda_r > 0$ où $r = min(m, n)$ le rang de la matrice A est égal au nombre de valeurs singulières (SVs) non nulles que possède la matrice A.

Le principal intérêt de cette méthode vient du fait que les SVs sont très stable, i.e., lorsque des petites informations (perturbations) sont ajoutées à l'image, leurs SVs ne changent pas significativement. A cause de cette propriété plusieurs algorithmes de tatouage utilisent les SVs pour insérer des watermaks numériques. Dans la Section 3.3.1.1 quelques algorithmes de tatouage très connus sont présentés.

Un autre intérêt de cette méthode est que la SVD range le maximum d'énergie de l'image dans un minimum de valeurs singulières, la compression est obtenue donc intuitivement en forçant les valeurs singulières les plus faibles à zéro.

[1] On la désigne souvent par son acronyme anglo-saxon "SVD", pour "Singular Value Decomposition"

3.2.2 Interprétation géométrique

La SVD peut s'interpréter géométriquement de diverses façons qui rendent plus compréhensible sa structure quelque peu abstraite. Nous donnons ci-dessous une de ces interprétations.

Toute matrice A de taille $m \times n$ peut être interprétée comme étant la représentation matricielle d'un opérateur linéaire de R^n dans R^m. Soit alors une matrice A dont nous considérons la SVD :

- U étant orthogonale, ses colonnes forment une base orthonormée de R^m.
- V étant orthogonale, ses colonnes (les lignes de V^T) forment une base orthonormée de R^n.

Une expression telle que $Av = su$ est interprétée géométrique comme suit : l'image dans R^m d'un vecteur singulier droit de R^n est égal à s fois le vecteur singulier gauche associé à la valeur singulière s.

Soit alors x un vecteur de R^n quelconque. Pour simplifier, supposons que A soit de rang plein, disons $n(m)$. Alors pour obtenir Ax, il suffit de :

- Projeter x sur la base de R^n constituée des n vecteurs colonnes de V (les vecteurs singuliers droits). Les valeurs des projections sont les coordonnées de x dans cette base.
- Multiplier chacune de ces n coordonnées par la valeurs singulière correspondante.
- Utiliser les nombres ainsi obtenus comme coordonnées d'un vecteur y sur les n premiers vecteurs singuliers gauches dans R^m (les n premières colonnes de U).
- Affecter la valeur "0" aux $(m - n)$ coordonnées restantes de y (sur les $(m - n)$ dernières colonnes de U).

Alors y est le vecteur cherché Ax.

La figure 3.1 illustre ce processus pour la première coordonnée v_1 d'un vecteur x (avec $n = 2$ et $m = 3$).

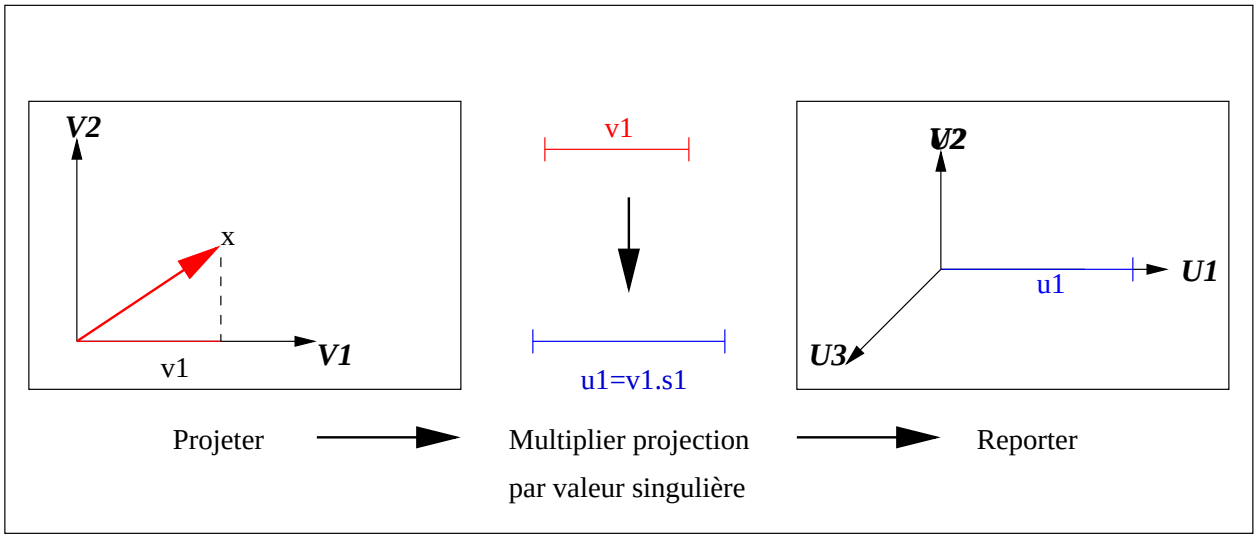


FIG. 3.1 – Interprétation géométrique de la SVD

3.2.3 Exemple

Afin d'illustrer notre propos nous pouvons montrer le résultat d'une SVD sur l'image *House* Figure 3.2. Il s'agit de la première image singulière (b) où nous ne gardons qu'une valeur singulière par composante couleur (en RGB), et de sa troncature de rang 10 (i.e. on reconstruit l'image avec les 10 premières valeurs singulières (c)). On remarque que la première image singulière est plutôt basse fréquence alors que la dixième est haute fréquence.

(a) (b) (c)

FIG. 3.2 – Image originale (a), sa première image singulière (b), et sa troncature de rang 10 (c).

3.3 Algorithmes de tatouage utilisant la transformée SVD

La transformée SVD est un outil mathématique très utilisé dans le traitement d'images numériques. Récemment cette technique est utilisée pour le tatouage d'images numériques, et les résultats obtenus sont très efficaces en termes de robustesse et imperceptibilité.

Dans ce qui suit on présente quelques algorithmes de tatouage basés sur cette transformée. On a classifié ces algorithmes selon le type d'algorithmes de détection (aveugles ou non aveugles).

La SVD est appliquée soit à toute l'image (Global-SVD), soit sur des blocs de celle-ci (Bloc-SVD)

3.3.1 Algorithmes non aveugles

3.3.1.1 Algorithme Global-SVD de Chandra

Dans [10] D.V. Satish Chandra propose deux algorithmes de tatouage d'images non aveugles. Le premier algorithme est Global-SVD où la SVD est appliquée sur toute l'image hôte et le watermark, ces derniers ont la même taille. Les SVs du watermark sont multipliées par un scalaire et ensuite ajoutées aux SVs de l'image hôte. La phase de détection requis la connaissance de trois matrices qui sont la matrice diagonale de l'image hôte et les matrices orthogonales du watermark original. Cela veut dire que l'espace demandé pour stocker ces matrices égale le triple de la taille de l'image hôte. Tandis que, le deuxième algorithme est Bloc-SVD, i.e. l'image hôte est décomposée en blocs, et un bit du watermark est multiplié par un scalaire et ajouté à la plus grande SV du

bloc correspondant. La phase de détection requis le transfert de l'image hôte. Ces algorithmes sont présentés ci-dessous.

Algorithme d'insertion

Entrées :

– f : image hôte de taille $n \times m$.
– W : watermark original de taille $n \times m$.

Sorties :

– f_w : image tatouée.
– Les matrices :
  – S : matrice diagonale de l'image hôte.
  – Uw et Vw : matrices orthogonales du watermark original.

Étapes :

1. La décomposition de l'image hôte f en valeurs singulières :

$$f = USV^T, \tag{3.2}$$

2. La décomposition du watermark W en valeurs singulières :

$$W = U_w S_w V_w^T, \tag{3.3}$$

3. Construction d'une nouvelle matrice diagonale S_y dont les valeurs diagonales sont λ_{y_i} selon la formule suivante :

$$\lambda_{y_i} = \lambda_i + \alpha \lambda_{w_i}, \tag{3.4}$$

   Où α est un scalaire choisit pour maintenir la qualité de l'image tatouée, λ_i sont les éléments diagonaux de S (SVs de f) et λ_{w_i} sont les éléments diagonaux de S_w (SVs de W). .

4. Reconstruction de l'image tatouée f_w en utilisant S_y et les matrices orthogonales (U,V) de l'image originale comme suit :

$$f_w = US_yV^T. \tag{3.5}$$

Algorithme d'extraction

Entrées :

– f_w^* : image tatouée et éventuellement attaquée.
– Les matrices :
  – S : matrice diagonale de l'image hôte.
  – Uw et Vw : matrices orthogonales du watermark original.

Sortie :

– Le watermark W^*.

Étapes :

1. La décomposition de l'image f_w^* en valeurs singulières :

$$f_w^* = U^* S^* V^{*^T}; \tag{3.6}$$

2. Le calcul de la matrice diagonale S_w^* :

$$S_w^* = \frac{(S^* - S)}{\alpha}; \tag{3.7}$$

3. Reconstruction du watermark W^* en utilisant S_w^*, U_w et V_w comme suit :

$$W^* = U_w S_w^* V_w^T. \tag{3.8}$$

3.3.1.2 Algorithme Bloc-SVD de Chandra

Dans cet algorithme l'image hôte est décomposée en blocs B_i de taille $k \times k$, et la SVD est appliquée sur chaque bloc B_i . Le principe de cet algorithme est présenté ci-dessous.

Algorithme d'insertion

Entrées :

– f : image hôte de taille $n \times m$.
– Taille du bloc $k \times k$.
– W : le watermark original de taille $\frac{n}{k} \times \frac{m}{k}$.

Sortie :

– f_w : image tatouée.

Étapes :

1. La décomposition de l'image hôte f en blocs B_i de taille $k \times k$.
2. Pour chaque bloc B_i faire :
   – Décomposition de B_i en valeurs singulières :

$$B_i = U_i S_i V_i^T; \tag{3.9}$$

   – Insertion d'un bit du watermark (W_i) dans la plus grande SV (λ_i^1) du bloc B_i comme suit :

$$\lambda w = \lambda_i^1 + \alpha * W_i; \tag{3.10}$$

   Où, α est un scalaire choisit pour maintenir la qualité de l'image tatouée, et λw est la plus grande SV du bloc tatoué Bw_i.
   – S_w est la matrice diagonale S_i où le premier élément est remplacé par λw. Cette matrice est utilisée pour construire le bloc tatoué Bw_i comme suit :

$$Bw_i = U_i S_w V_i^T; \tag{3.11}$$

3. Construction de l'image tatouée à partir des blocs tatoués.

Algorithme d'extraction

Entrées :

– f : image hôte de taille $n \times m$.
– f_w^* : image tatouée et éventuellement attaquée.
– Taille du bloc $k \times k$.

Sortie :
– W^* : le watermark extrait.
Étapes :

1. La décomposition de f_w^* en blocs B_i^* de taille $k \times k$.
2. Pour chaque bloc B_i^* faire :
   – Décomposition de B_i^* en valeurs singulières :

$$B_i^* = U_i^* S_i^* V_i^{*T}; \tag{3.12}$$

   – Le bit W_i^* du watermark est obtenu à partir du la plus grande SV du bloc tatoué (λw^*) et celle du bloc original (λ_i^1) comme suit :

$$W_i^* = \frac{(\lambda w^* - \lambda_i^1)}{\alpha}; \tag{3.13}$$

3. Construire le watermark W^* à partir des bits W_i^*.

3.3.1.3 Algorithme de R.Liu et T.Tan

Dans [63] R.Liu et T. Tan proposent un algorithme de tatouage non aveugle. Dans ce cas, le watermark est multiplié par un scalaire et ensuit ajouté à la matrice des SVs de l'image hôte. L'image tatouée est reconstruit en utilisant cette nouvelle matrice et les deux matrices orthogonales de l'image hôte. Les résultats expérimentaux montrent que cette méthode est robuste contre plusieurs attaques, tel que low pass filtre, compression JPEG (Q=5%), rotation jusqu'à 30° et le cropping. Par contre le point de faible de cette méthode réside dans la phase de détection qui demande la connaissance de trois matrices comme dans l'algorithme Global-SVD de Chandra. Nous détaillons dans la suite le principe de cet algorithme.

Algorithme d'insertion
Entrées :
– f :image hôte de taille $n \times m$.
– W : le watermark original de taille $n \times m$.
Sorties :
– f_w image tatouée.
– Les matrices :
  – S : matrice diagonale de l'image hôte
  – U_w,V_w : matrices orthogonale du watermark original.
Étapes :

1. La décomposition de l'image hôte f en valeurs singulières :

$$f = USV^T; \tag{3.14}$$

2. Le watermark W est ajouté à la matrice S comme suit :

$$D = S + \alpha * W; \tag{3.15}$$

3. La décomposition de D en valeurs singulières :

$$D = U_w S_w V_w; \tag{3.16}$$

4. L'image tatouée f_w est obtenue en utilisant les SVs modifiées (S_w) de l'image originale comme suit :

$$f_w = U S_w V^T. \tag{3.17}$$

Algorithme d'extraction

Entrées :

– f_w^* : l'image tatouée et éventuellement attaquée.
– Les matrices
  – S : matrice diagonale de l'image hôte ;
  – U_w, V_w : matrices orthogonales du watermark original.

Sorties :

– W^* : watermark extrait.

Étapes :

1. La décomposition de l'image f_w^* en valeurs singulières :

$$f_w^* = U^* S^* V^{*T}; \tag{3.18}$$

2. Le calcul de la matrice D^* qui contient le watermark en utilisant U_w et V_w comme suit :

$$D^* = U_w S^* V_w^T. \tag{3.19}$$

3. Le watermark W^* est obtenu en utilisant S comme suit :

$$W^* = \frac{D^* - S}{\alpha}. \tag{3.20}$$

3.3.1.4 Algorithme de Y. Xing et J. Tan

Dans [104], Y. Xing et J. Tan proposent un algorithme bloc-SVD pour le tatouage d'images couleurs RGB. Un bit de chaque composante de couleurs RGB du watermark est inséré dans la plus grande SV du bloc correspondant de la composante RGB correspondante. La phase de détection requis la connaissance de l'image hôte. Le principe de cet algorithme est présenté ci-dessous.

Algorithme d'insertion

Entrées :

– f : image hôte (une image couleur RGB de taille $N \times N$ où $N = 2^n$).
– W : watermark original (une image couleur de taille $M \times M$, où $M = 2^m$ et $n \geq m$).

Sortie :

– f_w : image tatouée.

Étapes :

1. Pour chaque composante (canal) de couleur $C \in \{R, G, B\}$ faire :

- Diviser la composante C en blocs B_i de taille $\frac{N}{M} \times \frac{N}{M}$.
- Pour chaque bloc B_i faire
  - La décomposition de B_i en valeurs singulières :

$$B_i = U_i S_i V_i^T. \tag{3.21}$$

  - Un bit W_i du watermark est ajouté à la plus grande SV (λ_i^1) du bloc correspondant B_i comme suit :

$$\lambda w = \lambda_i^1 + \alpha * W_i. \tag{3.22}$$

  - S_w est la matrice diagonale S_i avec le premier élément est λw.Construire le bloc tatoué Bw_i comme suit :

$$Bw_i = U_i S_w V_i. \tag{3.23}$$

- Construction de la composante tatouée C_w à partir des blocs tatoués.

2. Construire l'image tatouée f_w à partir des trois composantes tatouées.

Algorithme d'extraction
Entrées :
- f_w^* : l'image tatouée et éventuellement attaquée ;
- f : l'image hôte.

Sortie :
- W^* : watermark extrait (une image couleur RGB)

.

Étapes :

1. Pour chaque composante (canal) de couleur $C_w \in \{R_w, G_w, B_w\}$ faire :
   - Diviser la composante C_w en blocs Bw_i^* de taille $\frac{N}{M} \times \frac{N}{M}$.
   - Pour chaque bloc Bw_i^* faire :
     - La décomposition de Bw_i^* en valeurs singulières :

$$Bw_i^* = U_i^* S_i^* V_i^{*T}. \tag{3.24}$$

     - Le bit W_i^* du watermark est obtenu à partir de la plus grande SV (λw^*) du bloc correspondant Bw_i^* et celle du bloc original (λ_i^1) comme suit :

$$W_i^* = \frac{(\lambda w^* - \lambda_i^1)}{\alpha}. \tag{3.25}$$

   - Construction de la composante W_c du watermark extrait à partir des bits extraits.
2. Construire le watermark W^* à partir des trois composantes extraites W_c.

3.3.2 Algorithmes aveugles

Dans le tatouage aveugle seule l'image tatouèe et la clè secréte doivent être disponibles au moment de l'extraction. L'idée utilisée pour le tatouage aveugle est de maintenir l'ordre des SVs. Ci-dessous on présente deux algorithmes de tatouage aveugle qui utilisent la transformation SVD.

3.3.2.1 Algorithme de J.Liu et al.

Dans [62], J.Liu et al. proposent un algorithme de tatouage aveugle dont la phase de détection ne requis que l'image tatouée. L'idée de base consiste à maintenir l'ordre décroissant des SVs, pour que le détecteur (la phase de détection) peut récupérer le bit insérer dans la SV utilisée par la phase d'insertion. Le watermark (qu'est une séquence binaire de taille k) est inséré dans k valeurs singulières du milieu. Le principe de cet algorithme est présenté ci-dessous.

Algorithme d'insertion

Entrées :

- f : l'image hôte.
- W : le watermark original $\in \{0, 1\}$ de taille K.
- Le watermark est inséré dans K valeurs singulières du milieu tel que :
  - l_1 : l'indice de la première valeur singulière du milieu à utiliser ;
  - l_2 : l'indice de la dernière valeur singulière du milieu à utiliser ;
  - $K = l_2 - l_1$.

Sorties :

- f_w : image tatouée.

Étapes :

1. La décomposition de l'image hôte f en valeurs singulières :

$$f = USV^T. \tag{3.26}$$

   Soient λ_i les élèments diagonaux de S (SVs de f).

2. Modifier les valeurs singulières du milieu comme suit :
   - Pour $i = l_1$ à l_2 faire
     - Si $W_i = 1$ et $\lambda_{i-1} - \lambda_i < 1.25\Delta$ alors : $\lambda w_i = \lambda_{i-1} - 1.25\Delta$;
     - Si $W_i = 1$ et $\lambda_{i-1} - \lambda_i \geq 1.25\Delta$ alors : $\lambda w_i = \lambda_i$;
     - Si $W_i = 0$ et $\lambda_{i-1} - \lambda_i \; 0.75\Delta$ alors : $\lambda w_i = \lambda_{i-1} - 0.25\Delta$;
     - Si $W_i = 0$ et $\lambda_{i-1} - \lambda_i \leq 1.25\Delta$ alors : $\lambda w_i = \lambda_i$.

     Où Δ est un seuil choisit expérimentalement.

3. L'image tatouée est obtenue en utilisant S_w (la matrice S avec les nouvelles SVs λw_i) comme suit : $f_w = US_wV^T$.

Algorithme d'extraction

Entrées :

- f_w^* : l'image tatouée et éventuellement attaquée.
- l_1 : l'indice de la première valeur singulière du milieu utilisée ;
- l_2 : l'indice de la dernière valeur singulière du milieu utilisée ;

Sortie :

- W^* : le watermark extrait.

Étapes :

1. La décomposition de l'image f_w^* en valeurs singulières :

$$f_w^* = U^* S^* V^{*T}; \tag{3.27}$$

soient λ_i^* les élèments diagonaux de S^* (SVs de f_w^*).

2. Extraire le watermark W^* comme suit :
   – j=1 ;
   – Pour $i = l_1$ à l_2
     – Si $\lambda_{i-1}^* - \lambda_i^* > \Delta$; alors $W_j = 1$;
     – Si $\lambda_{i-1}^* - \lambda_i^* \leq \Delta$; alors $W_j = 0$;
     – $j = j + 1$.

3.3.2.2 Algorithme de C. Chang et al.

Dans [11], C. Chang et al. proposent un algorithme aveugle pour le tatouage numérique des images. L'image hôte est décomposée en blocs de taille 4x4. Pour augmenter la robustesse de l'algorithme, chaque bit du watermark est inséré dans trois blocs différents. Cependant le watermark est copié trois fois. Pour des raisons de sécurité, les positions (ou les pixels) utilisées pour insérer le watermark sont obtenues en utilisant deux clés, la première est secrète et la deuxième est publique. Le principe de cet algorithme est présenté ci-dessous.

Algorithme de préparation des positions utilisées pour insérer le watermark

Entrées :

– Taille de l'image hôte : $n \times n$.
– Taille du watermark : $m \times m$.

Sortie :

– P : Matrice des positions de taille $m \times m \times 3$.

Étapes :

1. Choisir deux grands nombres premiers p et q (p et q sont secrèts).
2. $Z = p \times q$ (Z publique).
3. Choisir aléatoirement deux valeurs secrètes k_1 et k_2.
4. Calculer les positions comme suit :
   Pour $i = 1$ à $m \times m \times 3$ faire :

$$X_i = X_{i-1}^2 \mod Z, X_0 = k_1^2 \mod Z; \tag{3.28}$$

$$Y_i = Y_{i-1}^2 \mod Z, Y_0 = k_2^2 \mod Z; \tag{3.29}$$

$$x_i = X_i \mod \frac{N}{4}; \tag{3.30}$$

$$y_i = Y_i \mod \frac{N}{4}. \tag{3.31}$$

Le bit du watermark W_i est inséré dans le pixel (x_i , y_i).

Algorithme d'insertion

Entrées :

– f : image hôte de taille $n \times n$.
– W : le watermark de taille $m \times m$ ($W \in \{0, 1\}$).
– P : Matrices des positions.

Condition :

$\frac{n}{4} \times \frac{n}{4} > m \times m \times 3$.

Sortie :

– f_w : image tatouée.

Étapes :

1. La décomposition de l'image hôte en blocs de taille 4×4.
2. Pour $i = 1$ à $m \times m \times 3$ faire :
   – Calculer le bloc B_j qui contient le pixel (x_i,y_i) : $B_j = x_i \times \frac{n}{4} + y_i$;
   – Calculer la SVD du bloc B_j : $B_j = U_j S_j V_j^T$;
   – Soient λ_i les élèments diagonaux de S (SVs de f) ;
   – Mettre $\lambda_3 = \lambda_2$;
   – $\lambda_2 = \lambda_2 + \alpha W_i$
   – Si $\lambda_1 < \lambda_2$ alors $\lambda_1 = \lambda_2$.
   – Reconstruire le bloc tatoué en utilisant les SVs modifiés.
3. Reconstruire l'image tatouée en utilisant les blocs tatoués.

Algorithme d'extraction

Entrées :

– F_w^* : image tatouée et attaquée de taille $n \times n$.
– La clé secrète (k_1, k_2).
– La clé publique Z.

Sortie :

– W^* : le watermark extrait.

Étapes :

1. Obtenir la matrice des positions en appliquant les équations (3.28, 3.29, 3.30 et 3.31) avec la clé secrète et publique.
2. La décomposition de l'image f_w^* en blocs de taille 4×4.
3. Pour $i = 1$ à $m \times m \times 3$ faire :
   – Calculer le bloc B_j^* qui contient le pixel (x_i, y_i) :$B_j^* = x_i \times \frac{n}{4} + y_i$;
   – Calculer la SVD du bloc B_j^* : $B_j^* = U_j^* S_j^* V_j * T$;
   – Si $\lambda w_1 - \lambda w_2 > \frac{\alpha}{2}$ alors : $WT_i = 1$ sinon $WT_i = 0$.
4. Pour $i = 1$ à $m \times m$ faire :
   – Si $WT_i + WT_{i+m\times m} + WT_{i+m\times m\times 2} \geq 2$ alors : $W_i^* = 1$ sinon $W_i^* = 0$.

Récapitulation

Le tableau 3.1 résume les algorithmes présentés précédemment.

Discussion :

Algorithme	Type SVD	Image hôte	Watermark	détection
Chandra Bloc-SVD	Bloc-SVD	Niveau de gris	Niveau de gris	Non aveugle
Chandra Clobal-SVD	Global-SVD	Niveau de gris	Niveau de gris	Non aveugle
R.Liu et T.Tan	Global-SVD	Niveau de gris	Niveau de gris	Non aveugle
Y.Xing et J.Tan	Bloc-SVD	RGB couleur	couleur	Non aveugle
J.Liu et al.	Global-SVD	Niveau de gris	M-sequence $W \in \{0, 1\}$	Aveugle
C. Chang et al	Bloc-SVD	Niveau de gris	Image binaire	Aveugle

TAB. 3.1 – Tableau récapitulatif des algorithmes de tatouage présentés précédemment.

Généralement ces méthodes maintiennent une haute qualité d'images tatouées et elles sont robustes contre certaines attaques. Toutefois, les travaux récents montrent que certains points de faibles peuvent être soulignés. La méthode de Liu est amélioré dans [34]. Dans cette nouvelle méthode, l'algorithme de Liu est appliquée sur des blocs de taille 16×16. Le watermark de taille 16×16 est inséré dans chaque bloc. En effet, cette méthode rend le watermark plus robuste contre les attaques. La méthode de Liu et Global-SVD de Chandra ont aussi un problème d'ambigüité. Dans le processus de détection, le watermark est construit en utilisant les vecteurs singuliers U_w et V_w du watermark originales. Si les vecteurs singuliers d'une autre image plutôt que le watermark original sont utilisés par l'algorithme de détection, cette image est reconstruite comme watermark extrait. Ce problème est résolu dans [107], en intégrant U_w et V_w comme paramètres de contrôle. Dans [93], une autre solution est proposée. L'idée est de modifier l'ordre des SVs. Dans cette méthode, l'image originale est décomposée en blocs de taille 8×8, ensuite la SVD est appliqué sur chaque bloc. La deuxième et la troisième SV sont échangées si le bit du watermark est 1. Ce changement dans la relation d'ordre sera constaté par le processus de détection.

3.4 Conclusion

Ce chapitre fournie une vue globale sur la décomposition SVD, et son efficacité pour le tatouage numérique. On a présenté son principe et ses propriétés algébriques, ensuite on a présenté quelques algorithmes de tatouage très connus utilisant cette technologie.

Dans le chapitre 5, une nouvelle approche de tatouage aveugle d'images couleurs RGB sera présentée.

Chapitre 4

Tatouage fragile d'images numériques

Résumé : Dans le monde numérique, le célèbre adage qui dit : «voir c'est croire. »*[1] *n'est plus vrai en raison de l'évolution et la puissance des outils de traitement numérique des multimédia. Pour garantir la fiabilité et la sécurité des documents multimédia, des techniques d'authentification sont en cours d'élaboration.

Selon les différentes manières de transmettre les données d'authentification pour les médias numériques, les techniques d'authentification peuvent être généralement divisées en deux catégories : techniques basées sur la signature numérique et techniques basées sur le tatouage fragile [65].

Ce chapitre n'a pas pour but d'arborer les différentes approches permettant d'assurer un service d'authentification et d'intégrité pour les images. Néanmoins, l'objectif est de présenter dans les grandes lignes l'efficacité des approches fondées sur le tatouage fragile par rapport à celles fondées sur la signature électronique, afin d'introduire progressivement les notions clés associées à une approche de tatouage fragile.

4.1 Introduction

Avec le développement sans cesse des réseaux informatique et des outils du traitement numérique des multimédia, la duplication , la falsification et l'usurpation d'identité sont devenues des préoccupations majeures des chercheurs. Par conséquence, l'importance de l'authentification et de la vérification du contenu sont devenues plus apparentes. En réponse à ces défis, plusieurs approches d'authentification des données numériques ont été proposées.

L'authentification de message repose sur trois concepts :

– La protection de l'intégrité d'un message ;
– La validation de l'identité du créateur du message ;
– La non-répudiation de l'origine (résolution de conflit).

Les systèmes d'authentification des documents multimédias peuvent être appliqués dans de nombreux domaines :

[1]Proverbe anglais : "seeing is believing"

L'archivage d'images médicales : Les données d'authentification des patients peuvent être incorporées au moment où leurs images médicales sont prises pour protéger les droits des patients quand une faute professionnelle médicale arrive et doit être résolue au tribunal.

Enregistrement image/son d'événements criminels : l'authentification d'image ou la conversation d'événement juridiquement indispensable pourrait conduire à des percées dans les affaires criminelles, toute falsification s'elle n'est pas détectée, pourrait entraîner une décision erronée.

Radiodiffusion : lors des crises internationales, les médias falsifiés ou contrefaits pourraient être utilisés pour la propagande et la manipulation de l'opinion publique. Par conséquent, la radiodiffusion est un domaine où l'authentification des multimédias est applicable.

Le renseignement militaire : un système d'authentification multimédia permet d'authentifier si les médias qu'ils ont reçus viennent d'une source légitime et de vérifier si le contenu est original. Quant le contenu est modifié, un système d'authentification efficace devrait déterminer la localisation des manipulations [89, 66].

L'authentification est un problème bien étudié dans la cryptographie. Friedman [32], propose de créer un appareil photo (trustworthy camera) avec une signature, qui est associée à une image, en utilisant un système cartographique. Si un seul bit d'un pixel de l'image est modifié, il ne correspond plus à la signature, de sorte que toute manipulation puisse être détectée. Cependant, cette signature est une méta-donnée qui doit être transmise avec la photographie, dans un champ de l'en-tête de l'image à transmettre. Si l'image est copiée ensuite dans un autre format de fichier qui ne contient pas ce champ de l'en-tête, la signature sera perdue et l'image ne peut plus être authentifiée. La solution préférable est d'insérer la signature directement dans l'image en utilisant les techniques de tatouage numérique.

Contrairement aux applications de protection des droits d'auteur, les données insérées pour but d'authentification devraient être fragiles dans le sens où elles devraient être facilement modifiées lorsque les données sont manipulées. Cet objectif peut être atteint avec des techniques de tatouage fragile qui sont peu robustes à certaines modifications (compression JPEG).

Dans ce chapitre, nous présentons le problème d'authentification, et les solutions proposées pour résoudre ce problème. Nous commençons par la solution de signature numérique, ensuite nous nous intéressons au tatouage fragile pour assurer un service d'authentification et d'intégrité d'images.

4.2 Problématique d'intégrité des images numériques

Le service d'intégrité 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 applicable à tout type de documents numériques, néanmoins, ce service s'avère être trop strict et pas bien adapté aux documents images.

Le problème de l'intégrité des images se pose principalement en termes de contenu sémantique, c'est-à-dire la détection des modifications du document pouvant engendrer une gêne dans sa visualisation et/ou une erreur dans son interprétation (modification de la légende, disparition d'un visage, etc.). Afin d'assurer un service d'intégrité approprié aux images, il est donc important 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, ré-échantillonage, filtrage, etc.) réalisées 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 [85, 66].

En effet, les critères d'intégrité d'une image artistique et une image médicale ne seront pas les mêmes. Dans le premier cas, une compression JPEG n'affecte pas la perception de l'image. Tandis que dans le second cas, des manipulations anodines, comme une simple compression, voir le processus d'insertion de la signature lui-même, peuvent causer la disparition de certains signes visibles d'une pathologie faussant alors le diagnostic du médecin. Dans ce contexte, l'utilisation de méthodes, dites classiques, sera plus appropriée pour garantir une intégrité stricte du document [85, 84].

Dans ce cas, une définition stricte de l'intégrité est alors requise. La première classe de ces méthodes est le tatouage inversible [31], en ce sens que, si l'image est réputée authentique, la distorsion dûe au processus du tatouage peut être retirée pour obtenir l'image originale.

Dans [13], les auteurs proposent une autre approche qui consiste à séparer l'image en deux zones : la première région est une zone d'intérêt (ROI) qui est la partie de l'image utilisée pour le diagnostic, où l'intégrité des données doit être strictement contrôlée, et la deuxième région (où les distorsions sont autorisée) permettant d'intégrer les données d'authentification.

4.2.1 Schéma générique d'un système d'authentification d'image

Dans [103, 59], les auteurs proposent un schéma générique d'un système d'authentification d'images. Ce dernier doit satisfaire les critères suivants :

- **Sensibilité :** le système doit être capable de déceler des manipulations pouvant modifier l'interprétation que l'on a d'une image ;
- **Tolérance :** le système doit être tolérant vis-à-vis des algorithmes de compression avec pertes 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 capable de donner une information visuelle permettant d'identifier rapidement les régions qui ont été manipulées ;
- **Reconstruction des régions altérées :** éventuellement, le système doit avoir la capacité de restaurer, même partiellement, des zones qui ont été manipulées ou détruites, afin de permettre à l'utilisateur de savoir quel était le contenu original des zones manipulées.
- **Mode de stockage :** les données d'authentification devraient être intégrées dans l'image elle-même, sous la forme d'un watermark, plutôt que dans un fichier séparé, comme dans le cas d'une signature externe.
- **Mode d'extraction :** suivant que les données d'authentification sont dépendantes ou non de l'image, on favorisera pour un mode d'extraction du tatouage *aveugle* ou *semi-aveugle*. En mode d'extraction aveugle, le watermark (les données d'authentification) est récupérée utilisant seulement l'image tatouée (et éventuellement attaquée), tandis qu'en semi-aveugle il s'agit particulièrement de vérifier la présence de tel watermark dans une image (via un

score de corrélation). Il est très clair qu'un mode d'extraction non aveugle n'est pas préféré pour un service d'intégrité dans la mesure où il fait appel à l'image originale ;
- **Algorithme asymétrique :** Contrairement aux services de sécurité classiques tels que la protection des droits d'auteur, un service d'authentification nécessite une asymétrie de l'algorithme de tatouage (ou cryptage). Par exemple, seul l'auteur d'une image peut l'assurer, mais n'importe quel utilisateur doit être en mesure de vérifier le contenu d'une image).
- **Visibilité :** les données d'authentification doivent être invisibles (dans les conditions normales de visualisation). C'est une question de s'assurer que l'impact visuel du tatouage est aussi faible que possible afin que l'image tatouée reste fidèle à l'original.
- **Robustesse et sécurité :** les données d'authentification doivent être protégées par des méthodes de chiffrement de manière à éviter qu'elles soient falsifiées ou manipulées.
- **Protocoles :** les protocoles sont un aspect important de tout système d'authentification d'images. Il est évident que n'importe quel algorithme seul ne peut pas garantir la sécurité du système. Il est nécessaire de définir un ensemble de scénarios et des spécifications décrivant le fonctionnement et les règles du système, telles que la gestion des clés ou des protocoles de communication entre le propriétaire, vendeur, client, etc.

4.3 Approches basées sur la signature électronique

Les schémas de signature permettent de garantir l'intégrité d'un fichier et l'authentification de l'émetteur. Les signatures électroniques doivent garantir les mêmes propriétés que les signatures manuscrites. Elles doivent pouvoir être opposées aux signataires. La propriété de non-répudiation assure au destinataire d'un message signé que son signataire ne pourra pas déclarer qu'il ne l'a pas signé [21].

4.3.1 Généralités sur les schémas de signature électronique

Propriétés

Une signature électronique doit :
- Dépendre du message signé ;
- Employer une information unique propre à l'expéditeur pour empêcher la contrefaçon et le démenti ;
- Être relativement facile à produire, à reconnaître et à vérifier ;
- Être mathématiquement infaisable à forger (par construction de nouveaux messages pour une signature numérique existante, ou par construction d'une signature numérique frauduleuse pour un message donné) ;
- Être facile à stocker.

Un schéma de signature est composé d'un algorithme de génération de clé, d'un algorithme de génération de signature et d'un algorithme de vérification de signature. L'algorithme de génération de clé retourne une clé publique k_p et une clé de signature k_s. Ensuite, l'algorithme prend comme entrée un message m et une clé k_s et génère une signature s pour le message m.

L'algorithme de vérification de signature prend comme entrée le message m, la signature s et la clé k_p et retourne un bit 0 si la signature n'est pas correcte pour le message m et 1 si la signature est valide. Un algorithme de signature doit être capable de signer des messages de taille quelconque.

Pour des raisons de performance et de sécurité des schémas, on ne signe pas en général tout le message m mais seulement un haché h. Ce modèle de schémas de signature est appelé *hash and sign*. Le problème est que deux messages qui ont la même image par H auront la même signature. Il est donc essentiel que les fonctions de hachage employées vérifient les propriétés de résistance aux collisions et de résistance à une seconde pré-image.

La propriété de résistance aux collisions est essentielle car elle permet par exemple d'empêcher un signataire de répudier une signature en créant des fichiers ayant la même image par H. Si un signataire est capable de trouver des collisions pour deux messages x et x', alors il pourrait renier une signature sur le message x en prétendant avoir signé le message x'. De même, la propriété de résistance à un deuxième antécédent empêche un attaquant de trouver un deuxième message ayant la même signature qu'un message signé donné [26].

4.3.2 Signature électronique pour les images numériques

4.3.2.1 Fonctions de hachage

On parle de "haché", de "résumé", ou de "condensé" pour nommer la caractéristique d'un texte ou de données uniques. La probabilité d'avoir deux messages avec le même haché doit être extrêmement faible. Le haché ne contient pas assez d'informations en lui-même pour permettre la reconstitution du texte original. L'objectif est d'être représentatif d'une donnée particulière et bien définie (en l'occurrence le message).

Les fonctions de hachage possèdent de nombreuses propriétés :

- Elles peuvent s'appliquer à n'importe quelle longueur de message m ;
- Elles produisent un résultat de longueur constante ;
- Il doit être facile de calculer $h = H(M)$ pour n'importe quel message m ;
- Pour un h donné, il est impossible de trouver x tel que $H(x) = h$. On parle de propriété à sens unique ;
- Pour un x donné, il est impossible de trouver y tel que $H(y) = H(x)$, résistance faible de collision ;
- Il est impossible de trouver x, y tels que $H(y) = H(x)$, résistance forte de collision ;

En d'autres termes, une fonction de hachage sert à produire un condensé (ou une empreinte) unique, représentatif du document original. Il existe de nombreuses fonctions de hachage parmi lesquelles on peut citer : MD-4, MD-5 (Message Digest), CRC-32 (32 bits Cyclic Redundancy Check), SHA-1 (Secure Hash Algorithm), etc [21].

Row-column hash function

La technique « row-column hash function » [100] consiste à calculer une valeur de hachage pour chaque ligne et chaque colonne de l'image originale. Lorsque l'on souhaite vérifier l'intégrité d'une image, on recalcule les valeurs de hachage des lignes et des colonnes de l'image à tester et on les compare avec celles de l'image originale (Figure 4.1).

Pour localiser les éventuelles disparités, il suffit d'identifier les lignes et les colonnes qui sont différentes. Cependant, dans le cas où plusieurs zones de l'image ont été modifiées, on n'est plus capable de les localiser sans ambiguïté, c'est-à-dire, que des régions intègres seront considérées comme altérées , ce qui réduit considérablement l'intérêt de cette technique [83].

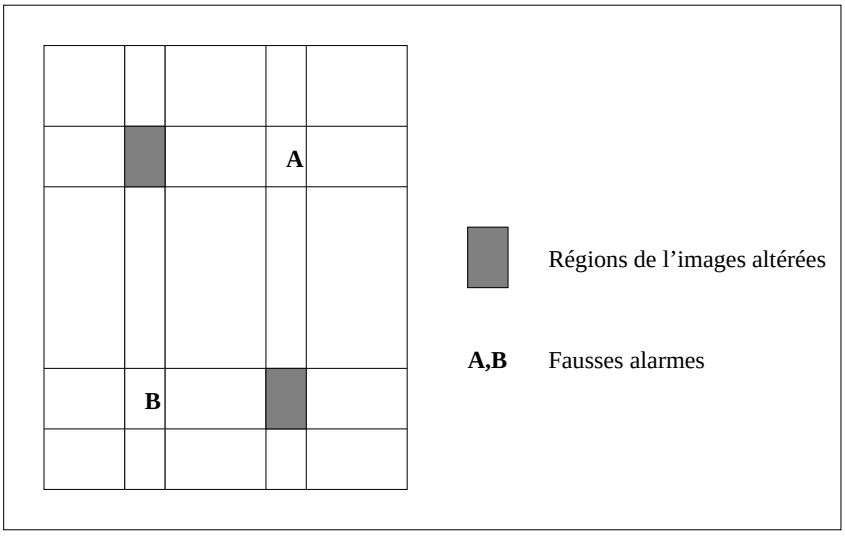


FIG. 4.1 – Ambiguïté dans la localisation des régions altérées de l'image.

Block based hash function

Un autre algorithme utilise également des fonctions de hachage, il s'agit du Block-Based Hash function (BBH) [100]. Le principe est similaire à celui décrit précédemment, à la différence près qu'il n'opère plus sur les lignes ou les colonnes de l'image, mais sur des blocs [83].

Ainsi lorsque l'on constate des différences dans les valeurs de hachage, il suffit de se reporter aux blocs concernés pour localiser les zones de l'image qui ont été manipulées. Les fonctions de hachage ont la particularité d'être extrêmement sensibles à la moindre variation ; en effet il suffit de modifier la valeur d'un pixel d'un seul bit pour changer radicalement la valeur de hachage du bloc associé. Elles ne permettent donc pas de distinguer les manipulations malveillantes des manipulations bienveillantes (i. e., utilisateurs ou fournisseurs de contenus) [84].

4.3.2.2 Signature basée sur des caractéristiques de l'image

Contrairement aux techniques ayant recours à des fonctions de hachage pour générer une empreinte de l'image, certains auteurs [82, 58, 59] proposent d'extraire des caractéristiques intrinsèques de l'image, telles que les contours, et de les crypter à l'aide d'un algorithme de chiffrement asymétrique afin de les transmettre en même temps que l'image [83, 85].

La figure 4.2 représente le processus de génération de la signature (a), et le processus de vérification de l'intégrité (b).

Dans le cas d'un système d'authentification basé sur l'utilisation d'une signature externe, la distinction entre des manipulations innocentes et malveillantes repose principalement sur le choix

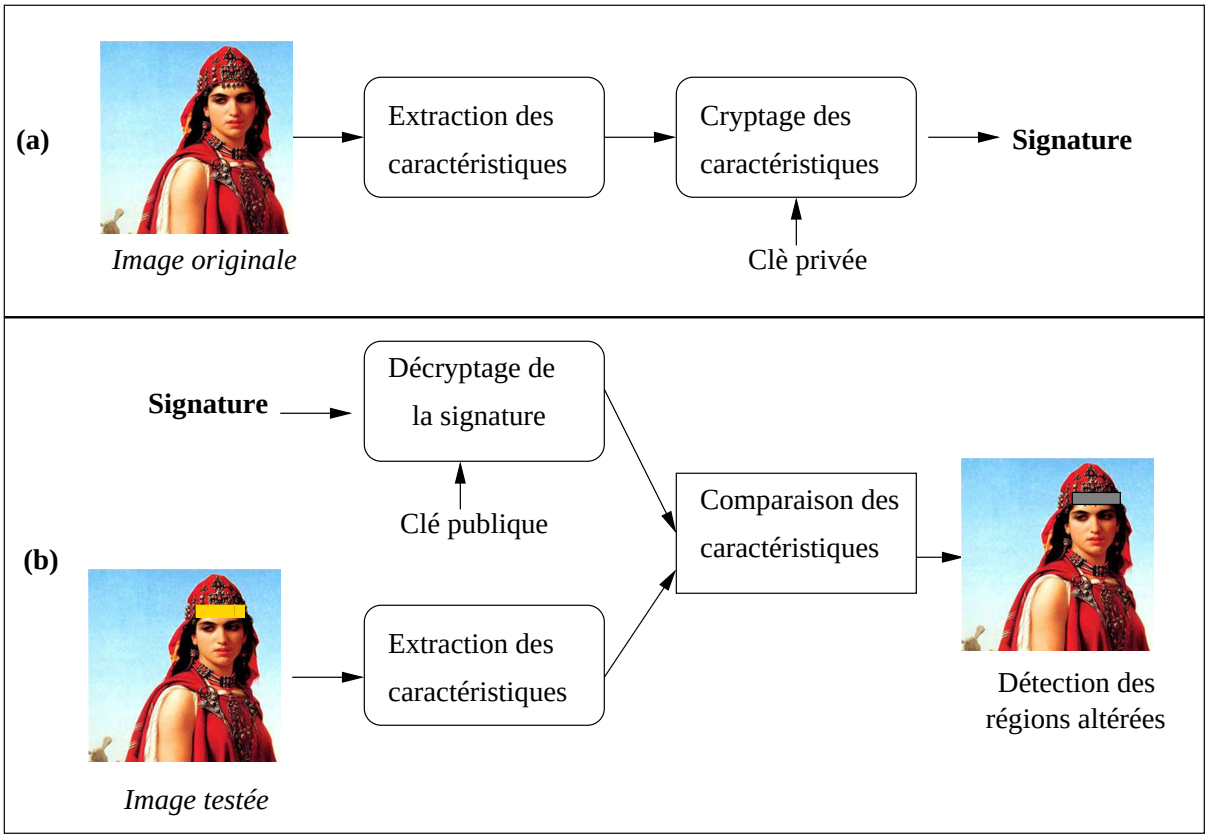


FIG. 4.2 – Principe général d'un système d'authentification utilisant une signature externe.

des caractéristiques de l'image pour générer la signature. Ce problème est exactement le même que celui rencontré par certaines méthodes semi-fragiles, à la différence près qu'ici la contrainte de quantité d'informations, liée à la capacité de l'algorithme de tatouage, ne se pose plus (puisque les informations sont stockées dans un fichier séparé). Certains auteurs, comme Lin et Chang [58], suggèrent de coder la relation d'ordre entre les coefficients DCT homologues de deux blocs distincts.

Queluz [82], quant à elle, opte pour des caractéristiques plus visuelles (principalement les contours), mais également moins stables. Pour compenser ce manque de stabilité, elle a mis en place des post-traitements complexes afin de réduire les fausses alarmes liées à une compression JPEG.

Bhattacharjee et Kutter [7] proposent également une technique ayant recours à une signature externe ; mais plutôt que d'extraire des caractéristiques par bloc d'image, ils suggèrent de rechercher des points d'intérêts (basée sur les travaux de Manjunath et al. [69]) et de coder leurs coordonnées. La signature ainsi obtenue est ensuite chiffrée à l'aide d'un algorithme à clé privée/publique tel que RSA (méthode de chiffrement asymétrique inventée par Ronald Rivest, Adi Shamir et Leonard Adleman [86]).

4.4 Approches basées sur le tatouage fragile

4.4.1 Modèle générique d'une technique de tatouage fragile

Cette section traite les techniques de tatouage pour assurer un service d'authentification. Le modèle général d'un système d'authentification basé sur le tatouage numérique est illustré dans la Figure 4.3.

Généralement, une clé secrète K connue par l'émetteur et le récepteur est utilisée pour générer un watermark W qui sera inséré dans l'image hôte f.

L'image tatouée f_w est ensuite délivrée par le canal de communication (par exemple, Internet, satellite, etc.) ou stockée dans une base de données.

Pour authentifier l'image reçue f_w^*, la même clé secrète est utilisée pour générer le watermark original W. Ce dernier est utilisé pour extraire et comparer la version intégrée W^* [89].

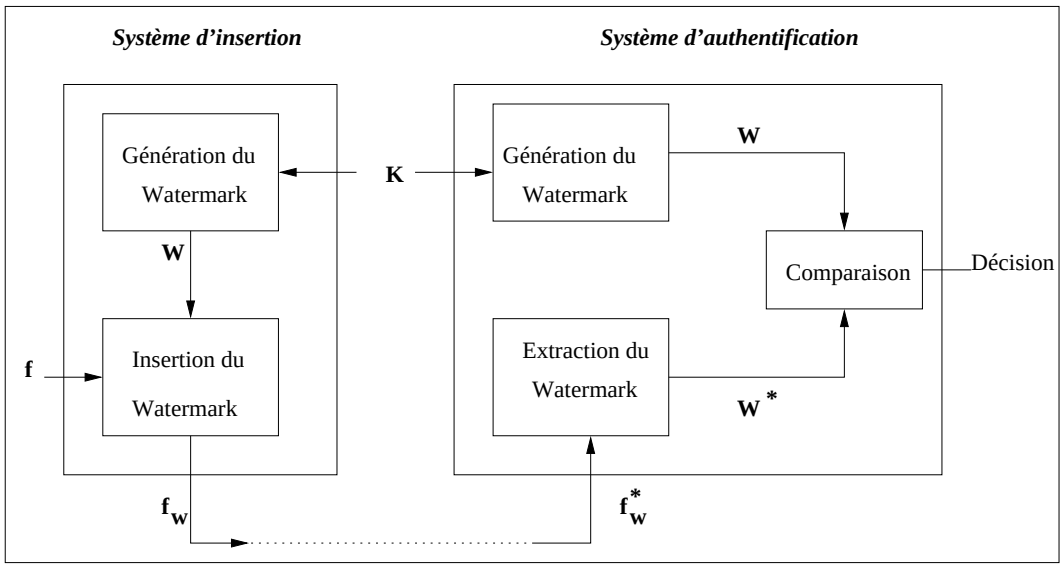


FIG. 4.3 – Le modèle général d'un système d'authentification basé sur le tatouage fragile.

4.4.2 Caractéristiques d'un système de tatouage fragile

- **Détection des falsifications :** une technique de tatouage fragile devrait détecter (avec une probabilité élevée) toute altération de l'image tatouée. C'est la propriété la plus fondamentale d'une méthode de tatouage fragile et elle est une exigence pour tester de manière fiable l'authenticité de l'image. Dans de nombreuses applications, il est également souhaitable de donner une indication de la quantité d'altération et sa localité (voir Caractéristique 4 ci-dessous).
- **Imperceptibilité :** le watermark inséré ne doit pas être visible par l'observateur [101]. Dans la plupart des cas il s'agit de préserver la qualité visuelle de l'image tatouée.

- **La phase de détection ne doit pas requérir l'image originale :** l'image originale peut ne pas être existée ou le propriétaire peut avoir des raisons de ne pas faire confiance à un tiers avec l'original (ce dernier pourrait alors placer son propre watermark sur l'originale et réclamer qu'il en appartient).
- **Le détecteur doit être capable de localiser et de caractériser les transformations apportées à une image tatouée :** cela inclut la possibilité de localiser les régions spatiales au sein d'une image modifiée. Le détecteur devrait aussi être en mesure d'estimer ce type de modification qui s'était passée.
- **La détectabilité du watermark après le recadrage (cropping) d'image :** dans certaines applications, la capacité de détecter le watermark après le recadrage est très souhaitable. Par exemple, un attaquant peut être intéressé par certaines parties (visages, des personnes, etc.) de l'image tatouée. Dans d'autres applications, cette fonctionnalité n'est pas requise, cependant le recadrage est traitée comme une modification.
- **Les watermark générés par différentes clés de tatouage devraient être «orthogonales» lors de la phase de détection :** le watermark généré à l'aide d'une clé particulière doit être détecté seulement en fournissant au détecteur les informations de détection correspondantes.
- **L'espace des clés de tatouage doit être suffisamment grand :** cela permet d'accueillir de nombreux utilisateurs et à entraver la recherche exhaustive d'une clé particulière, même si des parties hostiles, sont en quelque sorte capable d'obtenir à la fois les versions tatouées et la version originale d'une image particulière.
- **L'insertion du watermark par des personnes non autorisées doit être difficile :** une attaque particulière mentionnée dans [73] consiste en la suppression du watermark d'une image tatouée, et l'insertion de ce dernier dans une autre image.
- **Le watermark doit être capable d'être inséré dans le domaine fréquentiel :** cela ne signifie pas que le watermark devrait survivre à la compression, qui peut être considérée comme une attaque. La possibilité d'insérer le watermark dans le domaine fréquentiel constitue un avantage important dans de nombreuses applications [60].

4.4.3 Types d'attaques

Il faut être attentif aux éventuelles attaques lors de la conception et l'évaluation des systèmes de tatouage. Pratiquement, il est très difficile de concevoir un système sensible à toute forme d'attaque mais la connaissance sans doute des modes d'attaque est une obligation pour la conception de systèmes efficaces.

Le premier type d'attaque est la modification aveugle d'une image tatouée (c'est-à-dire changer arbitrairement l'image en supposant qu'aucun watermark n'est présent). Cette forme d'attaque doit être facilement reconnue par toute technique de tatouage fragile, mais nous le mentionnons parce qu'il peut être le type le plus courant d'attaque qu'un système de tatouage. Des variantes de cette attaque sont le recadrage et le remplacement localisés (notamment, en substituant le visage d'une personne à une autre). Ce dernier type de modification est une raison importante pour laquelle une application de tatouage fragile doit être capable d'indiquer les régions sinistrées dans une image altérée [60].

Une des attaques les plus courantes contre les systèmes à base de tatouage fragile, consiste à tenter de modifier une image protégée sans affecter le watermark qu'elle contient, ou bien encore à tenter de créer un nouveau watermark que le détecteur considérera comme authentique. Prenons par exemple le cas volontairement simplifié où l'intégrité d'une image est assurée par un watermark fragile, indépendant du contenu, et inséré 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 le watermark soit dégradé et l'attaque détectée. Par contre, si on prend soin de modifier l'image sans toucher aux LSB, le watermark restera intacte et le système ne décèlera aucune falsification.

D'un point de vue plus général, dès lors que l'insertion est assurée par un watermark indépendant du contenu de l'image à protéger, il est possible d'imaginer une attaque qui recopie un watermark valide d'une image dans une autre (exemple : la « Copy Attack » de Kutter et al. [54]). De cette manière, la deuxième image se retrouve alors protégée. Ce type d'attaque peut également être effectuée sur la même image ; dans ce cas, le watermark est dans un premier temps retiré de l'image, l'image est ensuite manipulée, et enfin le watermark est réinséré dans l'image [84, 85].

Dans le même esprit, l'attaque « Collage-Attack » proposée par Fridrich et al. [30] qui consiste à créer une image contrefaite de toutes pièces à partir d'une banque d'images protégées par le même watermark et la même clé. Cette attaque ne présuppose aucune connaissance a priori sur le watermark binaire caché, ni sur la clé secrète utilisée. Son principe est relativement simple puisqu'il consiste à remplacer chaque pixel de l'image à manipuler par le pixel qui lui est le plus similaire parmi les pixels de même position des images de la base. La difficulté de cette méthode est de disposer d'une banque d'images suffisamment variées pour obtenir une image falsifiée de bonne qualité visuelle [84, 85].

Un attaquant peut être intéressé par la suppression totale du watermark. Pour ce faire, un attaquant peut ajouter un bruit aléatoire à l'image, en utilisant des techniques visant à détruire des watermark(telles que StirMark[2]), ou en utilisant une analyse statistique ou de collusion pour estimer l'image originale.

Une autre attaque classique consiste à essayer de trouver la clé secrète utilisée pour générer le watermark. Ce type d'attaque, également appelé « Brute Force Attack ». Une fois la clé trouvée, il devient alors très facile pour un pirate de falsifier le watermark d'une image protégée avec cette clé. La seule parade efficace est d'utiliser des clés de grande taille de manière à rendre cette attaque très dissuasive en termes de temps de calcul.

4.4.4 Algorithmes de tatouage fragile

Les premières méthodes proposées pour garantir un service d'intégrité des images étaient basées sur l'utilisation d'un tatouage fragile, par opposition au tatouage robuste classiquement utilisé pour la protection des droits d'auteur.

Le principe de ces approches est d'insérer un watermark indépendant des données à protéger dans l'image d'hôte de telle manière que les moindres modifications apportées à l'image se reflètent

[2]http ://www.cl.cam.ac.uk/ fapp2/watermarking/stirmark

également sur le watermark inséré. Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence du watermark inséré [85].

De se qui suit, nous présentons les algorithmes de tatouage fragile les plus connus :

4.4.4.1 Algorithme de Walton

L'algorithme proposé par Walton [98] en 1995 consiste à sélectionner, d'une manière pseudo-aléatoire (en utilisant une clé k), des groupes de pixels et de calculer, pour chacun d'eux, une valeur de «Checksum». Ces valeurs sont obtenues à partir des 7 bits MSB[3] des pixels sélectionnés, et sont ensuite insérées sous forme binaire au niveau des bits LSB[4]. Le principe de cet algorithme est présenté ci-après :

Algorithme d'insertion

Entrées :

– f : image hôte ;
– K : clé secrète ;
– N : entier suffisamment grand.

Sortie :

– f_w : image tatouée.

Étapes :

– Diviser f en blocs de taille 8×8 pixels ;
– Pour chaque bloc B_i :

1. Définir un ordre de parcours pseudo-aléatoire des 64 pixels $(p_1, p_2, , p_{64})$ en utilisant K ;
2. Générer une séquence pseudo-aléatoire de 64 entiers $(a_1, a_2, \cdots, a_{64})$ du même ordre de grandeur que N ;
3. La valeur de checksum S est alors calculée de la manière suivante :
   $S = \sum_{j=1}^{64}(a_j.g(p_j)) \mod N$;
   Avec $g(p_j)$ est le niveau de gris du pixel p_j en ne tenant compte que des 7 MSB.
4. Coder et crypter S en binaire ;
5. Insérer la séquence binaire obtenue au niveau des LSB des pixels du bloc B_i.

Algorithme de vérification

L'algorithme de vérification est similaire à celui d'insertion. Il consiste à vérifier pour chaque bloc, la valeur de « checksum » S^* recalculée à partir des MSB des pixels de l'image tatouée et éventuellement attaquée f_w^*, avec celle de l'image hôte f codée au niveau des LSB.

Cette méthode garantit une haute qualité des images tatouées, car les données d'authentification sont insérées directement aux niveaux des LSB de l'image.

D'autre part, elle a l'avantage d'être simple, rapide et sensible à la moindre modification de l'image (i.e., réponse binaire équivalente à une intégrité stricte). Si on échange, par exemple, les

[3]Main Significant Bits
[4]Last Significant Bits

MSB de deux pixels quelconques d'un même bloc, la valeur de S s'en trouvera automatiquement modifiée car chaque pixel p_j est multiplié par un coefficient a_j différent. De plus, l'ordre de parcours des pixels p_j ainsi que les valeurs des coefficients a_j sont dépendants du bloc, ce qui rend impossible un éventuel « copier/coller » entre deux blocs différents d'une même image [85].

Avec cette méthode, il est possible d'intervertir deux blocs homologues (i.e., de même position) de deux images protégées avec la même clé, sans que le système ne décèle une perte d'intégrité. Une solution simple à ce type d'attaque est de rendre le watermark dépendant du contenu de l'image [28].

4.4.4.2 Algorithme de Fridrich et Goljan

Fridrich et Goljan [29] proposent une méthode qui repose également sur l'utilisation des LSB, mais cette fois-ci, dans le but de cacher suffisamment d'informations afin de pouvoir non seulement déceler d'éventuelles manipulations, mais surtout de permettre une reconstruction partielle des blocs altérés.

Le principe de base consiste à découper l'image en blocs de taille 8×8 pixels, et on calcule les coefficients DCT en ne tenant compte que des MSB. Ces coefficients DCT sont ensuite quantifiés à l'aide de la table de quantification correspondant à une compression JPEG d'une qualité de l'ordre de 50%. La matrice quantifiée résultante est alors encodée sur 64 bits et insérée au niveau des LSB des pixels d'un autre bloc. Le bloc servant de support au tatouage doit être suffisamment éloigné afin d'éviter qu'une modification locale de l'image n'altère à la fois l'image et les données de reconstruction.

Comme c'est le cas de toutes les méthodes de tatouage utilisant les LSB comme support, l'impact visuel est très faible. Par contre, la qualité des régions restaurées est nettement inférieure à celle d'une compression JPEG 50%, mais largement suffisante pour informer l'utilisateur sur le contenu original de ces régions.

Afin d'améliorer légèrement la qualité de la reconstruction, les auteurs ont proposé une nouvelle variante. Dans cette version, la matrice quantifiée étant alors codée sur 128 bits (en utilisant les deux bits de poids faible). La reconstruction est certes meilleure, mais l'image tatouée perd sensiblement en qualité.

Le major inconvénient de cette méthode est lié à la nature très fragile du tatouage qui n'assure pas une restauration correcte lorsque plusieurs régions de l'image ont été modifiées. En effet, les données de reconstruction correspondant à un bloc erroné peuvent elles aussi être altérées si les LSB les supportant ont eux aussi été modifiés. Ce problème est d'autant plus vrai lorsque l'image subie des modifications globales, même « faibles », comme un filtrage passe-bas ou une compression JPEG [85].

4.5 Conlusion

Dans ce chapitre, nous avons présenté deux catégories de techniques pour garantir un service d'authentification et d'intégrité d'images numériques : techniques basées sur la signature électronique et techniques basées sur le tatouage fragile.

La principale différence entre ces deux catégories de techniques, c'est que dans les techniques de signature numérique, les données d'authentification (la signature) sont transmises dans un fichier (ou un en-tête) séparé des données brutes stockées dans le même dossier. Tandis que dans les techniques de tatouage, les données d'authentification (watermark) sont intégrées dans les données brutes.

Par rapport aux techniques de tatouage, les techniques de signature numérique ont potentiellement les avantages suivants :

- Elles ont une capacité de dissimulation des données d'authentification supérieure aux techniques du tatouage.
- Elles peuvent détecter le changement de chaque bit de l'image si l'intégrité stricte doit être assurée.

Les approches fondées sur la signature électronique ont certains points faibles :

- Le stockage de la signature numérique (dans un fichier séparé ou dans des segments distincts de l'en-tête du fichier contenant les données brutes) augmente le coût de la transmission. Lorsque le document signé est manipulé, la signature insérée n'est pas soumis au même processus de manipulation, ce qui rend difficile de déterminer les localités temporelle et spatiale, où l'altération se produit.
- Les signatures numériques utilisées ne sont pas adaptées pour des applications de transmission avec pertes. Par exemple, dans le cas d'encombrement du réseau, les couches à faible priorité du support (habituellement, les éléments à haute fréquence ou les détails) sont susceptibles d'être ignorées, ce qui rend les données reçues différentes des données originale. Le support reçu va échouer l'authentification.
- La conversion du format des supports protégés par des techniques de signature n'est pas toujours possible. Par exemple, convertir une image JPEG avec ses données d'authentification (signature), stockées dans l'entête à un autre format d'image sans aucun segment d'en-tête signifie que la signature sera perdue.

Par contre, les approches fondées sur le tatouage insèrent les données d'authentification dans l'image hôte directement. Les données d'authentification subissent les mêmes transformations effectuées sur l'image hôte. Par conséquent, les techniques de tatouage fragiles et semi-fragiles n'ont pas les deux premiers problèmes précités.

Par ailleurs, les techniques de tatouage semi-fragiles peuvent également contourner les deux derniers problèmes mentionnés ci-dessus [60].

Dans le chapitre 6 nous proposons une nouvelle méthode de tatouage fragile.

Deuxième partie

Algorithmes proposés

Chapitre 5

Algorithme du tatouage aveugle d'images couleurs RGB

Résumé : L'objectif de nos travaux est de proposer un nouveau algorithme du tatouage aveugle qui vise à insérer un watermark couleur RGB dans une image couleur RGB.

Dans cette nouvelle méthode nous nous sommes intéressés à trois défis. Le premier est la proposition d'un algorithme aveugle, car le caractère aveugle constitue un enjeu majeur dans les applications réelles. Cela permet de ne pas diffuser les données originales qui peuvent être détruites après tatouage. Le deuxième défi est le tatouage d'images couleurs. Cela est motivé par le fait que la couleur est devenus un élément clé pour beaucoup, si on dit pas tous les systèmes modernes de traitement d'images et de la vidéo. Enfin, le défi le plus primordial est de garantir un bon compromis entre l'imperceptibilité et la robustesse du watermark inséré. L'objectif de ce chapitre est de présenter la méthode proposée.

5.1 Introduction

Il est bien connu que la couleur joue un rôle primordial dans le cinéma numérique, les systèmes de photographie numérique comme les caméras numériques, les téléphones cellulaires et les imprimantes. En outre, la couleur est également cruciale dans la reconnaissance des formes multiples et les systèmes multimédias, où l'extraction de caractéristiques basée sur la couleur et de la segmentation de couleur se sont avérées pertinentes pour détecter et classer des objets dans divers domaines allant de l'inspection industrielle aux applications géométriques et biomédicales.

Malgré l'intérêt capital des images couleurs, la plus part des méthodes de tatouage d'images sont pointées vers les images à niveaux de gris. Pour cette raison, nous avons proposé une nouvelle méthode de tatouage numérique d'images couleurs.

Nous avons proposée une méthode Bloc-SVD, i.e., l'image hôte est décomposée en blocs avant l'application de la SVD sur chacun de ces blocs. Ensuite, chaque élément du watermark est inséré dans une SV du milieu du bloc correspondant.

Le choix de l'utilisation des SVs du milieu pour l'insertion du watermark est motivé par le fait que les grandes SVs sont plus importantes pour la qualité d'image et les petites SVs sont plus

sensible au bruit.

L'algorithme de détection est qualifié *aveugle*, i.e. seul l'image tatouée et la clé sont utilisées pour détecter le watermark.

Pour assurer le caractère aveugle de l'algorithme de détection, l'ordre décroissant des SVs doit être maintenu. Pour cela, nous avons proposé une nouvelle méthode pour maintenir cet ordre.

Dans ce chapitre, nous expliquerons l'implémentation de notre méthode. Nous commençons d'abord par l'algorithme d'insertion et ensuite l'algorithme de détection.

5.2 Méthode proposée

5.2.1 Modèle utilisé

En se basant sur le modèle générique présenté dans la section 2.3, le principe de notre méthode de tatouage est présenté par le schéma 5.1. L'algorithme d'insertion comprend en entrée un watermark W, une image hôte f et une clé secrète K spécifique au tatoueur. Cette phase d'insertion génère en sortie une image tatouée f_w.

La phase d'insertion est modélisée par la fonction suivante :

$$f_w = E(f, W, K). \tag{5.1}$$

L'image tatouée pourrait ensuite être copiée et attaquée. L'image reçue par la destination est notée f_w^*.

La phase d'extraction consiste à calculer une estimation W^* de W. Elle est modélisée par la fonction :

$$W^* = D(f_w, K). \tag{5.2}$$

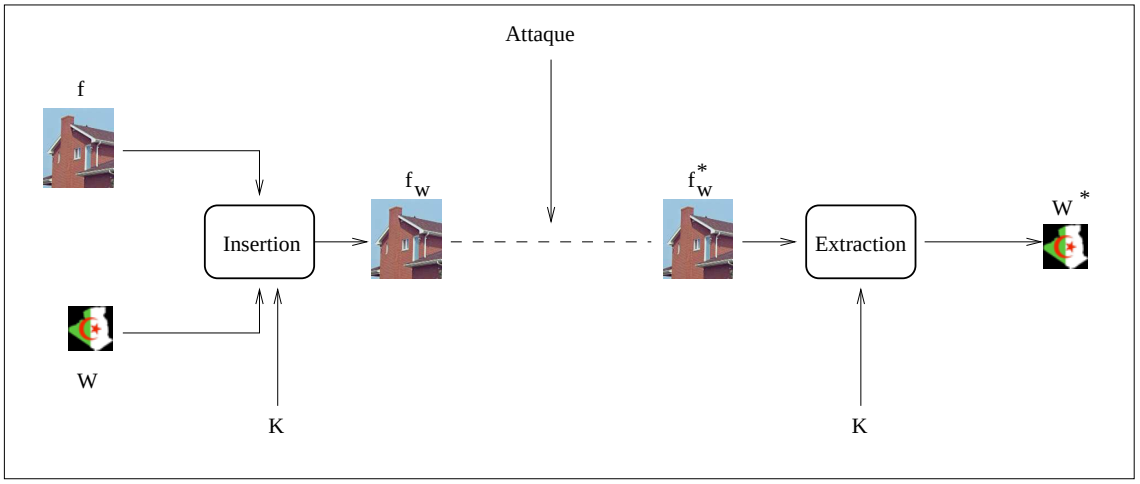


FIG. 5.1 – Modèle utilisé.

5.2.2 Algorithme d'insertion

Dans cette section, nous présentons l'algorithme d'insertion (voir Figure 6.4).
Le résultat dépend de deux constantes x et α où :
– x est l 'ordre de la SV du milieu utilisé ;
– α est un paramètre positif choisit pour maintenir la qualité de l'image tatouée.
Elles sont choisies expérimentalement et elles peuvent être vues comme clés privées (elles ne seront connues que des personnes ayant droit d'extraire le watermark).

Détaillons maintenant les différentes étapes de l'algorithme.

Entrées :
– f : image hôte (une image couleur RGB de taille $n \times m$) ;
– W : watermark (une image couleur RGB de taille $w \times h$).
– La clé secrète (x,α).

Sortie :
– f_w image tatouée (une image couleur RGB de taille $n \times m$).

Étapes :

1. Pour chaque composante de couleur $C \in \{R, G, B\}$ faire :
   (a) Diviser la composante C en blocs B_i de taille $\frac{n}{w} \times \frac{m}{h}$;
   (b) Pour chaque bloc B_i faire :
      i. La décomposition de B_i en valeurs singulières :

$$B_i = U_i S_i V_i^T; \tag{5.3}$$

      λ_i sont les SVs de B_i (éléments diagonaux de S_i).
      ii. Insérer le pixel i de la composante C du watermark $W_C(i)$ directement dans une des SVs du milieu λ_x comme suit :

$$\lambda_x = \frac{W_C(i)}{\alpha}; \tag{5.4}$$

      iii. Maintenir l'ordre des SVs comme suit :
      – j=x-1, Tant que $\lambda_x > \lambda_j$ faire :
        $\lambda_j = \lambda_x$; j=j-1 ;
      – j= x+1, Tant que $\lambda_x < \lambda_j$ faire :
        $\lambda_j = \lambda_x$; j=j+1 ;
      iv. Utiliser les SVs modifiées (la matrice Sw_i) pour construire les blocs tatoués Bw_i :

$$Bw_i = U_i Sw_i V_i^T; \tag{5.5}$$

   (c) Reconstruire la composante tatouée C_w en utilisant les blocs tatoués.
2. Reconstruire l'image tatouée f_w à partir des trois composantes R_w, G_w et B_w

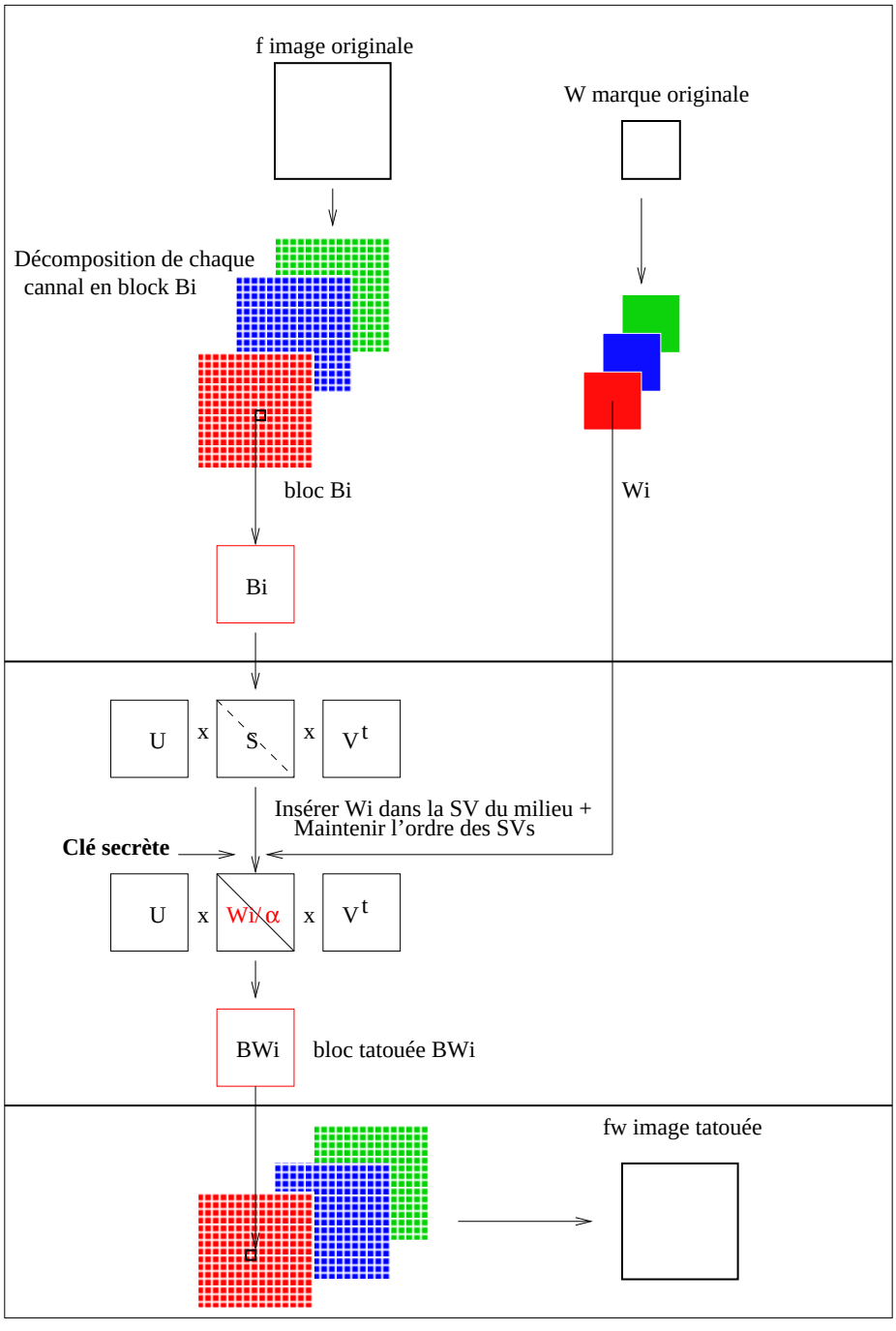


FIG. 5.2 – Algorithme d'insertion.

Exemple d'application de l'algorithme d'insertion :

Dans la suite, nous appliquons l'algorithme décrit ci-dessus à deux images hôtes Figure 5.3. La première (a) est très utilisée en traitement d'images (*Lena*), la deuxième (b) est l'image de l'*Emir Abdel Kader*.

On utilise deux watermarks : le premier (c) est le logo de *peugeot* qui sera utilisé pour tatouer Lena, le deuxième (d) est *la carte de l'Algerie* qui sera utilisé pour tatouer l'image Emir Abdel Kader.

Les images tatouées f_w de Lena et Emir sont respectivement (e) et (f).

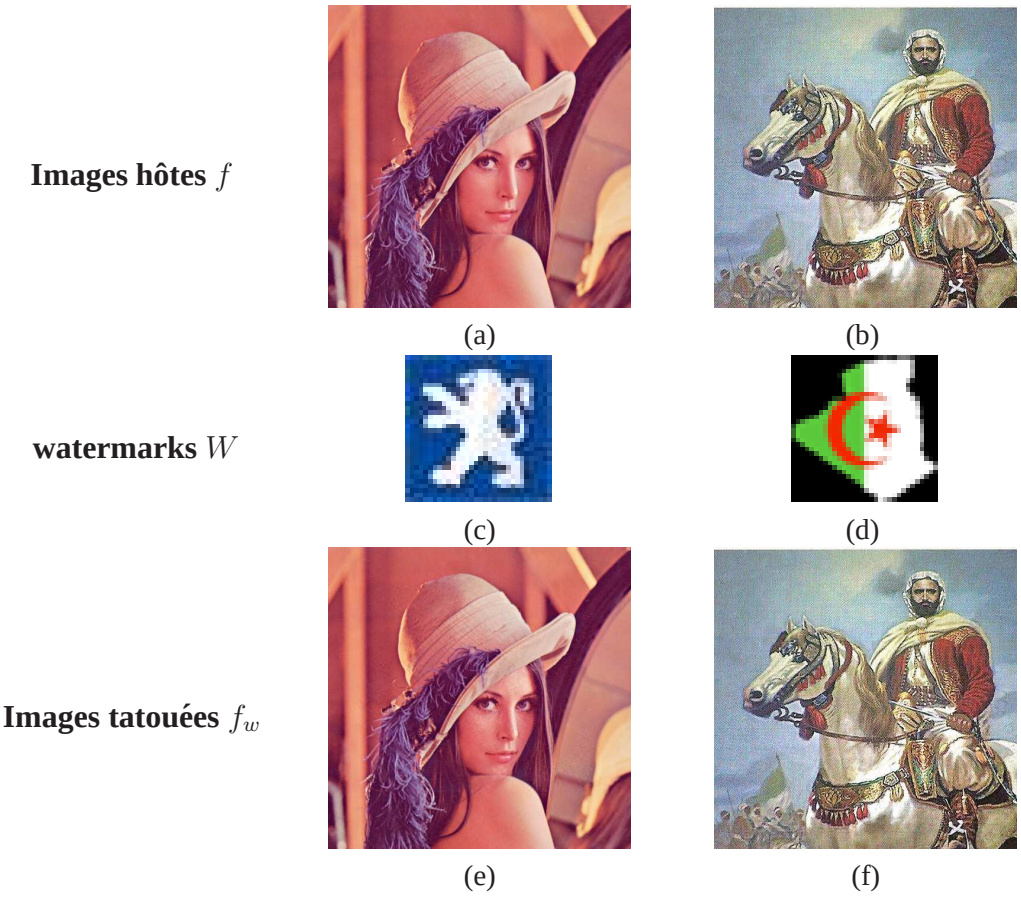


FIG. 5.3 – Exemple d'application de l'algorithme d'insertion.

5.2.3 Algorithme d'extraction

Dans cette section, nous présentons l'algorithme d'extraction (voir Figure 5.4).

Entrées :

– f_w^* image tatouée et éventuellement attaquée (une image couleur RGB de taille $n \times m$) ;
– La clé secrète (x,α) : la même clé utilisée par l'algorithme d'insertion.

Sortie :

– W^* : watermark extrait (une image couleur RGB de taille $w \times h$).

Étapes :

1. Pour chaque composante de couleur $C_w^* \in \{R_w^*, G_w^*, B_w^*\}$ faire :
   (a) Diviser la composante C_w^* en blocs Bw_i^* ;
   (b) Pour chaque bloc Bw_i^* faire :
      i. La décomposition de Bw_i^* en valeurs singulières :
      $$Bw_i^* = U_i^* S_i^* V_i^{*T}; \tag{5.6}$$
      ii. Le pixel $W_C^*(i)$ du watermark est obtenu à partir de la SV du milieu λw_x^* du bloc correspondant Bw_i^* comme suit :
      $$W_C^*(i) = \lambda w_x^* \times \alpha. \tag{5.7}$$
   (c) Construire la composante extraite W_C^* à partir des pixels extraits $W_C^*(i)$.
2. Construire le watermark extrait W^* à partir des trois composantes W_R^*, W_G^* et W_B^*.

Exemple d'application de l'algorithme d'extraction :

Dans la suite, nous appliquons l'algorithme décrit ci-dessus aux images tatouées f_w dans la Figures 5.3. Les watermarks extraits sont présentés dans la Figures 5.5, où (a) est le watermark extrait de l'image *Lena* et (b) est celui extrait de l'image *Emir*.

5.3 Simulations et résultats expérimentaux

Dans cet section, nous évaluons les performances de notre méthode en termes d'imperceptibilité et robustesse. Les résultats expérimentaux sont séparés en deux parties : la première est consacrée au teste de la propriété d'imperceptibilité alors que la deuxième est consacrée à l'analyse de la robustesse contre quelques types d'attaques standards et plus intéressants.

Dans toutes ces expériences, la clé K est (5,4), car les résultats obtenus avec ces paramètres sont meilleurs.

5.3.1 Propriété d'imperceptibilité

Afin de tester la propriété d'imperceptibilité de notre méthode de tatouage, plusieurs images couleurs RGB de taille 512×512 sont tatouées avec le logo de Peugeot de taille 32×32.

Les images hôtes et leurs images tatouées sont présentées respectivement dans les Figures 5.6 et 6.6.

A partir de ces figures, on peut voir qu'il est difficile de différencier entre les images originales et leurs images tatouées.

Les watermarks extraits à partir des images f_w sont illustrés par la figure 5.8.

Pour évaluer concrètement la qualité de notre méthode, on utilise le PSNR pour estimer la distortion des images tatouées.

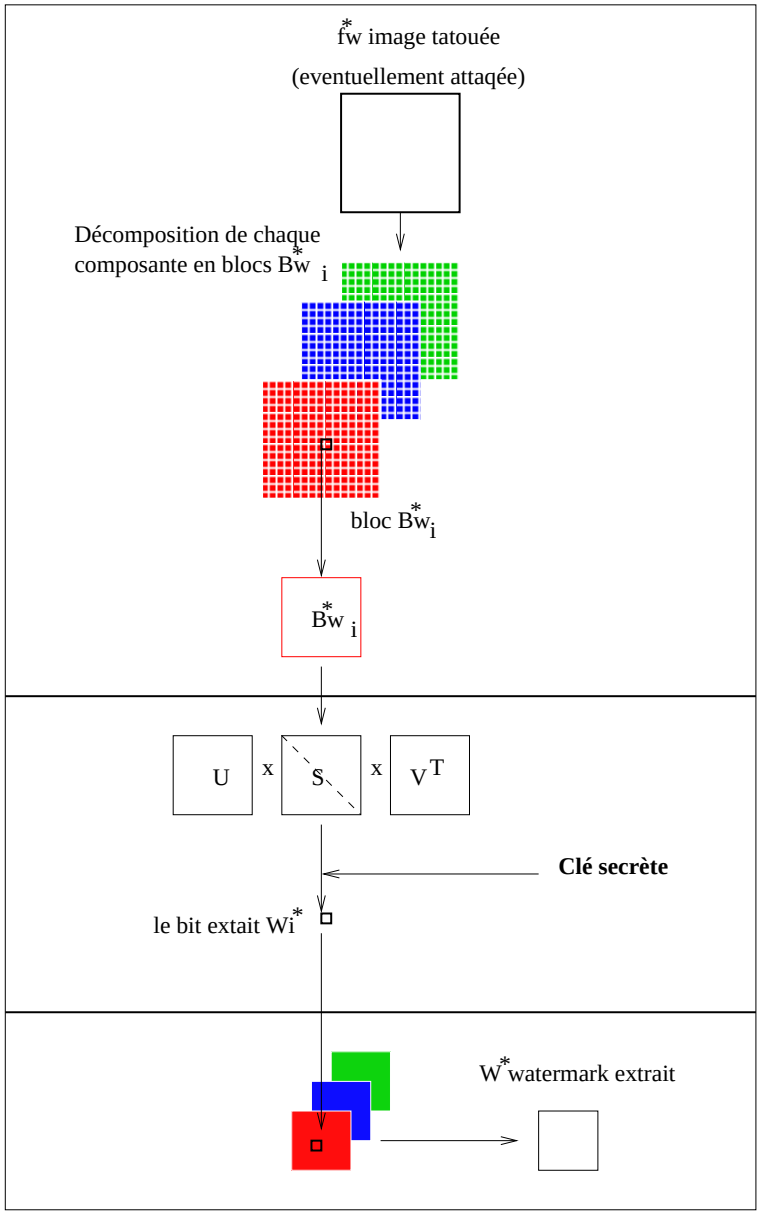


FIG. 5.4 – Algorithme d'extraction.

(a) (b)

FIG. 5.5 – Exemple d'application de l'algorithme d'extraction.

FIG. 5.6 – Images hôtes f.

FIG. 5.7 – Images tatouées f_w.

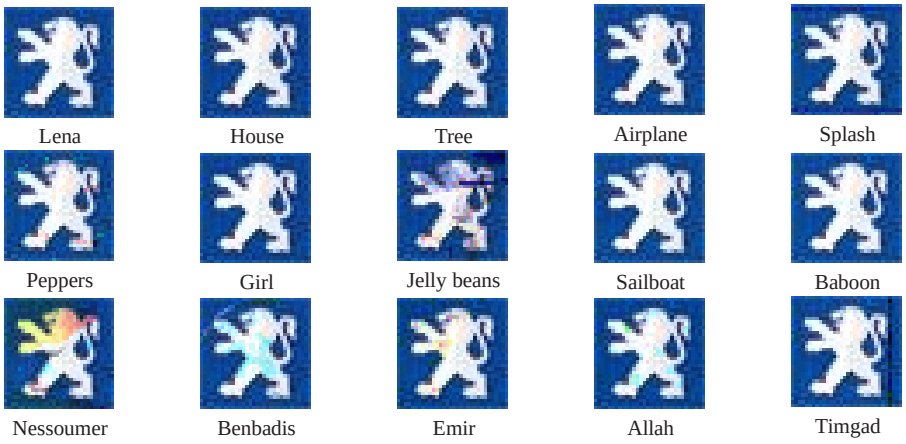


FIG. 5.8 – Watermarks extraits W^*.

Après l'extraction du watermark, le coefficient de corrélation est calculé en utilisant le watermark original et celui extrait. Ce coefficient permet de juger l'existence et l'exactitude du watermark extrait. Ces deux métriques sont présentées dans la Section 2.7.

Les valeurs du PSNR et du CC entre W et W^* sont présentées dans la Table 5.1.

Host image	PSNR	CC
Lena	44.2581	0.9990
House	43.5751	0.9990
Tree	43.5100	0.9985
Airplane	43.2926	0.9992
Splash	42.5156	0.9980
Peppers	42.4005	0.9912
Jelly beans	41.4907	0.9990
Girl	41.0879	0.9990
Sailboat on lake	40.0560	0.9991
Baboon	33.0856	0.9994
Fatma Nessoumer	43.2148	0.9146
Benbadis	42.2316	0.9866
Emir Abedel Kader	41.8159	0.9801
Allah	40.5846	0.9929
Timgad	37.3686	0.9864

TAB. 5.1 – Qualité des images tatouées et corrélation entre W et W^*.

5.3.2 Propriété de robustesse

Une propriété très importante que doit garantir un algorithme de tatouage est la robustesse contre les attaques.

Afin d'évaluer la robustesse de notre technique de tatouage, plusieurs types d'attaques ont été implantés. Dans cette partie, les expériences sont conduites sur l'image couleur RGB *House* de taille 512×512.

Les attaques contre la robustesse étudiées dans cette partie d'expériences sont classifiées comme présenté dans la Section 2.6. La première classe consiste en les attaques géométriques visant à déformer suffisamment le document tatoué. Tandis que, la deuxième classe consiste en les attaques d'effacement visant à supprimer le watermark.

5.3.2.1 Attaques géométriques

Rotation

Afin d'évaluer la robustesse de notre méthode contre la rotation, on effectue la rotation de l'image tatouée avec divers angles de rotation. La Figure 6.8 présente les images tatouées et attaquées et aussi les watermarks extraits à partir de ces dernières.

Les valeurs de CC (la Figure 6.8) montrent que notre méthode de tatouage résiste contre des petites angles de rotation.

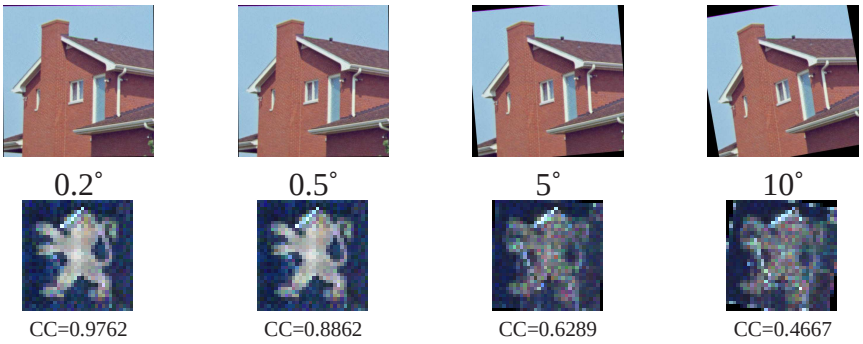


FIG. 5.9 – Performances contre la rotation.

Fliping

Pour analyser la robustesse de notre méthode contre le filiping, on effectue le fliping horizontal, vertical et total. La Figure 5.10 illustre les images tatouées et attaquées et aussi les watermarks extraits à partir de ces dernières.

Malgré que les valeurs de CC ne sont pas bonnes, les watermarks extraits peuvent être facilement reconnus par l'oeil humaine.

Cropping

Pour tester la robustesse de notre méthode contre le croping, les images tatouées sont coupées dans divers points. Les images tatouées et attaquées et aussi les watermarks extraits à partir de ces dernières sont illustrés par la Figure 5.11.

Généralement notre méthode résiste bien à l'opération de croping, que ce soit visuellement où par la métrique CC.

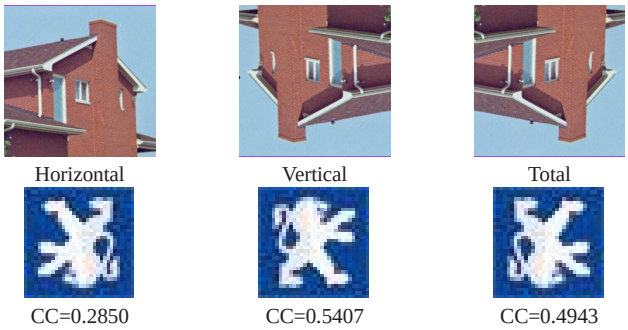


FIG. 5.10 – Performances contre le fliping.

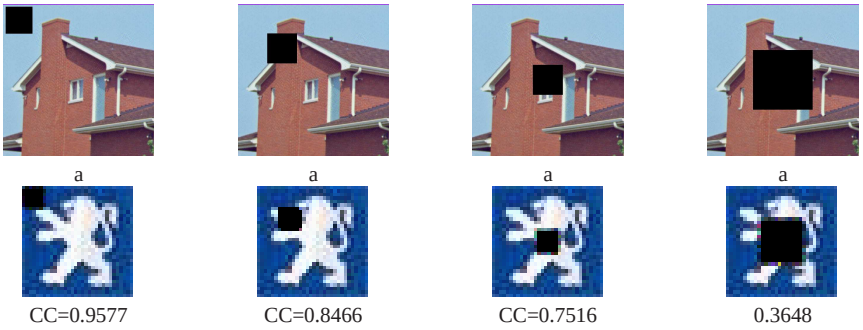


FIG. 5.11 – Performances contre le croping.

Zooming

Afin de tester la robustesse de notre méthode contre l'opération de zooming, les dimensions de l'image tatouée sont modifiées par divers ratios.

La Figure 5.12 illustre les watermarks extraits après des opérations de zooming.

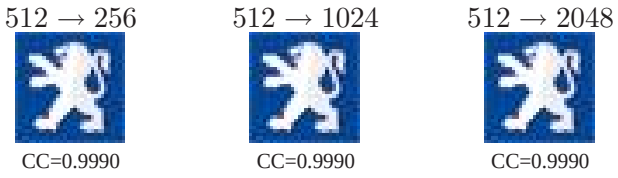


FIG. 5.12 – Performances contre le zooming.

D'après les valeurs de CC et la clarté des watermarks extraits, on conclue que notre méthode est très robuste contre l'opération de zooming.

5.3.2.2 Attaques d'effacement

Compression JPEG

On s'intéresse d'abord à la compression JPEG, car c'est le schéma de codage d'images le plus populaire et généralement considéré comme une attaque dure contre les algorithmes de tatouage d'images. En effet, plusieurs méthodes ne sont pas robustes à ce type d'attaque.

Le Table 5.2 montre que notre méthode est robuste contre la compression JPEG . Les watermarks extraits après la compression JPEG sont illustrés par la Figure 6.10.

Q (%)	80	60	50	35	25
Corrélation	0.861	0.829	0.815	0.810	0.777

TAB. 5.2 – Performances contre la compression JPEG.

80% 60% 50% 35% 25%

FIG. 5.13 – Watermarks extraits après la compression JPEG.

Filtrage

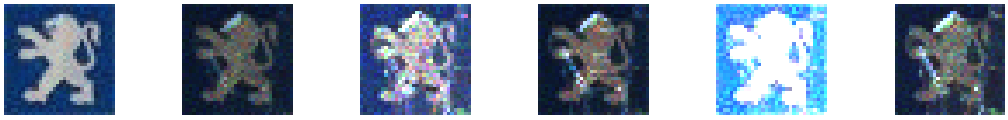
La Table 5.3 présente les divers types de filtres ainsi que les paramètres utilisés.

Type de filtre	paramètres	CC
Filtre Gaussian	3x3	0.9919
	5x5	0.9918
Filtre Average	3x3	0.8470
Filtre Laplacian	0.0	0.7892
	0.2	0.7767
	1.0	0.7508
Filtre de Wiener	3x3	0.7871
Filtre Median	3x3	0.6842
Filtre Sharpen	1.0	0.6128
	0.2	0.5693
	0.0	0.5406

TAB. 5.3 – Performances contre divers types de filtre.

La Figure 5.14 montre les watermarks extraits après les divers types de filtre utilisés.

A partir de la Table 5.3 et la Figure 5.14, on peut conclure que notre méthode est robuste contre certains types de filtres.



Gaussian Filter Average Filter Laplacian filtre Wiener filter Sharpen Filter Median Filter

FIG. 5.14 – Watermarks extraits après les divers types de filtre.

Débruitage

La Table 5.4 présente quelques types d'attaques avec divers paramètres.

Type of attaque	Paramètres	CC
Blurring	radius = 0.1	0.9990
	radius = 1.0	0.9566
Contrast adjustement		0.9939
Salt and pepper	Noise density=0.002	0.9494
	Noise density=0.008	0.7354
Gaussian Noise	M = 0.0, V = 0.001	0.8365
	M =0.1,V = 0.001	0.7945

TAB. 5.4 – Performances contre divers opérations de débruitage.

La Figure 5.15 montre les watermarks extraits après les divers attaques présentés dans la Table 5.4.

Blurring Constact Salt& pepper Gaussian Noise

FIG. 5.15 – Watermarks extraits après divers opérations de débruitage.

5.4 Conclusion

Dans ce chapitre, une nouvelle méthode de tatouage d'images couleurs RGB a été proposée. L'idée de base consiste à insérer un pixel du watermark dans une SV du milieu de l'image hôte. Cette nouvelle méthode est performante en termes d'imperceptibilité et de robustesse. Elle est aussi efficace car elle peut extraire facilement le watermark en utilisant seulement l'image tatouée, i.e., sans nécessité de l'image hôte ou d'autres matrices. Les résultats expérimentaux montrent que notre méthode maintien une haute qualité d'images tatouées et très robuste contre plusieurs attaques conventionnels.

Chapitre 6

Algorithme du tatouage fragile d'images couleurs RGB

Résumé : L'utilisation accrue des applications multimédia pose de plus en plus des problèmes concernant la préservation de la confidentialité et de l'authenticité de la transmission des données numériques. Ces données, et en particulier les images doivent être protégées de toute falsification. La solution adaptée est l'utilisation du tatouage fragile.

Le tatouage fragile peut être modélisé comme un problème de communication d'un signal sur un canal bruité. En effet, l'emploi des codes détecteur d'erreur apparaît naturel.

Dans ce chapitre, nous élaborons une nouvelle approche de tatouage fragile basée sur l'utilisation du contrôle de redondance CRC qui représente la méthode de détection d'erreurs la plus utilisée dans les télécommunications.

6.1 Introduction

Le développement des réseaux de communication et des supports numériques a encouragé l'utilisation des réseaux informatiques pour la transmission des informations numériques. Beaucoup d'organisations, à la foi publiques et privées, ont remplacé leurs dossiers, dispersés et tenus manuellement, par des systèmes informatiques leur offrant un meilleur accès aux données. Ce qui a posé le problème de la sécurité de ces données.

Dans ce contexte un nouveau schéma de tatouage fragile d'images couleurs est présenté. Le principe de ce schéma est basé sur l'utilisation du code CRC pour détecter les pixels modifiés. Le contrôle de redondance cyclique (noté CRC, ou en anglais Cyclic Redundancy Check) est un moyen de contrôle d'intégrité des données puissant et facile à mettre en œuvre. Il représente la principale méthode de détection d'erreurs utilisée dans les télécommunications. Pour ces raisons, on a choisit de l'utiliser dans le contexte du tatouage fragile afin de détecter si l'image a subi des modifications ou pas.

En utilisant le CRC, les séquences binaires sont traitées comme des polynômes dont les coefficients correspondent à la séquence binaire. On ajoute à la séquence binaire le reste d'une division

polynomiale (division par un polynôme générateur). A la réception, le reste de la division reçu et le reste de la division calculé doivent coïncider ou alors il y a erreur de transmission.

Notre nouveau schéma de tatouage est composé de trois phases. La première phase consiste à générer un watermark de taille 6 bits qui dépend des 18 bits MSB des trois pixels R,G et B en utilisant une clé secrète K. La deuxième phase consiste à insérer respectivement deux bits du watermark dans les deux bits LSB des pixels R, G et B. Enfin, la dernière phase consiste à détecter si l'image tatouée a subi des modifications. Si le reste de la division du message reçu (18 bits MSB des trois pixels R,G et B concaténés avec les 6 bits du CRC) sur la clé secrète K est égale à zéro, alors l'image est authentique à l'image originale, sinon elle n'est pas.

Dans ce chapitre, nous présentons le principe du schéma proposé ainsi que les résultats expérimentaux.

6.2 Contrôle de redondance cyclique CRC

6.2.1 Principe

Ce mécanisme consiste à protéger des blocs de données (trame) en ajoutant un code de contrôle. Ce code CRC contient des éléments redondants par rapport aux données transmises de manière à permettre la détection des erreurs. Il est utile dans le cas de transmission d'une grande série d'octets. Ce code est basé sur le fait que toute chaîne binaire permet de construire un polynôme, chacun des bits donnant sa valeur au coefficient polynomial correspondant. Ainsi la séquence binaire 10101001 peut être représentée sous la forme polynomiale suivante :

$1 * X^7 + 0 * X^6 + 1 * X^5 + 0 * X^4 + 1 * X^3 + 0 * X^2 + 0 * X^1 + 1 * X^0$.

soit $X^7 + X^5 + X^3 + X^0$.

ou encore $X^7 + X^5 + X^3 + 1$.

La mise en place du code CRC nécessite de choisir un polynôme de référence appelé *polynôme générateur* noté $G(X^d)$, qui est connu par l'émetteur et le récepteur. La détection d'erreur consiste pour l'émetteur à effectuer un algorithme (procédure de codage) sur les bits de la trame afin de générer un CRC, et de transmettre ces deux éléments au récepteur. Il suffit alors au récepteur d'effectuer le même calcul (procédure de décodage) afin de vérifier que le CRC est valide. La Figure 6.1 illustre le principe général de fonctionnement de CRC.

6.2.2 Procédure de codage et décodage CRC

Procédure de codage

Entrées :

– $P(X)$: polynôme associé à la séquence de bits à protéger ($P(X)$ est la représentation polynomiale du message à envoyer par l'émetteur).

– $G(X^d)$: polynôme générateur de degré d.

Sortie

– M : message envoyé au récepteur.

Étapes :

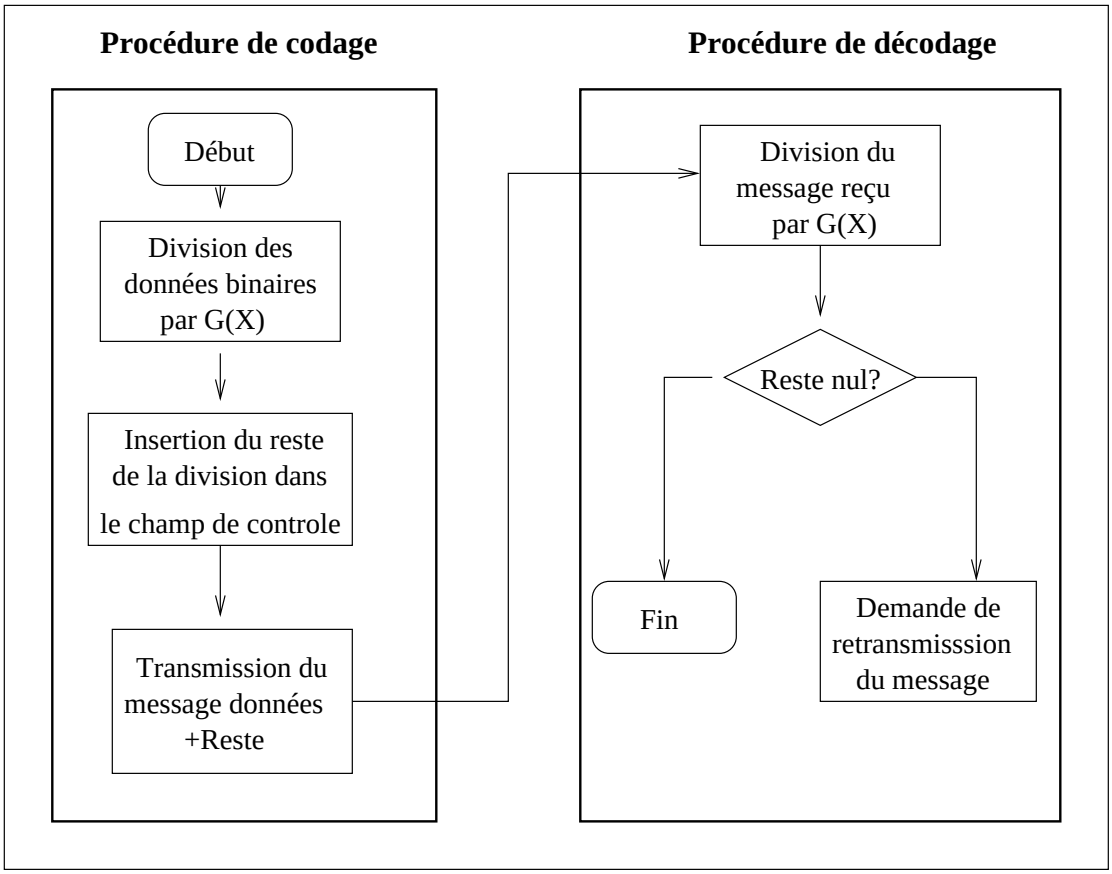


FIG. 6.1 – Principe de CRC.

1. On calcule $P'(X) = P(X).X^d$. Ceci est équivaut à un décalage de $P(X)$, de d positions vers la gauche.
2. On divise $P'(X)$ par $G(X^d)$: $P'(X) = Q(X).G(X^d) + R(X)$
3. Le message M envoyé est : $P'(X) + R(X)$.

Procédure de décodage
Entrée :
– Soit $M'(X)$ le polynôme associé à la séquence de bits reçus.
Sortie :
– Le reste de la divion de $M'(X)$ par $G(X^d)$.
Étapes :

1. On divise $M'(X)$ par $G(X^d)$.
2. Si le reste de division est non nul alors : détection d'une erreur.
3. Sinon (reste de division nul) il y a une forte probabilité que la transmission est correcte.

6.2.2.1 Exemple

Procédure de codage

- Soit la séquence 1101 à envoyer alors $P(x) = x^3 + x^2 + 1$;
- $G(x^3) = x^3 + x + 1$.
- $P'(x) = P(x).x^3 = x^6 + x^5 + x^3$;
- La division de $P'(x)$ par $G(x^3)$ comme suit :

$$\begin{array}{l|l}
x^6 + x^5 + x^3 & x^3 + x + 1 \\
\underline{x^6 + x^4 + x^3} & \overline{x^3 + x^2 + x + 1} \\
\quad x^5 + x^4 & \\
\quad \underline{x^5 + x^3 + x^2} & \\
\qquad x^4 + x^3 + x^2 & \\
\qquad \underline{x^4 + x^2 + x} & \\
\qquad\quad x^3 + x & \\
\qquad\quad \underline{x^3 + x + 1} & \\
\qquad\quad \mathbf{1} &
\end{array}$$

- $R(x) = 1$, alors le message envoyé M=1101**001**.

Procédure de décodage

- Soit la séquence reçue 1101001 alors $M'(x) = x^6 + x^5 + x^3 + 1$;
- $G(x^3) = x^3 + x + 1$;
- La division de $M'(x)$ par $G(x^3)$:

$$\begin{array}{l|l}
x^6 + x^5 + x^3 + 1 & x^3 + x + 1 \\
\underline{x^6 + x^4 + x^3} & \overline{x^3 + x^2 + x + 1} \\
\quad x^5 + x^4 + 1 & \\
\quad \underline{x^5 + x^3 + x^2} & \\
\qquad x^4 + x^3 + x^2 + 1 & \\
\qquad \underline{x^4 + x^2 + x} & \\
\qquad\quad x^3 + x + 1 & \\
\qquad\quad \underline{x^3 + x + 1} & \\
\qquad\quad \mathbf{0} &
\end{array}$$

- $R(x) = 0$, alors le message reçu est correcte.

6.3 Méthode proposée

6.3.1 Modèle utilisé

Le principe général de notre méthode est présenté dans la Figure 6.2.

L'algorithme de génération du watermark prend en entré l'image hôte f et la clé secrète K, et il génère en sortie un watermark de taille égale à la taille de l'image hôte. Cette phase est modélisée par la fonction G suivante :

$$W = G(f, K). \tag{6.1}$$

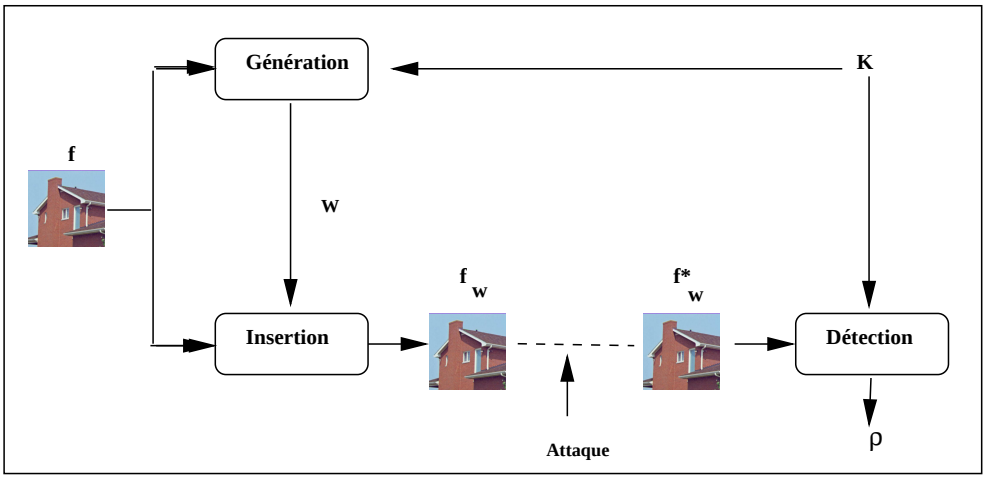


FIG. 6.2 – Modèle utilisé.

L'algorithme d'insertion génère l'image tatouée en utilisant l'image hôte f et le watermark W généré précédemment. Il est modélisé par la fonction d'insertion E comme suit :

$$f_w = E(f, W). \tag{6.2}$$

L'algorithme de détection (vérification) consiste à calculer une mesure ρ, en prenant en entrée l'image tatouée et éventuellement attaquée f_w^* et la clé K. Cet algorithme est modélisé par la fonction D comme suit :

$$\rho = D(f_w^*, K). \tag{6.3}$$

Si $\rho = 0$; alors l'image n'est pas attaquée sinon elle est attaquée.

6.3.2 Algorithme de génération du watermark

Cette phase génère un watermark de taille 6 bits qui dépend des 18 bits MSB des trois pixels R, G et B correspondants (voir Figure 6.3). Le détail de cet algorithme est présenté ci-dessous.

Entrées :

– f : Image hôte (une image couleur RGB de taille $n \times m$).

– K : clé secrète (polynôme générateur $G(X^d)$ de degré d (où $d = 6$).

Sortie :

– W : matrice de taille $n \times m$, où chaque élément $W(i, j)$ est une séquence binaire de taille 6 bits $\{W_1, \cdots, W_6\}$.

Étapes :

– Pour chaque pixel $R(i, j)$, $G(i, j)$ et $B(i, j)$ faire :

1. Construire le message m à transmettre à partir des trois pixels $R(i, j)$, $G(i, j)$ et $B(i, j)$ par la concaténation des 6 bits MSB.
2. Application de l'algorithme CRC :

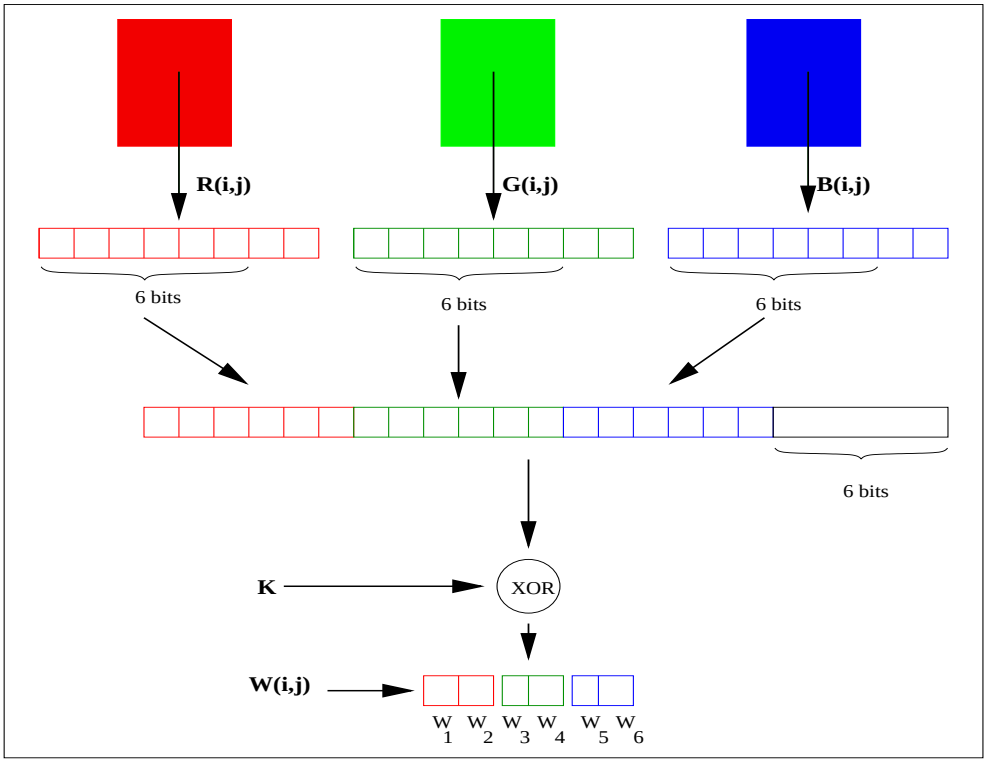


FIG. 6.3 – Algorithme de génération du watermark.

– Ajouter d bits nuls à m (dans notre cas en ajoute 6 bits)
– Le watermark $W(i,j)$ est égal au reste de la division (en binaire = opération XOR) de m par $G(X^d)$.

6.3.3 Algorithme d'insertion

Dans cet algorithme le watermark généré précédemment est inséré dans les deux bits LSB des trois pixels R, G et B correspondants (voir Figure 6.4). Le principe de cet algorithme est présenté ci-dessous.

Entrées :
– f : Image hôte : image couleur RGB de taille $n \times m$.
– W : watermark de taille $n \times m$.
Sortie :
– f_w : image tatouée de taille $n \times m$.
Étapes :
– Pour chaque pixel $R(i,j)$, $G(i,j)$ et $B(i,j)$ faire :

1. Remplacer les deux bits LSB de $R(i,j)$ par les deux premiers bits de $W(i,j)$.
2. Remplacer les deux bits LSB de $G(i,j)$ par les deux bits suivants de $W(i,j)$.

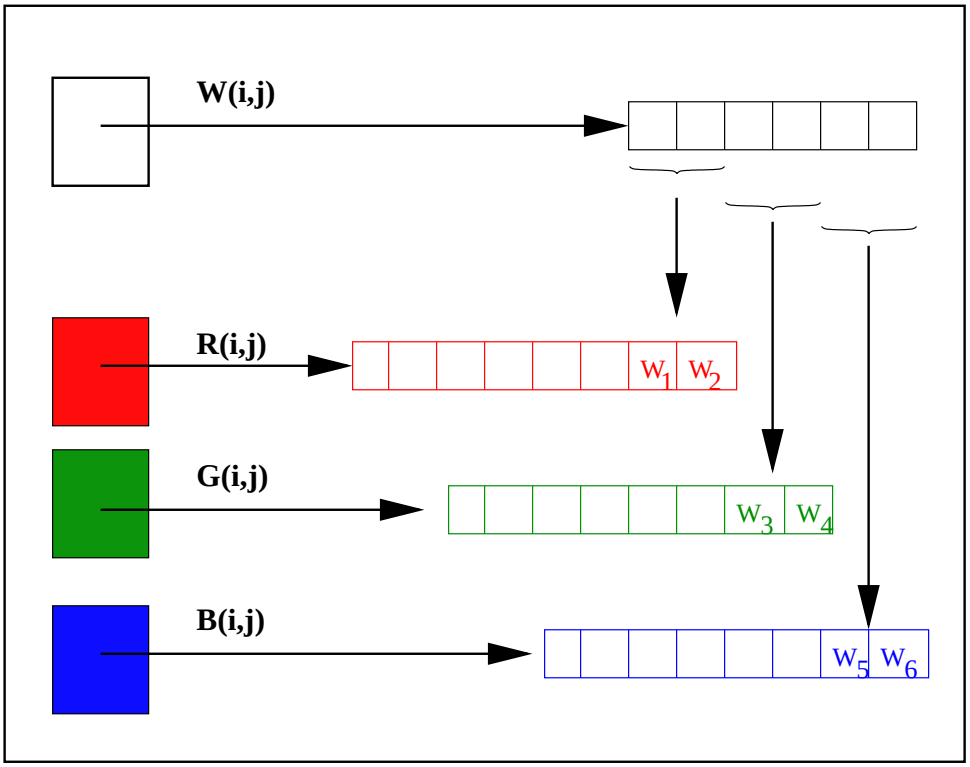


FIG. 6.4 – Algorithme d'insertion.

3. Remplacer les deux bits LSB de $B(i,j)$ par les deux derniers bits de $W(i,j)$.

6.3.4 Algorithme de détection

Dans cet algorithme, les 6 bits MSB des trois pixels R, G et B concaténés avec le CRC sont divisés sur la clé k, si le reste de cette division égale à 0 alors le pixel n'est pas attaqué, sinon il est attaqué (voir Figure 6.5). Le principe de cet algorithme est présenté ci-dessous.

Entrées :

– f_w : Image tatouée (image couleur RGB de taille $n \times m$).

– K : clé secrète utilisée par la phase de génération.

Sortie :

– ρ : mesure de confidentialité.

Étapes :

– Pour chaque pixel $R(i,j)$, $G(i,j)$ et $B(i,j)$ faire :

1. Construire le message m^* reçu à partir des 3 pixels $R(i,j)$, $G(i,j)$ et $B(i,j)$ par la concaténation des 6 MSB de chacun d'eux.
2. Extraction du watermark $W(i,j)$: IL est obtenu par la concaténation des 2 bits LSB de chaque pixel.

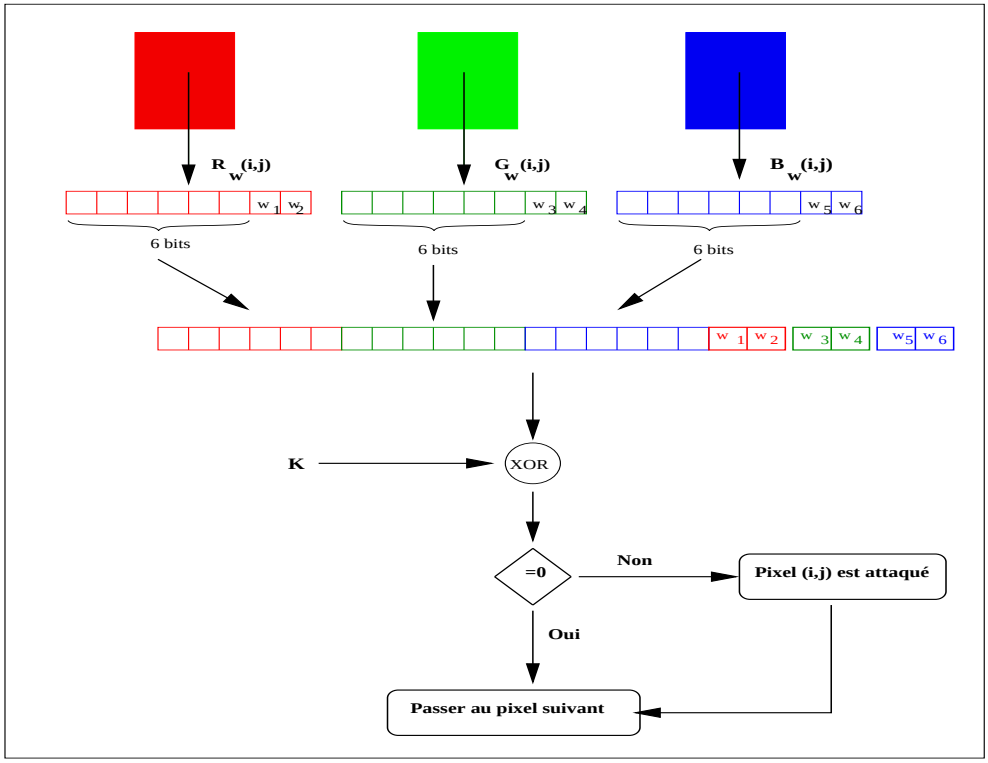


FIG. 6.5 – Algorithme de détection.

3. Application de l'algorithme CRC :
   - Ajouter les d bits de $W(i,j)$ à m^*.
   - Calculer ρ : le reste de la division de m^* par $G(X^d)$.
     - Si $\rho = 0$ alors le pixel (i,j) n'est pas modifié.
     - Sinon, il est modifié.

6.4 Simulations et résultats expérimentaux

Dans cette section, nous avons évalué l'efficacité de notre méthode en terme de degré de dégradation de l'image tatouée et la sensibilité et l'aptitude de détecter toute transformation dans l'image. Pour ceci, nous avons séparé les tests en deux parties : la première est d'analyser la propriété d'imperceptibilité et la deuxième est l'évaluation de la propriété de fragilité par rapport aux attaques.

6.4.1 Propriété d'imperceptibilité

Nous avons appliqué notre méthode à 12 images différentes de taille 128×128 afin de s'assurer des résultats obtenues.

Les images hôtes sont les mêmes que nous avons utilisé pour tester l'imperceptibilité de notre algorithme aveugle (Figure5.6) et leurs images tatouées sont illustrées dans la Figure 6.6.

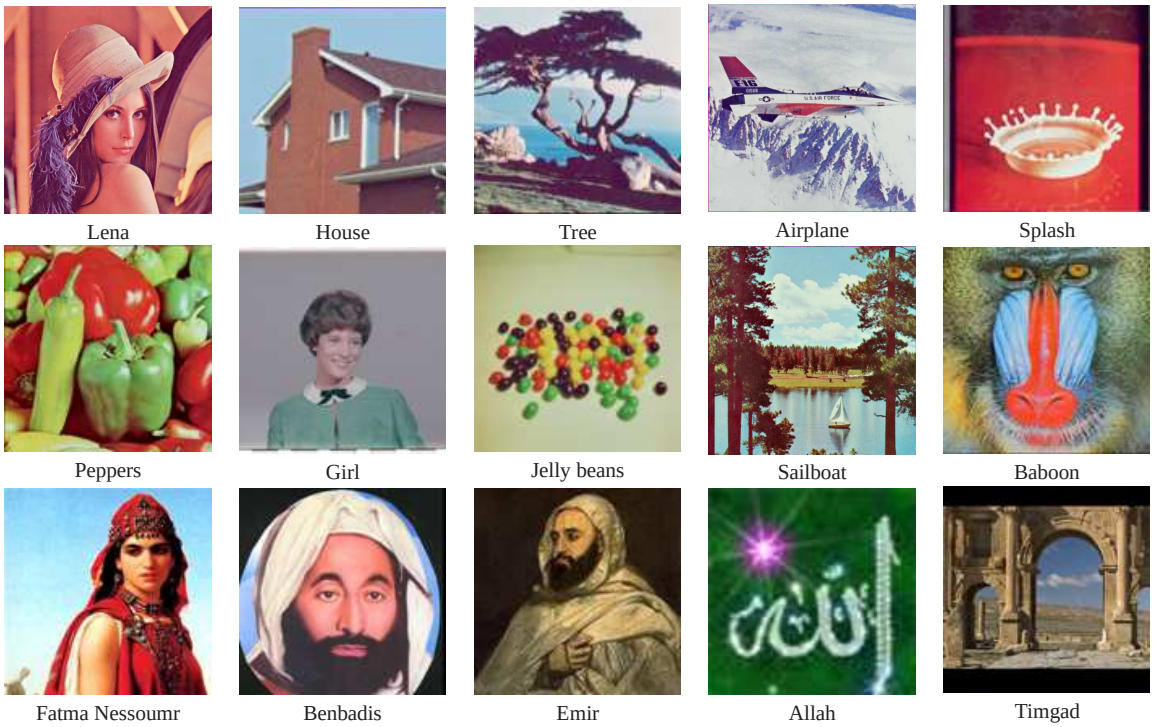


FIG. 6.6 – Images tatouées f_w.

A partir de ces figures, on peut voir que la dégradation des images tatouées est imperceptible par l'observateur.

Nous avons jugé utile de présenter aussi le PSNR des images tatouées afin de déterminer le degré de dégradation de l'image tatouée. La table 6.1 présente les valeurs de PSNR.

D'après cette dernière table 6.1, il est claire que les valeurs de PSNR sont très bonnes, ce qui signifie que notre méthode de tatouage maintien une haute qualité d'images tatouées.

6.4.2 Propriété de fragilité

La validité de toute technique de tatouage ne peut prendre de l'importance que si elle résiste à différents types d'attaques. Pour ceci, nous avons choisi de faire subir à chaque image tatouée un ensemble d'attaques et de vérifier la sensibilité de son tatouage et son aptitude de détecter toute transformation dans l'image.

L'image CRC est la matrice des restes de la division, elle est calculée afin de montrer si l'image est modifiée ou non (si la matrice est égale à 0 donc l'image n'est pas modifiée, sinon elle est modifiée).

La figure 6.7 présente certaines images CRC extraites à partir des trois premières images tatouées *Lena*, *House* et *Tree*.

Host image	PSNR
Lena	47.2578
House	47.4048
Tree	47.2048
Airplane	47.2914
Splash	47.0813
Peppers	47.2557
Jelly beans	47.1444
Girl	47.2048
Sailboat on lake	47.2407
Baboon	47.2633
Fatma Nessoumer	47.2853
Benbadis	47.4061
Emir Abedel Kader	47.2658
Allah	47.2109
Timgad	48.2409

TAB. 6.1 – Qualité des images tatouées.

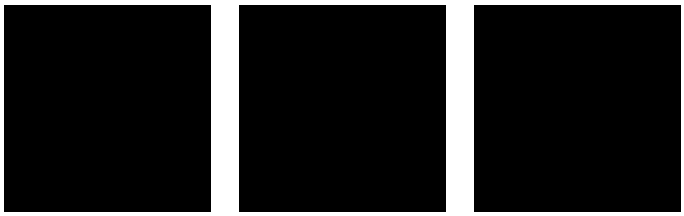


FIG. 6.7 – Images CRC extraites à partir des trois premières images tatouées.

En effet, nous avons appliquée des attaques de natures diverses sur l'image tatouée *House* et nous avons mesuré l'efficacité de notre technique et son aptitude à détecter toute anomalie dans l'image.

6.4.2.1 Attaques géométriques

Rotation

L'image tatouée est retournée avec des petites angles de rotation afin d'analyser la fragilité de notre méthode. Les images tatouées et retournées et leurs images CRC sont illustrées par la figure 6.8.

Les images CRC ne sont pas noires, ce qui signifie que notre méthode est très efficace contre les opérations de rotation, même avec des très petites angles de rotations.

Zooming

Afin d'évaluer la capacité de détecter les opérations de Zooming, les dimensions de l'image tatouée sont modifiées par divers ratios.

La Figure 6.9 illustre les images CRC extraites après différentes opérations de Zooming.

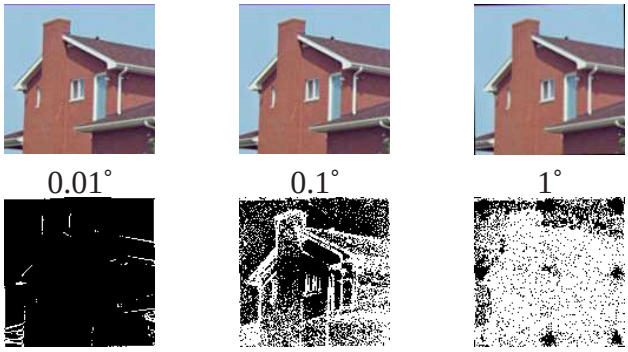


FIG. 6.8 – Performances contre la rotation.

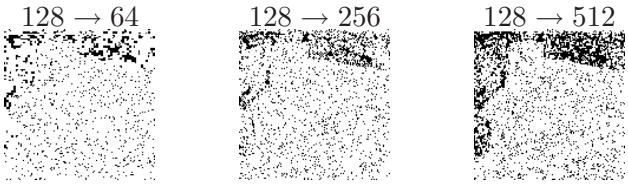


FIG. 6.9 – Performances contre le zooming.

D'après cette dernière, il est clair que notre méthode est capable de détecter les opérations de Zoming.

6.4.2.2 Attaques d'effacement

Compression JPEG

L'image tatouée est compressée avec divers facteurs pour tester la fragilité de notre méthode contre la compression JPEG. La figure 6.10 illustre les images CRC extraites après une compression JPEG.

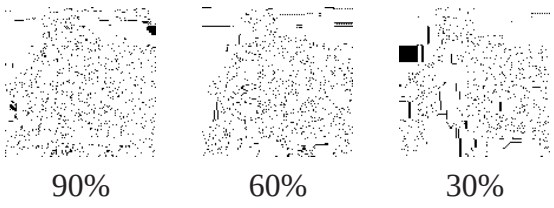


FIG. 6.10 – Performances contre la compression JPEG.

Les images CRC montrent que notre méthode est capable de détecter très efficacement la compression effectuée sur les images tatouées.

Filtrage

La Figure 6.11 présente les images tatouées et attaquées par divers de types de filtres ainsi que les images CRC extraites.

D'après cette dernière, on peut déduire que notre méthode est sensible aux divers types de filtres appliqués sur l'image tatouée.

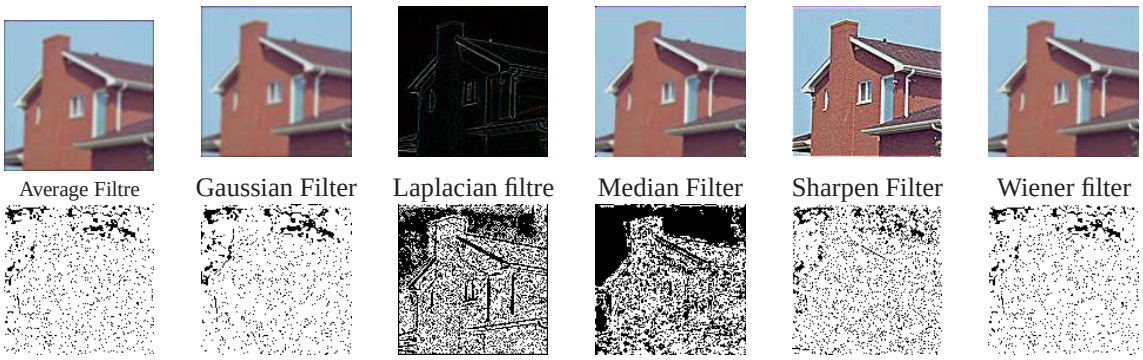


FIG. 6.11 – Performances contre divers types de filtre.

Débruitage

La figure 6.12 montre que notre méthode est capable de détecter très efficacement que l'image tatouée a subi des modifications après l'ajout de divers types de bruit.

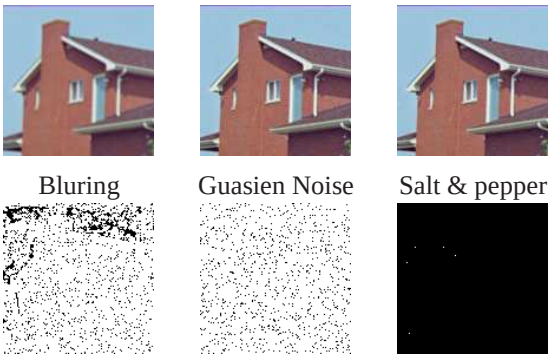


FIG. 6.12 – Performances contre divers types de bruit.

6.4.3 Discussion

Les résultats obtenus nous permettent de déduire que la méthode du tatouage fragile proposée est efficace du point de vue qualité de l'image tatouée et aussi efficacité de détection des anomalies dans l'image tatouée. Le point faible de cette méthode est que l'efficacité dépend de la clé secrète. Si l'attaquant connaît la clé, il peut modifier le message envoyé (18bits MSB + 6bits W) de telle manière qu'il sera divisible sur la clé. Afin de résoudre ce problème on propose d'utiliser une clé ayant la même taille de l'image hôte, où chaque élément $K(i,j)$ est associé à un point de l'image hôte $f(i,j)$. Cette nouvelle clé doit être cryptée par un algorithme de cryptage efficace, pour renforcer la sécurité. Par conséquence cette nouvelle proposition permet de détecter les opérations de fliping.

6.5 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle méthode de tatouage fragile d'images couleurs RGB. Cette méthode est basée sur le principe du CRC qui présente le mécanisme principal de détection d'erreurs et de la vérification d'intégrité dans les télécommunications. Cette nouvelle méthode est efficace en termes d'imperceptibilité et fragilité par rapport aux divers types d'attaques standards et conventionnelles.

Conclusion et perspectives

Au cours de ce mémoire nous avons étudié deux problématiques liées au tatouage numérique des images. Le premier problème concerne le tatouage robuste et aveugle d'images couleurs RGB. L'autre problème étudie le tatouage fragile d'images couleurs RGB. Après avoir étudié un panel assez diversifié des techniques de tatouage, nous avons élaboré nos deux approches du tatouage numérique.

Notre première contribution a porté sur le développement d'une nouvelle technique de tatouage robuste d'images couleurs RGB. Dans ce cas, le watermark est inséré dans le domaine transformé en utilisant la décomposition SVD. Cette contribution prend en compte : la détection aveugle du watermark et le bon compromis entre la qualité visuelle d'images tatouée et la robustesse contre la majorité dattaques connues.

L'analyse des résultats expérimentaux a permis de montrer que cette méthode maintien une haute qualité d'images tatouées et une robustesse contre plusieurs types d'attaques standards comme la compression JPEG, le filtrage, cropping, le bruit, etc. Ensuite, nos efforts se sont orientés vers une deuxième contribution. Celle-ci concerne le tatouage fragile utilisant le principe du code détecteur d'erreurs CRC qui est largement utilisé dans les télécommunications. A l'inverse de la première contribution, cette approche repose sur l'insertion du watermark dans le domaine spatial. Les résultats ont montré que cette méthode est efficace du point de vue qualité d'images tatouées et aussi efficacité de détection des anomalies dans l'image tatouée.

Bien que les approches proposées sont assez efficaces, elles ne sont pas suffisantes pour réaliser une protection complètement sûre. De nombreuses pistes sont possibles pour améliorer et développer des nouvelles solutions.

Pour la première méthode, nous pouvons envisager à la correction des erreurs en utilisant des codes correcteurs d'erreurs tels que les turbo-codes. Concernant la deuxième méthode, nous pouvons envisager l'augmentation de la taille du code CRC. Cela peut être effectué en découpant l'image en blocs. D'autre part, le travail est en progrès afin de proposer notre propre code de détection d'erreurs.

Nous nous sommes basés dans l'étude expérimentale sur l'utilisation des métriques basées pixels. Dans le future, nous essayerons d'utiliser des métriques psycho-visuelles telles que JNCD (voir 2.7.2.3). Nous essayerons aussi d'élaborer un mécanisme pour assurer la contrainte de sécurité.

Bibliographie

[1] J. Autrusseau, F. Guédon and Y. Bizais. Mojette Cryptomarking Scheme for Medical Images. In *SPIE Medical Imaging*, volume 5032, 2003.

[2] M. Barni and F. Bartolini. *Watermarking Systems Engineering : Enabling Digital Assets Security and Other Applications*. 2004.

[3] B. Bas, P. Roue and J. M. Chassery. Tatouage d'images couleurs additif : vers la sélection d'un espace d'insertion optimal. In *Coresa03*, volume 1, 2003.

[4] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for Data Hiding. *IBM Systems Journal*, 35(3) :313–336, 1996.

[5] A. Benoit. *Le système visuel humain au secours de la vision par ordinateur*. PhD thesis, Ecole Doctorale EEATS : Electronique, Electrotechnique, Automatique et Traitement du signal, Grenoble - France, 2007.

[6] M. Bergounioux. Quelques méthodes mathématiques pour le traitement d'image. In *Cours MASTER, chapter 1*, 2009.

[7] S. Bhattacharjee and Kutter. M. Compression Tolerant Image Authentication. In *IEEE International Conference on Image Processing (ICIP98), Chicago, USA*, 1998.

[8] J. Brassil, S. Low, N. Maxemchuk, and L. O´ Gorman. Electronic Marking and Identification Techniques to Discourage Document Copying. In *Infocom'94*, pages 1278–1287, 1994.

[9] P. Campisi, M. Carli, G. Giunta, and A. Neri. Blind Quality Assessment System for Multimedia Communications using Tracing Watermarking. *IEEE Transactions on Signal Processing*, 51(4) :966–1002, 2003.

[10] D.V. Chandra. Digital Image Watermarking using Singular Value Decomposition. In *45th IEEE Midwest Symposium on Circuit and Systems, Tulsa*, volume 3, pages 264–267, 2002.

[11] C. Chang, Y. Hu, and C. Lin. A Digital Watermarking Scheme based on Singular Value Decomposition. In *Combinatorics, Algorithms, Probabilistic and Experimental Methodologies- First International Symposium (ESCAPE 2007), Springer Verlag, Germany*, pages 82–93, 2007.

[12] L. Chen and J. Lin. Mean Quantization Based Image Watermarking. *Image Vision and Computing*, 21(8) :717–727, 2003.

[13] G. Coatrieux, B. Sankur, and H. Maître. Strict Integrity Control of Biomedical Images. In *Security and Watermarking of Multimedia Contents III*, volume 4314, 2001.

[14] L. Cordier, L. et Bergmann. *Proper Orthogonal Decomposition : An Overview.* post-processing of experimental and numerical data. Von Karman Institute for Fluid Dynamics, 2002.

[15] I. Cox and M Miller. A Review of Watermarking and the Importance of Perceptual Modeling. In *Electronic Imaging'97*, 1997.

[16] I. Cox and M. Miller. The first 50 years of electronic watermarking. *EURASIP Journal on Applied Signal Processing*, 2002(2) :126–132, 2002.

[17] I. Cox, M. Miller, and J. Bloom. *Digital Watermarking : Principles & Practices.* Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.

[18] I.J. Cox, M.L. Miller, and J.A. Bloom. Watermarking Applications and Their Properties. In *IEEE International Conference on Information Technology : Coding and Computing*, pages 6–10, 2000.

[19] T. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure Spread Spectrum Watermarking for Multimedia, 1997.

[20] F. Davoine and S. Pateux. *Tatouage de Documents Audiovisuels Numèriques.* Traité IC2 : Traitement du Signal et de l'Image, Hermès Science Publications, Lavoisier, France, 2004.

[21] R. Dumont. *Introduction á la Cryptographie et á la Sécurité : Notes Provisoires*. Université de Liège : Faculté des Sciences Appliquées, 2007.

[22] J. Eggers, R. Buml, R. Tzschoppe, and B. Girod. Scalar Costa Scheme for Information Embedding. *IEEE Transactions on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery*, 4(51) :1003–1019, 2003.

[23] G. El-Taweel, H. Onsi, M. Samy, and M. Darwish. Secure and Non-Blind Watermarking Scheme for Color Images. *ICGST International Journal on Graphics, Vision and Image Processing*, 2005.

[24] E. Elbasi and A. Eskicioglu. A Semi-Blind Watermarking Scheme for Images Using a Tree Structure. In *IEEE Symposium*, 2006.

[25] A. Eskicioglu and P. Fisher. Image Quality Measures and their Performance. *IEEE Transaction on communication*, 43(12) :2959–2965, 1995.

[26] P. Fouque. Cryptographie Appliquée. *Techniques de l'Ingénieur*, H5210 :1–19.

[27] J. Fridrich. Applications of Data Hiding In Digital Images. In *In tutorial for the ISPACS Conference, Melbourne,Austoralia*, pages 1–3, 1998.

[28] J. Fridrich. Robust Bit Extraction from Images. In *IEEE International Conference on Multimedia Computing and Systems ICMCS'99*, volume 2, pages 536–540, 1999.

[29] J. Fridrich and M. Goljan. Protection of Digital Images using Self Embedding. In *The Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology*, 1999.

[30] J. Fridrich, M. Goljan, and N. Memon. Further Attacks on Yeung-Mintzer Fragile Watermarking Scheme. In *SPIE International Conference on Security and Watermarking of Multimedia Contents II, San Jose, California*, volume 3971, 2000.

[31] M. Fridrich and R. Du. Invertible Authentication. In *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents*, volume 4314, pages 97–208, 2001.

[32] G. L. Friedman. The Trustworthy Digital Camera : Restoring Credibility to the Photographic Image. *IEEE Transactions on Consumer Electronics*, 39(4) :905–910, 1993.

[33] E. Fullea and J. Martinez. Robust Digital Image Watermarking Using DWT, DFT and Quality Based Average. In *ACM Multimedia*, pages 489–491, 2001.

[34] R. Ghazy, M. Hadhoud, N. El-Fishawy, and F. Abd El-Samie. Performance Evaluation of Block Based SVD Image Watermarking. *Progress In Electromagnetics Research B. IEEE*, 7 :147–159, 2008.

[35] http ://cct.rncan.gc.ca/glossary/.

[36] http ://lecerveau.mcgill.ca/flash/.

[37] http ://membres.lycos.fr/imgnum/outils/4.html.

[38] http ://membres.lycos.fr/imgnum/outils/4.html.

[39] http ://www.commentcamarche.net/contents/video/filtres.php3.

[40] http ://www.eclairement.com/Image-numerique-quel format.

[41] http ://www.kaddour.com/chap1/.

[42] http ://www.map.toulouse.archi.fr/works/panoformation/imagenum/imagenum.htm.

[43] Y. Hu, J. Huang, S. Kwong, and Y. Chan. Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform. In *IWDW'2003*, pages 86–100, 2003.

[44] N. Johnson, Z. duric, and S. Jajodia. *Information Hiding : Steganography and Watermarking Attacks and Countermeasures*. Kluwer Academic Publishers, Boston, 2000.

[45] H. Joumaa and F. Davoine. Tatouage substitutif d'images intégrant un masque de pondération visuelle.

[46] M. Kankanhalli and R. Ramakrishnan. Adaptive Visible Watermarking of Images. In *IEEE International Conference on Multimedia Computing and Systems*, volume 1, pages 568–573, 1999.

[47] S. Katzenbeisser and F. Petitcolas. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

[48] T. Y. Kim, T. Kim, and H. Choi. Correlation-based Asymmetric Watermark Detector. In *IEEE International Conference on Information Technology Coding and Computing ITCC'2003*, pages 564–568, 2003.

[49] E. Koch, J. Rindfrey, and Z. Zhao. Copyright Protection for Multimedia Data. In *International Conference on Digital Media and Electronic Publishing*, pages 203–213, 1995.

[50] D. Kundur and D. Hatzinakos. A robust Digital Image Watermarking Method Using Wavelet Based Fusion. In *International Conference on Image Processing (ICIP'97)*, volume 1, pages 544–547, 1997.

[51] D. Kundur and D. Hatzinakos. Digital Watermarking Using Multiresolution Wavelet Decomposition. In *IEEE International Conference on Acoustics, Speech and Signal Processing, Seattle, Washington*, volume 5, pages 2969–2972, 1998.

[52] M. Kutter, F. Jordan, and F. Bossen. Digital Watermarking of Color Images using Amplitude Modulation. *Electronic Imaging*, 7(2) :326–332, 1998.

[53] M. Kutter and F. Petitcolas. A Fair Benchmark For Image Watermarking Systems. In *Electronic Imaging'99 : Security and Watermarking of Multimedia Contents*, volume 3657, page 226239, 1999.

[54] M. Kutter, S. Voloshynocskiy, and A. Herrigel. The Watermark Copy Attack. In *In Proceedings of SPIE Security and Watermarking of Multimedia Content II*, volume 3971, 2000.

[55] G. Langelaar, J. Van der Lubbe, and R. Lagendijk. Robust Labeling Methods for Copy Protection of Images. In *SPIE Electronic Imaging'97, Storage and Retrieval for Image and Video Databases, San Jose, California*, pages 298–309, 1997.

[56] C. Li. Reversible Watermarking Scheme With Image-independent Embedding Capacity. *IEE Proceedings Vision, Image and Signal Processing*, 152(6) :779–786, 2005.

[57] N. Li and X. Zheng. Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform. In *International Symposium on Electronic Commerce and Security*, pages 942–945, 2008.

[58] C. Y. Lin and S.F. Chang. Generating Robust Digital Signature for Image / Video Authentication. In *Multimedia and Security Workshop at ACM Multimedia 98, Bristol, UK*, 1998.

[59] C. Y. Lin and S.F. Chang. Semi-fragile Watermarking for Authenticating JPEG Visual Content. In *International Conference on Security and Watermarking of Multimedia Contents II*, volume 3971, 2000.

[60] E. T. Lin and E. J. Delp. A Review of Fragile Image Watermarks. In *Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99) Multimedia Contents,Orlando*, pages 25–29, 1999.

[61] D. Lingrand. *Introduction aux traitement d'images*. Vuibert, 2008.

[62] J. Liu, X. Niu, and W. Kong. Image Watermarking based on Singular Value Decomposition. In *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '06)*, pages 457–460. IEEE, 2006.

[63] R. Liu and T. Tan. An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. In *IEEE Transactions on Multimedia*, volume 4, pages 121–128, March 2002.

[64] T. Liu, R. Venkatesan, and M. Mihak. Scale-invariant Image Watermarking via Optimization Algorithms for Quantizing Randomized Statistics. In *Proceedings of the 2004 workshop on Multimedia and security*, 2004.

[65] C. Lou, J. Liu, and T. Li. *Digital Signature-based Image Authentication.* Idea Group Publishing, 2004.

[66] Chun-Shien Lu. *Multimedia Security : Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. Idea Group Publishing, 2005.

[67] Jean Luc Le Luron. Les images numerique,généralités. 2003.

[68] K. Maeno, Q. Sun, S. Chang, and M. Suto. New Semi-fragile Image Authentication Watermarking Techniques Using Random Bias ND Non Uniform Quantization. *IEEE Transactions on Multimedia*, 8(1) :32–45, 2006.

[69] B.S. Manjunath, C. Shekhar, and R. Chellappa. A New Approach to Image Feature Detection With Applications. *Pattern Recognition*, 29(4) :627–640, 1996.

[70] V. Martin. *Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique*. PhD thesis, Ecole doctorale : Informatique et Télécommunications,Spécialité : Signal, Image, Acoustique et Optimisation, 2006.

[71] F. Melgani, R. Benzid, and F. De Natale. Near-Lossless Spread Spectrum Watermarking for Multispectral Remote Sensing Images. *Journal of Applied Remote Sensing*, 1(013501), 2007.

[72] D. Minghui, Y. Fang, and J. Zhen. Robust Image Watermarking Algorithm Against Shearing. In *International Symposium on Electronic Commerce and Security*, pages 899–903, 2008.

[73] F. Mintzer, G. Braudaway, and M. Yeung. Effective and Ineffective Digital Watermarks. In *IEEE International Conference on Image Processing (ICIP'97)*, volume 3, pages 9–12, 1997.

[74] S. Mohanty, K. Ramakrishnan, and M. Kankanhalli. A DCT Domain Visible Watermarking Technique for Images. In *IEEE International Conference on Multimedia and Expo (II)*, volume 2, pages 1029–1032, 2000.

[75] S. Mohanty, N. Ranganathan, and K. Namballa. VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design. In *17th International Conference on VLSI Design*, pages 1063–1068, 2004.

[76] A. Ninassi, O. Le Meur, P. Le Callet, D. Barba, and P. Tirel. Task Impact on the Visual Attention in Subjective Image Quality Assessment. In *EUSIPCO-06*, 2006.

[77] M . Nixon and A. Aguado. *Feature Extraction and Image Processing*. British Library Cataloguing in Publication Data, 2002.

[78] J. Ohnisshi and K. Matsui. Embedding a Seal into a Picture under Orthogonal Wavelet Transform. In *IEEE International Conferance on Multimedia Computing and systems*, pages 514–521, 1996.

[79] F. Petiscolas, R. Anderson, and M. Kuhn. Information Hiding Terminology : A Survey. *IEEE Signal Processing*, 78(7) :1062–1078, 1999.

[80] F. Petitcolas. Watermarking Schemes Evaluation. *IEEE Signal Processing*, 17(5) :5864, 2000.

[81] I. Pitas and T. Kaskalis. Applying Signatures on Digital Images. In *IEEE Nonlinear Signal Processing, Thessaloniki, Greece*, pages 460–463, 1995.

[82] M.P. Queluz. Towards Robust Content Based Techniques for Image Authentication. In *IEEE Signal Processing Society 1998 Workshop on Multimedia Signal Processing*, 1998.

[83] C. REY. *Tatouage d'image : Gain en robustesse et intégrité des images*. PhD thesis, l'Université d'Avignon et des Pays de Vaucluse, 2003.

[84] C. REY and J. DUGELAY. Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images. *Traitement du Signal*, 18(4) :283–295, 2001.

[85] C Rey and J. Dugelay. A Survey of Watermarking Algorithms for Image Authentication. *EURASIP Journal on Applied Signal Processing*, 4314(6) :613–621, 2002.

[86] R. L. Rivest, A. Shamir, and L. Adelman. On Digital Signatures and Public Key Cryptosystems. In *MIT Laboratory for Computer Science Technical Memorandum 82*, 1977.

[87] R. Safabakhsh, S. Zaboli, and A. Tabibiazar. Digital Watermarking on Still Images using Wavelet Transform. In *IEEE International Conference on Information Technology ITCC 2004*, volume 1, pages 671–675, 2004.

[88] R. Schyndel, A. Tirkel, and C. Osborne. A Digital Watermark. In *IEEE International Conference on Image*, volume 2, pages 86–90, 1994.

[89] J. Seitz. *Digital Watermarking for Digital Media*. Information Science Publishing, 2004.

[90] G. Simmons. The Prisonerś Problem and the Subliminal Channel. In *Advances in Cryptology, Proceedings of CRYPTO' 83, Plenum Press*, page 5167, 1984.

[91] K. Solachidis and I. Pitas. Circularly Symmetric Watermark Embedding in 2-D DFT Domain. pages 3469–3472, 1999.

[92] D. Stanenscu, V. Groza, M. Stratulat, D. Borca, and I. Ghergulescu. Robust Watermarking with High Bit Rate. In *Third International Conference on Internet and Web Applications and Services*, pages 257–260, 2008.

[93] X. Sun, J. Liu, J. Sun, Q. Zhang, and W. Ji. A Robust Image Watermarking Scheme Based-on the Relationship of SVD. In *Intelligent Information Hiding and Multimedia Signal Processing*, pages 731–734, 2008.

[94] M. Swanson, B. Zhu, and A. Tewfik. Transparent Robust Image Watermarking. In *IEEE International Conference on Image Processing (ICIP'96)*, volume 3, pages 211–214, 1996.

[95] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding Secret Information into a Dithered Multilevel Image. In *1990 IEEE Military Communications Conference*, pages 216–220, 1990.

[96] A. Tirkel, G. Rankin, R. Schyndel, W. Ho, N. Mee, and C. Osborne. Electronic Watermark. In *DICTA 1993*, pages 666–672, 1993.

[97] S. Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, and J. Su. Attacks on Digital Watermarks : Classification, Estimation-based Attacks and Benchmarks. *IEEE Commun Mag*, 39(9) :118–126, 2001.

[98] S . Walton. Information Authentification for a Slippery New Age. *Dr. Dobbs Journal*, 20(4) :18–26, 1995.

[99] A. Watson. DCT Quantization Matrices Visually Optimized for Individual Images. In *SPIE*, volume 1913, pages 202–216, 1993.

[100] R. Wolfgang and E. Delp. A Watermark for Digital Images. In *IEEE International Conference on Image Proceeding (ICIP96)*, volume 3, pages 219–222, 1996.

[101] R. Wolfgang, I. Podilchuk, and E. Delp. Perceptual Watermarks for Digital Images and Video. *IEEE*, 87(7) :1108–1126, 1999.

[102] P. Wong and A. Memon. Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification. *IEEE Transactions on Image Processing*, 10(10) :1593–1601, 2001.

[103] M. Wu and B. Liu. Watermarking for Image Authentication. In *IEEE International Conference on Image Processing*, volume 2, pages 437–441, 1998.

[104] Y. Xing and J. Tan. A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation. In *Second Workshop on Digital Media and its Application in Museum and Heritage*, pages 3–8, 2007.

[105] Chen. Y. A Fragile Watermark Error Detection Scheme for Wireless Video Communications. *IEEE Transactions on Multimedia*, 7(2) :201–211, 2005.

[106] H. Yang, Y. Liang, L. Liu, and H. Sun. HVS-based Imperceptibility Measure of Watermark in Watermarked Color Image. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel / Distributed Computing*, volume 3, pages 722–727, 2007.

[107] E. Yavuz and Z. Telatar. Improved SVD-DWT Based Digital Image Watermarking Against Watermark Ambiguity. In *ACM Symposium on Applied computing*, pages 1051–1055, 2007.

[108] M. Yeung and F. Mintzer. On Resolving Rightful Ownership's of Digital Images by Invisible Watermarks. 1997.

[109] M. Yeung and F. Mintzer. An Invisible Watermarking Technique for Image Verification. In *International Conference on Image Processing (ICIP'97)*, pages 680–683, 2007.

[110] G. Yu, C. Lu, H. Liao, and J. Sheu. Mean Quantization Blind Watermarking for Image Authentication. In *IEEE Intnernational Conference on Image Processing (ICIP'2000)*, volume 3, pages 706–709, 2000.

[111] J. Yu, X. Wang, J. Li, and X. Nan. An Effective Fragile Document Watermarking Technique. In *IEEE International Symposium on Electronic Commerce and Security*, pages 908–911, 2008.

[112] Z. Zhang, Q . Sun, and W.C. Wong. A Novel Lossy-to-lossless Watermarking Scheme for JPEG2000 Images. In *International Conference on Image Processing,ICIP'04*, volume 1, pages 573–576, 2004.

[113] J. Zhao, R . Hayasaka, R . Muranoi, M . Ito, and Y . Matsushita. A Video Copyright Protection System Based on Content ID. *IEICE Transaction Information System*, E83-D(12) :2131–2141, 2000.

[114] D. Zheng, Y. Liu, J. Zhoa, and A. Saddik. A survey of RST Invariant Image Watermarking Algorithms. *ACM Computing Surveys*, 39(2), 2007.

Tatouage numérique des images couleurs RGB

Résumé : Le tatouage numérique a connu, ces dernières années, un essor spectaculaire. Initialement développé pour renforcer la protection des droits d'auteur des documents multimédia (images, son, vidéo) il tend de plus en plus a être utilisé pour remplir d'autres fonctions de sécurité, notamment des fonctions d'intégrité, ou des services d'information. Bien que, le tatouage numérique est un nouvel axe de recherche, il a gagné beaucoup d'attention et a évolué très rapidement. Plusieurs méthodes efficaces de tatouage des images numériques ont en effet été développées. Néanmoins, la plus part des méthodes proposées se sont focalisées sur les images à niveaux de gris, malgré que la couleur est devenue cruciale pour les systèmes de traitement d'images et de vidéos. Pour cette raison, nous avons proposé deux nouvelles méthodes de tatouage numérique d'images couleurs RGB. Nos objectifs sont centrés sur deux grands axes de recherche dans le domaine du tatouage numérique : le premier axe concerne le tatouage robuste qui a pour but de protéger les droits d'auteurs, tandis que, le deuxième axe concerne le tatouage fragile qui a pour objectif de garantir un service d'intégrité et d'authentification. Nous nous sommes aussi intéressés au mode d'extraction aveugle, car le caractère aveugle constitue un enjeu majeur dans les applications réelles. Dans la méthode du tatouage robuste proposée, le watermark est inséré dans le domaine transformé en utilisant la décomposition en valeurs singulières (SVD). Tandis que, Le nouveau scheme du tatouage fragile, utilise le principe du contrôle de redondance cyclique (CRC) pour insérer le watermark dans le domaine spatial.

Mots clés : tatouage fragile, tatouage robuste, CRC, SVD.

RGB color image digital watermarking

Abstract : In recent years, digital watermarking has been growing in a spectacular manner. Originally, developed to improve the protection of copyrighted multimedia content (images, sound, video), it tends to be increasingly used to perform other security functions, including integrity functions, or information services. Even if digital watermarking is a new research domain, it has gained much attention and has evolved very quickly. Indeed, many effective methods have been developed for watermarking digital images. But most of the proposed methods are focused on the gray-scale images, although the color becomes critical for image processing systems and video. For this aim, we have proposed two new RGB color image watermarking methods. Our objectives are focused on two main research domains in the field of digital watermarking : the first one concerns the robust watermark, which aims to protect the rights of authors, while the second one is the fragile watermarking, which seeks to ensure service integrity and authentication. We are also interested in the blind mode of extraction, because this feature is a major issue in real applications. In the proposed robust watermarking method, the watermark is inserted the Singular Value Decomposition (SVD). While the new fragile watermarking scheme uses efficiently the principle of the Cyclic Redundancy Check (CRC) to insert the watermark in the spatial domain.

Keywords : fragil watermarking, robust watermarking, CRC, SVD.