MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM

Faculté des Sciences Exactes & de l'Informatique
Département de Mathématiques et d'Informatique
Filière Informatique

MEMOIRE DE FIN D'ETUDES
Pour l'Obtention du Diplôme de Master en Informatique
Option : Ingénierie des Systèmes d'Information

Authentification des images numériques basée sur le tatouage numérique

Présenté par :

- ***Tayeb Bey Abdenour .***
- ***Touihr Khedidja .***

Encadré par:

- ***Bentaouza Merieme Chahinez***

Année Universitaire 2013/ 2014

Titre :

« Authentification des images numériques basée sur le tatouage numérique »

Résumé: Ce projet est une **application** des **algorithmes** de **tatouage numérique** appliqués sur les **images numériques.** L'utilisation **illégale** de l'image numérique relève du **droit d'auteur** et l'**authentification** des documents est encore une question très critique. Donc, le meilleur moyen de **protection** du **droit d'auteur** est le **tatouage numérique** en se basant sur le **système d'authentification d'image numérique**. Ce travail réalisé peut effectuer un **tatouage visible** , **invisible** ou **hybride** sur l'image.

Les résultats obtenus sont satisfaisants points de vue **temps** et **taux** de tatouage mais présentant dans certains cas une **perte d'information** dans **l'image tatouée**

Mots clés : Authentification, Image numérique, Walton, image dissimiler, Tatouage invisible, Tatouage visible.

Title:

"Authentication of digital images based on watermarking"

Summary: This project is a application of **watermarking algorithm** applied to **digital images**. The illegal use of **digital image** falls within the **copyright** and **authentication** of documents is still a very critical issue. So the best way to protect **copyright watermarking** is based on the system of **digital image authentication**. This work can perform a **visible**, **invisible or hybrid of** watermarking **image.**

The results obtained are satisfactory about **time** and **rate** watermarking but it presents in some case **loosely** information in **watermarking image**.

Keywords: Authentication, Digital Imaging, Walton, picture dissimiler, invisible tattoo, visible tattoo.

Table des matières :

Table des matières :

Introduction générale :

Ces dernières décades, les documents multimédias sont devenus un élément central dans les différents domaines d'applications grâce au développement des technologies liées à l'informatique. En effet, elles sont des outils de travail essentiel en biomédical, en imagerie satellitaire et astronomique, en production cinématographique, ou encore en informatique industrielle. Ce développement phénoménal ne s'est pas fait sans entraîner des inquiétudes de manipulations illicites puisque n'importe quelle personne peut facilement copier, modifier et distribuer les images numériques sans risque de les détériorer. Ces manipulations illicites sont un problème central pour la sécurité d'un système, quel que soit : un état, une entreprise ou un particulier. D'où, l'importance de protéger ces documents multimédias contre un accès ou une distribution non autorisée. Les techniques de cryptage constituent la première solution pour empêcher l'accès non autorisé à des données numériques. Elles répondent aux besoins des utilisateurs en matière de sécurité comme la confidentialité, l'intégrité et l'identification. Néanmoins, ces techniques se sont révélées insuffisantes ou d'un emploi difficile. En effet, les outils de cryptographie protègent l'image uniquement lors d'une transmission, mais une fois l'image est déchiffrée, il n'y a plus de contrôle pour empêcher une manipulation illégale.

Dans ce contexte, le tatouage numérique (Digital Watermarking en anglais) apparaît comme étant une alternative pouvant s'avérer efficace et complémentaire pour aider à établir une sécurité supplémentaire, à assurer un accès autorisé, à faciliter l'authentification du contenu ou empêcher la reproduction illégale. L'idée est de cacher dans une image (ou dans un document multimédia numérique) une marque invisible.

Le tatouage numérique a gagné beaucoup d'attention et a évolué très rapidement. Dans la littérature, plusieurs méthodes efficaces sont développées et satisfont certaines conditions selon le problème traité. Dans ce domaine plusieurs travaux sont réalisés [1], dans notre recherche on a abordé certains travaux .on peut citer parmi eux :

Gaëtan Le Guelvouit, Stéphane Pateux, Jonathan Delhumeau ont étudié la construction des codes pour le tatouage avec prise en compte de l'information adjacente pour résoudre le problème de transmission sur un canal avec information adjacente disponible lors de l'insertion (une partie du bruit est parfaitement connue au moment de l'encodage) , les phases d'encodage et de décodage se basent sur l'algorithme de Viterbi , assurant ainsi une faible complexité [2].

NourEl-HoudaGoleaa decrit dans son mémoire nommé tatouage numérique des images couleurs RGB. L'objectif du projet est centré 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. Ils se sont 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 le tatouage [3].

Un mémoire fait par **Messaoud Mostefa, Samira Djebrani , Youssef Chahir**présente une nouvelle approche pour le tatouage des images numériques basée sur la topologie des coupes. La technique proposée permet d'incruster une ou plusieurs marques dans une ou plusieurs parties de l'image localisées par un claque topologique contenant les composants connexes d'une coupe choisie. Le schéma de tatouage utilisé est spatial, additif et à clef secrète. Les expérimentations réalisées sur une base d'images importante montrent l'efficacité et la robustesse de la technique proposée [4].

Lahmar Abbou Djamel Eddine et Mostefa Daouadji Abdel Hakim et BentaouzaChahinez.Mont préparé un mémoire de fin d'étude en Licence sur tatouage numérique d'une image par une image ou ils ont fait une implémentation des méthodes pour tatouer des images numériques par l'approche de l'addition des couleurs de pixel. Il est clair que l'authentification des fichiers numériques est plus importante afin de préserver l'originalité de ces fichiers, et leur application peut être utilisée pour réaliser cette opération, On utilisant la technique du tatouage [5].

Notre projet sera comme suis :

Dans le premier chapitre nous présentons une suite de définitions qui permettront de mieux appréhender le sujet des images numériques.

Dans le deuxième chapitre nous intéresserons à définir le tatouage numérique avec ces deux types puis on va citer les applications qui existent dans le domaine de marquage et nous présenterons une classification des algorithmes de tatouage numériques selon plusieurs critères plus quelques éléments importants dans le domaine.

Dans le chapitre 3 on va expliquer la méthode de Walton qui base sur la somme de checksum pour le tatouage invisible en plus on va citer les étapes à suivre pour implémenter le tatouage d'image par image dans le coté de tatouage visible.

En fin, dans le chapitre 4on va présenter notre application et on va discuter sur notre problématique ou on va la réalisé.

Les figures :

Les figures de chapitre I :

Les figures de chapitre II :

Les figures de chapitre III:

Les figures de chapitre IV :

Liste des tables :

Référence :

[1] : thèse de doctorat de Mohamed El hajji « La sécurité d'images par le tatouage numérique dans le domaine d'ondelettes ». La Faculté des Sciences d'Agadir. En 28/01/2012

[2] : mémoire de Gaëtan Le Guelvouit, Stéphane Pateux et Jonathan Delhumeau : « Construction de codes pour tatouage avec prise en compte de l'information adjacente », Campus de Beaulieu 35042 Rennes Cedex, France en 2008

[3]: mémoire de NourEl-HoudaGolea :« Tatouage numérique des images couleurs RGB » du diplôme magister en informatique. Université El-HadjLakhder -Batna .Faculté des sciences de l'ingénieur département d'informatique. en 2010.

[4] : mémoire de Messaoud Mostefai, Samira Djebrani, Youssef Chahir : « Tatouage topologique des images numériques », institut d'informatique, université de Bordj Bou Arréridj, BP 64, 34265, Algérie, GREYC URA CNRS 6072, université de Caen, BP 5186,14032 en 2003.

[5] : mémoire de LahmarAbbou Djamel Eddine et Mostefa daouadji Abdel Hakim et Bentaouzachahinez .M, mémoire de licence L3 université Abdelhamid Ibn Badis faculté des sciences exacte et informatique Mostaganem Algérie : « Tatouage numerique d'une image par une autre image » année 2012/2013 .

[6] : synthèses de Jean-Pierre: « du réel au virtuel », Paris : marabout en 1998.

[7] : cour de Raphaël Isdant : « Traitement numérique de l'image » Raphaël en 2009

[8] : cour de Daniel Desmoulins : « L'image numérique « CARTOGRAPHIE » » en 2004

[9] : thèse de Khaled Loukhaoukha : « Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective ».Université Laval Québec en 2010.

[10] : cour de Marc Chaumont:«le tatouage de document numérique »en 12/11/2008

[11] :mémoire de Ali JabeurBouzidi « Développement de techniques de marquage d'authentification pour la protection de données multimédias». Université du Québec en Outaouais Département d'informatique et d'ingénierie .en 28/09/2009.

[12] :mémoire de Bouab Mohammed « Tatouage d'images base sur des propriétés psychovisuelles ».Université Mentouri Constantine Faculté des sciences de l'ingénieur. En 2005.

[13] :mémoire de Vu Duc Minh : « Tatouage des images dans un domaine fréquentiel », Ha noi, 15/1/2006

[14] :mémoire de Djabri Hamza, Benhmied Youcef,Adda BenatiaTekkouk, Faculté des Sciences Exactes & de l'Informatique Département de Mathématiques et d'Informatique Filière Informatique : « Les techniques de compression d'images de télédétection », année 2012/2013.

[15] : mémoire de Antoine Simon : « Application du tatouage d'images à l'imagerie médicale » , Université d'Angers Laboratoire d'Ingénierie des Systèmes Automatisés UPRES-EA 2168 en 2007

[16] : cours 243-648 communications numériques détection et correction d'erreurs

[17] : Laboratoire Codes redondants pour la détection d'erreurs faites , Profs. Peña& Perez-Uribe&Starkier

[18] : « introduction à Borland C++ » de Bruno-Laurent Garcia et Loïc Yon en Août 2006

Webographie :

[17] : les images numériques (vectorielle ou matricielle) :

[http://www.imedias.pro/cours-en-ligne/graphisme-design/definition-resolution-taille-image/images-numeriques-et-impressions/] consulté le 2/03/2014

[18] : caractéristique d'une image numérique :
[http://www.memoireonline.com/12/09/3040/m_La-liaison-automatique-des-plusieurs-images-percues-sur-un-scanner4.html] consulter le 03/03/2014

[19] :[http://tecfa.unige.ch/tecfa/teaching/staf13/fiches mm/bitmapvectoriel.htm]consulté le 01/03/2014

[20] :image numérique :
[http://www.imagenumerique.50webs.com/img.num.html] consulté le 01/1/2014

[21] :les images vectorielle et matricielles :
[http://www.imedias.pro/cours-en-ligne/graphisme-design/definition-resolution-taille-image/les-images-vectorielles matricielles/#image_vectorielle] consulter le 05/03/2014.
[22] : [http://bnazarian.free.fr/MyUploads/IN_GBM_06_BINAIRES].consulter le 01/03/2014.
[23]:[http://www.montpellier.iufm.fr/technoprimaire/]consulter le 05/05/2014.

I-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, 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.

Le traitement numérique d'images n'est pas un nouveau phénomène. Des techniques pour la 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[3].

L'objectif de ce chapitre est d'introduire le domaine des images numériques.

II-Image numérique :

II-1-Définition d'image numérique :

Une image numérique désigne toute image (dessin, icone, photographie…) acquise, créée, traitée et stockée sous forme binaire :

- acquise par des convertisseurs analogique-numérique situés dans des dispositifs comme les scanners, les appareils photo ou les caméscopes numériques, les cartes d'acquisition vidéo (qui numérisent directement une source comme la télévision) .
- créée directement par des programmes informatiques, grâce à une souris, des tablettes graphiques ou par de la modélisation 3D (ce que l'on appelle, par abus de langage, les « images de synthèse »).
- traitée grâce à des outils graphique, de façon à la transformer, à en modifier la taille, les couleurs, d'ajouter ou d'en supprimer des éléments, d'appliquer des filtres variés, etc.
- stockée sur un support informatique (disquette, disque dur, CD-ROM…) [17].

II-2- Caractéristiques des images numériques :

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants :

II-2-1-Pixel :

Contraction de l'expression anglaise « Picture Eléments » éléments d'image, le pixel est le plus petit point de l'image, c'est une entité calculable qui peut recevoir une structure et une quantification. Si le bit est la plus petite unité d'information que peut traiter un ordinateur, le pixel est le plus petit élément que peuvent manipuler les matériels et logiciels d'affichage ou d'impression. La lettre A, par exemple, peut être affichée comme un groupe de pixels dans la figure ci-dessous:

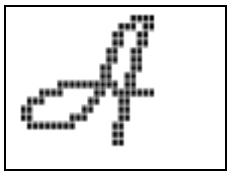


Figure 1: Groupe des pixels[18].

La quantité d'information que véhicule chaque pixel donne des nuances entre images monochromes et images couleurs. Dans le cas d'une image monochrome, chaque pixel est codé sur un octet, et la taille mémoire nécessaire pour afficher une telle image est directement liée à la taille de l'image.

Dans une image couleur (R.V.B.), un pixel peut être représenté sur trois octets : un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B) [18].

II-2-2- Dimension :

C'est la taille de l'image. Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multiplié par le nombre de colonnes nous donne le nombre total de pixels dans une image [18].

II-2-3- Résolution :

La résolution est définie par un nombre de pixels par unité de longueur de l'image à numériser en dpi (dots per inch) ou ppp (points par pouce)]. On parle de définition pour un écran et de résolution pour une image. Plus le nombre de pixels est élevé par unité de longueur de l'image à numériser, plus la quantité d'information qui décrit l'image est importante et plus la résolution est élevée (et plus le poids de l'image est élevé).La résolution d'une image correspond au niveau de détail qui va être représenté sur cette image [18].

II-2-4-Taille d'une image

Pour connaître la taille d'une image, il est nécessaire de compter le nombre de pixels que contient l'image, cela revient à calculer le nombre des cases du tableau, soit la hauteur de celui-ci que multiplie sa largeur. La taille de l'image est alors le nombre des pixels que multiplie la taille (en octet) de chacun de ces éléments [18].

Exemple : pour une image de 240 X 420 en True Color :

Nombre de pixels :

240 X 420 = 100800

Taille de chaque pixel : 24 bits / 8 = 3 octets

Le poids de l'image est ainsi égal à :

100800 X 3 = 302.400 égal 302.400/1024 = 295 Ko

II-2-5- Bruit :

Un bruit (parasite) dans une image est considéré comme un phénomène de brusque variation de l'intensité d'un pixel par rapport à ses voisins, il provient de l'éclairage des dispositifs optiques et électroniques du capteur [18].

II-2-6- Histogramme :

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image. Pour diminuer l'erreur de quantification, pour comparer deux images obtenues sous des éclairages différents, ou encore pour mesurer certaines propriétés sur une image, on modifie souvent l'histogramme correspondant, Il permet de donner un grand nombre d'information sur la distribution des niveaux de gris (couleur) et de voir entre quelles bornes est repartie la majorité des niveaux de gris (couleur) dans les cas d'une image trop claire ou d'une image trop foncée. Il peut être utilisé pour améliorer la qualité d'une image (Rehaussement d'image) en introduisant quelques modifications, pour pouvoir extraire les informations utiles de celle-ci [18].

II-2-7- Contours et textures

Les contours représentent la frontière entre les objets de l'image, ou la limite entre deux pixels dont les niveaux de gris représentent une différence significative. Les textures décrivent la structure de ceux-ci. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différentes [18].

II-3-Les types des images :

Les images produites et traitées par les ordinateurs sont de deux types: les images bitmap et les images "vectorielles". A chacun de ces types correspondent des familles distinctes de logiciels spécialisés respectivement, les paint (la progamme Paint des accessoires de Windows, Mac Paint, Painter, PSP 4, Photoshop, etc. et les *draw* (MacDraw Pro, Illustrator, FreeHand, Corel Draw, etc). Chaque type possède aussi ses avantages et ses inconvénients. On pourrait croire que ces deux modes, ce deux types d'images soient complétement distincts et étanches. Il n'en est rien : il y a des logiciels qui permettent de travailler dans les deux modes, tels Canevas (Deneba) et SuperPaint (Aldus). Enfin, les logiciels vectoriels offrent

souvent la possibilité de convertir, de "retracer", les images bitmap en images vectorielles (Corel Trace par exemple) et inversement de transformer une image vectorielle en une image bitmap [19].

II-3-1-Image vectoriel :

Contient des formes géométriques simple collés les autres, une représentation vectorielle est dessinée à nouveau à chaque visualisation, ce qui engendre la réalisation de plusieurs calculs sur la machine (pouvoir redimensionner l'image à volonté sans aucun effet).

Le principe est de décrire des formes géométriques simple (droite, cercle…)d'un point de vue mathématique auxquelles on peut appliquer différentes transformation (rotation, écrasement,..) donc au lieu de mémoriser une mosaïque de point élémentaires on stock la succession d'opération conduisant au trace ainsi, le dessin est mémorisé comme trace une droite entre les points (x1,y1) et (x2,y2) ,puis trace un cercle de couleur bleu de centre (x3,y3) et de rayon 30 etc. la représentation vectorielle introduit une notion de couche de dessin, il est possible de superposer plusieurs plans de courbes [6].

II-3-1-1-Avantages :

1. L'image numérique doit être calculée avant de pouvoir être affichée par le périphérique (opération qui porte le nom de *rastérisation*). Cette opération peut être faite pour n'importe quelle résolution du périphérique: l'image vectorielle est réellement indépendante du périphérique.
2. Toutes les modifications spatiales de l'image (réduction, agrandissement, translation, rotation,etc.) sont aisées et n'occasionnent aucune perte d'information. Il suffit en effet de modifier les coordonnées des points de contrôle qui définissent l'objet. On voit sur l'image ci-contre les points de contrôle de la courbe et, en traits pointillés, à partir de l'un de ceux-ci, l'axe selon lequel la courbe peut être modifié.

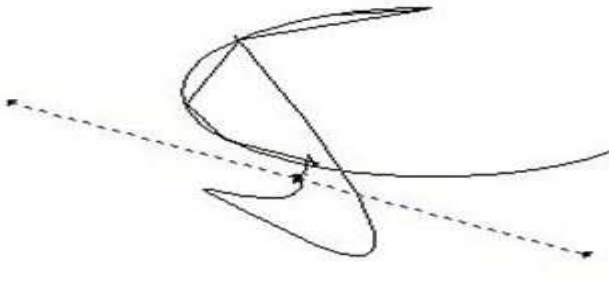


Figure 2 : image vectoriel [19]

3. L'image vectorielle est particulièrement adaptée aux représentations schématiques et stylisés constituées de formes géométriques, uniformément remplies par des à-plats de couleur ou des motifs.
4. Un fichier vectoriel est bien plus compact qu'un fichier en mode point. Sa taille varie en fonction de la complexité de l'image, mais pas en fonction de la résolution demandée. Un fichier de 2 Mo peut représenter une image déjà forte complexe [19].

II-3-1-2-Désavantages :

1. Une image vectorielle ne peut coder une image analogique telle qu'une image photographique.
2. Le travail sur des objets graphiques isolés qu'il faut ensuite associer ou grouper est peu familier au graphiste ou à l'illustrateur. Il faut donc une certaine habitude et un apprentissage de nouvelles procédures de création.
3. Certaines manipulations telles que les modifications de couleurs sont difficiles sur une zone d'un objet, sur un objet simple ou sur un groupe d'objets.
4. Un fichier vectoriel est plus fragile qu'un fichier bitmap dont l'en-tête surtout doit être intacte. La moindre dégradation de l'information est souvent irréparable.
5. Chaque format de fichier vectoriel possédant ses propres attributs, la compatibilité entre les formats est difficile [19].

II-3-2-Image bitmap :

Elle est constituée de point juxtapose, que l'œil reconstitue comme un tout .elle est formée d'un tableau a plusieurs dimensions, dont chaque dimension représente une dimension spatiale (hauteur, largeur profondeur).

Dans le cas des images a deux dimension(le plus courant), les points sont appelés pixels généralement rectangle d'un point de vue mathématique, on considère l'image comme une fonction de R x R dont R ou le couple d'entrée est considéré comme une position spatiale.

Plus la densité des points est élevée, plus il y aura de détails fins visibles, plus le nombre d'informations est grand .Ainsi, la place occupée en mémoire et la durée de traitement seront d'autant plus grandes [20].

II-3-2-1-Avantages :

1. Le mode de codage des images bitmap (24 bits, codage rgb) les rend adaptées au fonctionnement des principaux périphériques, notamment les contrôleurs d'écran "true colors" (point allumé ou non, codé sur x bits).
2. Elles conviennent fort bien aux images complexes, principalement d'origine analogique, qui ne peuvent être codées qu'en mode point.
3. Elles se laissent manipuler et traiter par des opérations techniques "naturelles" pour un graphiste qui retrouve des outils et les manipulations très proches de ceux qui caractérisent son métier et sa pratique professionnelle de type analogique.
4. Elles permettent des opérations comme l'anti-aliasing (suppression du crénelage produit à la rencontre de deux couleurs éloignées), le rehaussement des contours, les modifications locales de l'image (contraste, colorimétrie, effets, filtres, etc.).
5. Le mode de codage point par point étant relativement universel, une fois cette opération effectuée, le transcodage demande des calculs répétitifs mais relativement simples: la compatibilité est aisée entre les différents formats.
6. La structure du fichier est telle que des dégradations minimes des données -mais non pas de l'en tête- ne le rendent pas nécessairement inutilisable [19].

II-3-2-2-Désavantages :

1. Les images bitmap ont une résolution fixe: aussi la qualité maximale sur un périphérique d'affichage ou d'impression donné rend-elle nécessaire de travailler, dans la majorité des cas, dans la résolution native de ce périphérique. Concrètement cela veut dire qu'une résolution de type écran donnera d'assez mauvais résultats sur un imageur photographique. Les images bitmap sont donc dépendantes du périphérique.

2. Elles supportent mal les opérations de redimensionnement, réduction ou agrandissement. Les deux opérations se traduisent par une perte d'information. Après une réduction de taille, l'image réduite présentera souvent des effets d'escaliers plus marqués que ceux de l'image source. Un agrandissement se traduira par la multiplication à la taille voulue de chacun des pixels pris séparément: chaque point se voit grossi, mais la résolution demeurant identique, la définition de l'image sera de qualité inférieure.
3. Les images bitmap sont "lourdes": les fichiers, lorsque l'on traite des images en haute définition, ont des tailles qui varient entre 10 et 30 Mo par image.... Elles sont donc encombrantes, difficiles à faire passer sur le réseau, etc [19].

Figure3 : image bitmap & vectoriel [21]

II-4- Images matricielles les plus connues :

II-4-1. Image binaire :

C'est une image pour laquelle chaque pixel ne peut avoir pour valeur que 0ou 1 .

Figure4 : Image binaire [22].

II-4-2. Image en niveau de gris

Dans le cas de l'image est demi-teinte (en niveau de gris), chaque pixel de l'image peut prendre 256 nuances grisées différentes.

L'image en niveau de gris correspond à une image en noir et blanc avec des nuances de gris. Le pixel est dans ce format code sur 8 bit (un octet) [22].

Figure 5 : Image en niveaux de gris [22].

II-4-3.Image couleur

Une image couleur est une image MxN où chaque point est représenté par un vecteur de trois valeurs, chaque valeur de ce vecteur prendre une valeur comprise entre 0 et 255 et représentent respectivement les valeurs des couleurs rouge, vert et bleu. La couleur finale est obtenue par synthèse additive ou soustractive c'est-à-dire l'opération consistant à combiner l'effet d'absorption de plusieurs couleur afin d'en obtenir une nouvelle.

Figure6 : image couleur 1 [22].

Ces images sont utilisées pour la plupart des illustrations graphiques ayant un nombre de couleur important, comme celles présentées sur les pages web, les photographies et les vidéos numérisées, etc [22].

II-5-Format d'image :

Un format d'image est une représentation informatique de l'image, associée à des informations sur la façon dont l'image est codée et fournissant éventuellement des indications sur la manière de la décoder et de la manipuler.

La plupart des formats sont composés d'un en-tête contenant des attributs (dimensions de l'image, type de codage, etc.), suivi des données (l'image proprement dite). La structuration des attributs et des données diffère pour chaque format d'image.

De plus, les formats actuels intègrent souvent une zone de métadonnées (Meta data en anglais) servant à préciser les informations concernant l'image comme :

- la date, l'heure et le lieu de la prise de vue,
- les caractéristiques physiques de la photographie (sensibilité ISO, vitesse d'obturation, usage du flash…) [8].

II-5-1-Format d'image Bitmap [23] :

Nom du format	Points forts	Points faibles	Note
JPEG **JPEG 2000** Joint Photographic Experts Group	Excellente compression	Compression destructrice	Spécialement conçu pour les photographies, il est cependant à utiliser avec délicatesse tant sa compression peut brouiller l'image. Le format JPEG2000, évolution du format original, peut être réglé pour compresser sans pertes.
GIF (Graphical Interchange Format)	Possibilité d'animation et de transparence, compression efficace	Limité à 256 couleurs	Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos.
PNG (Portable Network Graphics)	Excellente compression sans perte. Possibilité de transparence. Standard donc pérenne.	Pas très efficace pour les larges photographies	Format destiné à remplacer le format GIF et ses limitations, mais ayant encore du mail à s'implanter dans les habitudes des développeurs. Peut remplacer les JPEG comme les GIF (sauf en ce qui concerne l'animation).
TIFF (Tagged Image File Format)	Compression sans perte efficace. Couche de transparence.	Lourdeur des fichiers non compressés. Format propriétaire.	Format de stockage très utilisé, à éviter pour le Web
BMP (Bitmap)	Format par défaut de Windows	Disponible uniquement sur la plateforme de Microsoft	Généralement non compressé et de ce fait des fichiers très « lourds »

II-5-2-Format d'image vectorielle [23] :

Nom du format	Points forts	Points faibles	Note
AI (Adobe Illustrator)	Reconnu par tous les logiciels graphiques.	Format propriétaire.	Format standard de Adobe Illustrator, l'un des plus utilisés du fait de la popularité du logiciel.
PS/EPS (Postscript / Encapsulated Postscript)	Très bien reconnu sur tous les systèmes.	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	Format hybride bitmap/vectoriel, réservé à l'impression. EPS est un fichier PS qui comporte quelques restrictions supplémentaires.
SVG (Scalable Vector Graphics)	Format XML donc extensible. Très compressible car format texte. Standard donc pérenne. Permet les animations et la transparence. Peut afficher des images bitmap.	Encore très peu reconnu, car peu d'outils disponibles et manque d'implémentation au sein de navigateurs (besoin d'un plugin).	Promis à un grand avenir malgré un démarrage lent, ce format est souvent cité comme capable de rivaliser avec les premières versions de Flash.
FLA/SWF (Flash)	Très polyvalent, peut utiliser des mp3, des JPEG, des vidéos... Très répandu sur le Web.	Format propriétaire et fermé.	C'est le standard de fait des animations vectorielles sur le Web.
PDF (Portable Document Format)	Affiche les documents	Taille prohibitive. Ne peut se lire qu'avec le logiciel Acrobat ou logiciel équivalent.	Version simplifiée de PostScript, il a été conçu pour afficher les documents de la même manière quel que soit le système.
PICT (Picture)	Format par défaut de Mac OS, donc encore utilisé.	Disponible uniquement sur la plateforme d'Apple	N'a plus grand intérêt face aux autres formats existants.

II-6-Codage des couleurs (ou profondeur des couleurs) :

Une image numérique utilise plus ou moins de mémoire selon le codage des informations de couleur qu'elle possède. C'est ce que l'on nomme le codage de couleurs ou profondeur des couleurs, exprimé en bit par pixel (bpp): 1, 4, 8, 16 bits...

En connaissant le nombre de pixels d'une image et la mémoire nécessaire à l'affichage d'un pixel, il est possible de définir exactement le poids que va utiliser le fichier image sur le disque dur (ou l'espace mémoire requis en RAM pour réaliser un calcul sur cette image) [7].

1-codage des images noir et blanc :

Codage en 1 bit par pixel (bpp) : => 21 = 2 possibilités : [0,1]

- ✓ Chaque pixel peut donc avoir 2 couleurs possibles : soit noir ou soit blanc[7].

1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	1	1	1
1	1	0	1	1	1	1	0	1	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Figure 7 : Codage des images noir et blanc [7].

2-codage des images en niveau de gris :

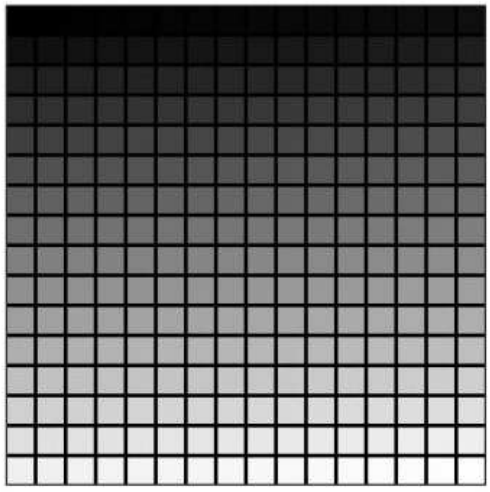
- ✓ Codage en 8 bits par pixel (bpp) => 2^8= 256 possibilités

Chaque pixel peut avoir 256 nuances de gris possibles

- ✓ Codage en 16 bits par pixel (bpp) => 2^16= 65536 possibilités

Chaque pixel peut avoir 65536 nuances de gris possibles[7].

Nuances de 256 gris



Exemple de photo possible en 8 bpp

Figure 8 : les images en niveau de gris [7].

3-codage des images couleur :

Codage en 8 bits par pixel (bpp) => 28= 256 possibilités

- ✓ Chaque pixel peut avoir jusque 256 couleurs fixes possibles [7].

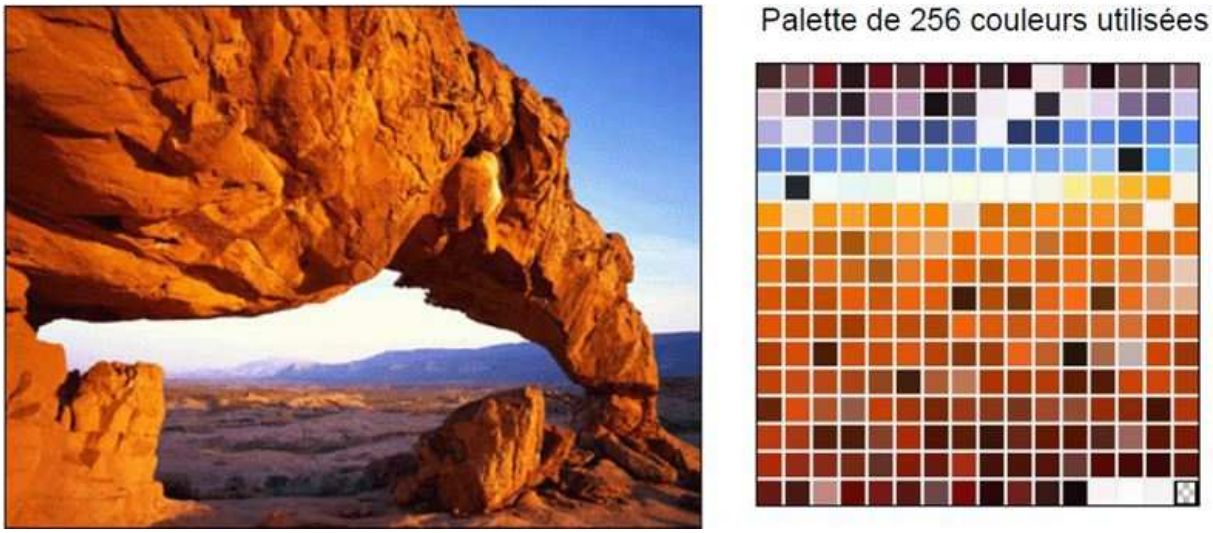


Figure9 : image couleur 2 [7].

III-Conclusion :

Au terme de ce chapitre, nous avons vu un aperçu général sur les images numériques.

D'abord, nous avons présenté les caractéristiques de l'image numérique pixel, dimension, résolution, taille et bruit).

Ensuite, les différentes modes d'images existantes (matricielle et vectorielle).

Enfin, les différente variétés de formats des fichiers d'image numérique et le codage de l'image.

Table des matières

I-Introduction :

Le besoin d'un échange d'information sécuritaire entre les personnes a fait naître la cryptologie, qui désigne les techniques de chiffrement pour rendre un message incompréhensible lors de sa transmission. A l'arrivée de l'ère numérique, cette technique est utilisée afin de protéger les documents numériques échangés à travers les réseaux informatiques. Néanmoins, une fois décryptés, ces documents ne possèdent aucune protection. A cet effet, le tatouage numérique a été introduit comme une technique permettant d'authentifier et de garantir l'intégrité des documents numériques. Elle consiste à inscrire une marque invisible, ou parfois visible, dans ces documents numériques [9].Dans ce chapitre on va voir la technique de tatouage plusdétaillée.

II-Historique du tatouage numérique :

L'information est un élément essentiel et déterminant dans tous les domaines. Tout au long de l'histoire, l'humanité a essayé d'échanger les informations d'une façon sécurisée. Pour cette raison, la dissimulation d'information a été utilisée pour les stratégies militaires et l'échange de données secrètes. On distingue, principalement deux grandes catégories : la stéganographie et le tatouage.

La stéganographie est l'art de dissimuler au sein d'un support anodin une information qui bien souvent est sans rapport avec le support. Cette dissimulation se fait de sorte qu'il soit difficile pour un observateur extérieur de se rendre compte qu'il y a eu dissimulation [10].

L'utilisation classique de la stéganographie prend place il y a plus de deux mille ans. Hérodote, l'historien grec raconte que Xerxès roi des Perses décida d'envahir la Grèce. Lorsque l'offensive fut lancée, les Grecs étaient depuis longtemps au courant de ses intentions. Démarrâtes, ancien roi de Sparte réfugié auprès de Xerxès apprit ses intentions et décida de transmettre l'information à Sparte. Il prit une tablette double en gratta la cire puis écrivit sur le bois même les projets de Xerxès, il recouvra ensuite de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis.

Dans les années 80, Margaret Thatcher, premier ministre britannique soupçonna certains de ses ministres de transmettre des informations à la presse. Pour identifier le coupable, elleexigea que tous les documents de son cabinet aient un espacement entre les mots spécifiques pour chaque ministère afin d'identifier la source de la fuite des informations.

Cependant, l'art du tatouage a été inventé en Chine depuis plus de mille ans pour tatouer le papier ipaperrnarking), mais le plus ancien papier marqué archivé date de 1292 et son origine est la ville Fabriano en Italie. Le but principal des premiers tatouages estincertain, mais ils ont

été utilisés pour des fonctionnalités pratiques telles que l'identification de l'origine de fabrication du papier ou pour l'identification du fabricant. Au 18éme siècle, le tatouage fut utilisé en Europe et en Amérique, initialement pour identifier un fabricant ou une usine de papeterie. Il a servi par la suite à indiquer le format et la qualité du papier, et aussi comme base d'authentification du papier et une mesure anti-contrefaçon pour la monnaie et autres documents. Le terme watermark semble avoir été inventé vers la fin du 18ème siècle et peut avoir été dérivé du mot Allemand wassermarke. Il est difficile de déterminer quand le tatouage numérique a été introduit pour la première fois, mais le premier article utilisant le terme Digital Watermark semble être celui de Komatsu et Tominaga en 1988.

En outre, à cette époque plusieurs organisations ont commencé à considérer le tatouage numérique pour l'inclure dans leurs normes. Vers la fin des années 90, plusieurs compagnies ont été établies pour lancer des produits de tatouage numérique sur le marché. Dans le domaine de l'imagerie [9].

III-Tatouage numérique :

III-1-Définition du tatouage :

Un tatouage numérique est une signature ajoutée à un document numérique, de type audio ou visuel en général (mais il peut également être placé sur un fichier texte, une vidéo, voire un modèle 3D) Dans le cas que nous étudions, celui de l'image, le tatouage numérique est un ensemble de bits, appelé marque ou message, ayant pour but d'identifier le propriétaire du document, de manière visible comme on peut le voir, ou de manière invisible à l'œil nu, ne pouvant être détectée qu'au scanner [5].

III-2-Autre Définitions du tatouage numérique :

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 [3].

III-2-1-Définition Miller et Cox 1997

Le tatouage numérique signifie l'incorporation d'une information numérique dans un contenu multimédia, de telle manière que l'information insérée doit être imperceptible pour un

observateur humain, puis à tenter de la récupérer après que le document tatoué ait éventuellement subi des manipulations de nature variée [3].

III-2-2-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 les 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 [3].

III-2-3-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 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 [3].

III-3-Les types de tatouage:

Selon la perception de la marque on distingue deux types d'algorithmes : visible et invisible. Tous les schémas de tatouage numérique des images cités dans les sections précédentes sont du type invisible. Le tatouage visible est le plus récent mais moins étudié à cause de sa problématique qui réside dans sa nature visible. Contrairement au tatouage invisible, un attaquant peut facilement distinguer si une image est tatouée ou non, ce qui lui facilite la tâche pour supprimer la marque.

Les tatouages visibles ont pour principe l'apposition d'une marque (aussi appelé tampon, en l'occurrence une image, logo ou autre sur une autre image afin de marquer l'appartenance. Ils sont très utilisés dans le domaine des agences photos sous forme de copyright [5].

Figure 1: Exemple de tatouage visible [5].

Les tatouages invisibles consistent également en l'apposition d'une marque mais qui a pour but d'être imperceptible à l'œil nu par l'utilisateur final. Les informations contenues dans ce tampon peuvent être de natures différentes comme une permission d'utilisation du document ou de copie de ce dernier, le propriétaire du document ou le (s) titulaire (s) de la copie [5].

Figure 2: Exemple de tatouage invisible [5].

Ce type de tatouage nécessite quelques critères afin d'être efficace :

- **Invisibilité** :

Invisibilité de la marque représente un critère important. Il s'agit de faire en sorte que l'impact visuel du marquage soit le plus faible possible afin que l'image marquée soit perçue comme fidèle à l'image originale. En plus de l'appréciation visuelle de l'image marquée ou de sa différence avec l'original, plusieurs auteurs proposent de mesurer le degré d'invisibilité en calculant le *PSNR* (Peak Signal to NoiseRatio) de l'image marquée. Il s'agit de comparer l'image originale et l'image marquée pixel à pixel et de mesurer la distorsion entre les deux par la formule suivante :

$$\mathrm{PSNR}_{\mathrm{dB}} = 10\log_{10}\frac{MN\max I(m,n)^2}{\sum_{m,n}(I(m,n)-I^*(m,n))^2} \qquad (1)$$

Les images sont de taille S=MxN et I (m, n) est la valeur du pixel (m, n). I et I* indiquent l'image originale et l'image marquée respectivement. L'équation 1 est celle utilisée dans leurs expérimentations. Généralement une valeur de PSNR supérieure à 34 dB représente une image marquée de bonne qualité. La Figure ci-dessous représente l'image de Lena avant et après l'insertion d'une marque. On remarque qu'il n'y a pas de dégradation visuelle au niveau

de l'image (b). Le PSNR de l'image (b) est de 35.5 dB, ce qui démontre que l'image marquéereste visuellement identique à l'image originale [11].

(a) Image Lena originale **(b)** Image Lena marquée

Figure 3 **:** L'image de Lena en 256 niveaux de gris. Le *PSNR* de (b) est de 35.5 dB [11].

- **sécurité :**

Comme dans toutes les disciplines proches de la cryptographie, la sûreté du système est assurée uniquement par la confidentialité de la clef *K*. Si *K* est inconnue, aucun utilisateur ne doit pouvoir retrouver l'image originale. Cette contrainte est souvent remplacée par la suivante, plus réaliste : Ne connaissant pas la clef secrète, un pirate ne doit pas pouvoir retrouver l'image originale sans pour cela mettre en œuvre des moyens plus coûteux que ceux correspondant à l'achat des droits de copyright [12].

- **robustesse :**

C'est l'un des critères les plus difficiles à vérifier. En effet beaucoup d'attaques permettent aujourd'hui de modifier l'image de telle sorte qu'on ne puisse plus y déceler la signature du propriétaire. Ces techniques utilisées pour le piratage combinent notamment les transformations géométriques, la compression, les filtrages divers et attaques de type cryptographique [12].

III-4-Applications du tatouage numérique :

Plusieurs applications industrielles de tatouage numérique sont proposées dans la littérature. Cox et al présentent dans leur livre une description détaillée des différentes applications du tatouage numérique. Ainsi, ils proposent dans leurs papiers blancs une liste des applications [1]. Parmi celle-ci, on cite :

III-4-1-La protection du copyright :

La protection du copyright constitue la première application pour laquelle le tatouage numérique a été utilisé. La technique traditionnelle consiste à mettre sur le document une information textuelle généralement sous forme " © *Auteur Date*".

L'objectif de tatouage numérique dans ce type d'application est d'insérer une information d'identification du propriétaire d'une manière imperceptible et inséparable aux documents multimédias [1].

III-4-2-Authentification :

Le tatouage permet de vérifier qu'une image n'a pas été modifiée. Ce type de tatouage permet d'assurer l'intégrité du document. Il est utilisé aussi bien dans l'authentification des images médicales, la télé-surveillance ainsi que la sécurité des papiers d'identité. Le processus de tatouage numérique consiste à cacher des informations servant à détecter une éventuelle modification ou un découpe de l'image par une personne non autorisée et à localiser précisément les régions manipulées, voir éventuellement à les restaurer [1].

III-4-3-Indexation :

Le tatouage peut avoir une application dans le domaine de l'indexation de documents.

Le tatouage numérique repose sur l'insertion une description caractéristique de l'image afin de faciliter sa recherche de manière plus simple dans une base de données. En effet, on peut envisager de compléter la signature du créateur par une description sommaire de l'image pour permettre son indexation de manière plus simple.

On peut aussi envisager d'insérer un tatouage représentant un lien vers une autre source d'information (un lien vers un site Internet) afin d'obtenir des renseignements complémentaires sur l'image [1].

III-4-4-Le contrôle de diffusion (Monitor Broadcasts) :

Cette application permet aux propriétaires ou aux distributeurs de contenu de suivre la diffusion des émissions sur la télévision ou sur Internet de leur contenu. Le tatouage numérique est utilisé pour prouver que le contenu a été joué dans son intégralité en générant des rapports sur l'état de diffusion dans un marché donné à un moment précis. Des informations complémentaires peuvent être fournies, y compris la conformité d'utilisation, de la licence et la détection d'une utilisation illégale [1].

III-4-5-Contrôle de copie :

L'objectif est de détecter la présence d'un copyright (une marque) pour contrôler ou rendre la copie de l'œuvre extrêmement difficile. Protégeant ainsi les droits et les bénéfices des détenteurs des droits d'auteur. Ce principe a été utilisé dans les vidéos où la marque indique si la vidéo peut être recopiée ou non. En effet, le détenteur d'un DVD a le droit de réaliser descopies de sauvegarde, mais non de diffuser des copies à d'autres personnes. Les systèmes de reproduction conformes doivent donc tolérer les copies de première génération (réalisées à partir d'un original) mais interdire les copies de copies. Cette application a besoin de la création d'une architecture matérielle adaptée au schéma de tatouage [1].

III-4-6-Contrôle d'Accès Sécurisé et Communiquant (CASC) :

Les documents d'identité, tels que les cartes d'identité, les passeports, les permis de conduire et le badge magnétique, contiennent des informations textuelles, une image d'identité, et éventuellement quelques autres caractéristiques biométriques comme les empreintes digitales ou une signature manuscrite. Aujourd'hui, avec le développement des nouvelles technologies, un contrefacteur peut aisément remplacer une photo ou modifier les informations sur ces documents dans la mesure où il est très difficile à le différencier de l'original. Dans le but de renforcer la sécurité, le tatouage numérique nous permet de marquer la photo d'identité par des informations liées au document (les empreintes digitales, la signature manuscrite, …) de manière à lier l'image aux autres composantes du document et ainsi d'élever significativement les performances du système d'accès [1].

III-5-Classification des algorithmes de tatouage numérique :

Au cours des deux dernières décennies, plusieurs schémas du tatouage numérique des images ont été développés pour diverses applications. À première vue ces schémas semblent très différents les uns des autres. Dans cette section, nous présentons une classification des algorithmes de tatouage numérique des images. Cette classification peut se faire selon différents critères tel que : le domaine d'insertion, la robustesse, la technique d'insertion utilisée, le mode d'extraction, la perception de la marque et la préservation de l'image originale [9].

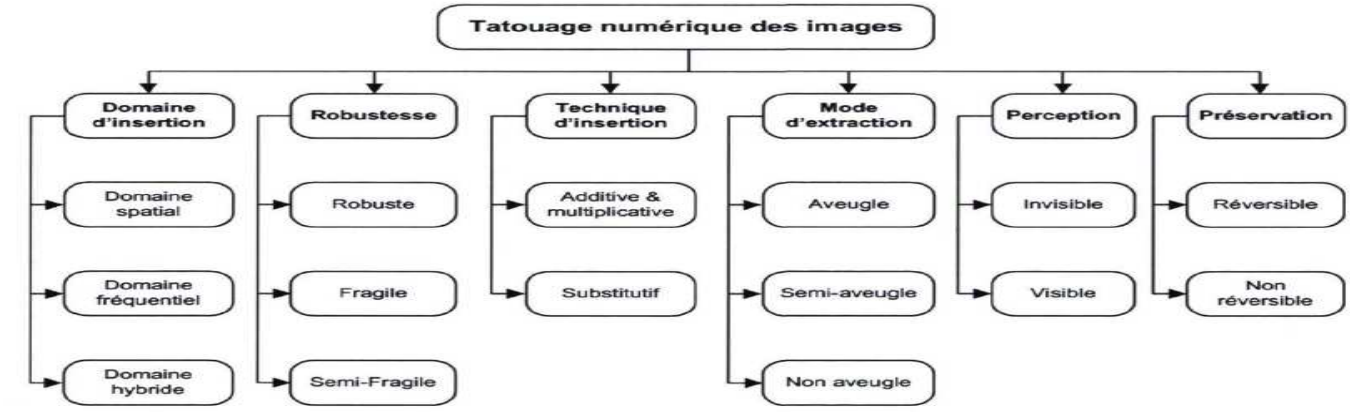


Figure 4:Organigramme de la classification des algorithmes de tatouage numérique [9].

III-5-1-Classification des algorithmes selon le domaine d'insertion:

Selon le domaine d'insertion, les algorithmes de tatouage numérique des images peuvent être groupés en deux catégories : ceux qui opèrent dans le domaine spatial et ceux qui opèrent dans le domaine fréquentiel. Néanmoins, il existe certains algorithmes qui utilisent les deux domaines, les algorithmes hybrides, mais ces algorithmes sont peu rencontrés dans la littérature [9].

III-5-1-1-Insertion dans le domaine spatial :

Les premiers algorithmes de tatouage numérique des images ont été conçus pour opérer dans le domaine spatial. Un algorithme développé dans ce domaine consiste à insérer la marque en modifiant l'intensité lumineuse d'un nombre donné de pixels pour le cas des images à niveaux de gris. Cependant, dans le cas des images couleurs, une ou plusieurs composantes d'un espace colorimétriquequelconque vont être modifiées. Les méthodes les plus couramment utilisées dans ce domaine sont : les bits les moins significatifs (LSB), la technique du Patchwork, le codage par blocs de texture et l'étalement du spectre [9].

III-5-1-2- Insertion dans le domaine fréquentiel :

D'un autre côté, les techniques de tatouage numérique conçues pour travailler dans le domaine fréquentiel sont plus robustes et plus complexes mais largement utilisées. La marque est insérée en modulant les coefficients de la transformée fréquentielle. Parmi les transformées utilisées dans les algorithmes du tatouage numérique des images on peut citer : la transformée en cosinus discrète (DCT), la transformée en ondelettes discrète (DWT), la transformée de Fourier discrète (DFT), la transformée de Hadamard discrète (DHT), la transformée ridgelet (RIT), la transformée de Radon (RAT), la transformée en curvelets (CUT), la transformée en contourlets (COT) et la transformée slant (SLT) [9].

III-5-2-Classification des algorithmes de tatouage numérique selon la robustesse :

Les algorithmes de tatouage numérique des images peuvent être classifiés selon leur robustesse. On peut distinguer dans cette classification trois catégories de tatouage numérique:robuste, fragile et semi-fragile.

- ✓ Un tatouage robuste recherche à préserver la marque insérée face aux attaques bienveillantes ou malveillantes afin qu'elle soit, toujours identifiable. La marque ne doit pas pouvoir être éliminée sans endommager l'image tatouée. Ce type de tatouage est utilisé pour la vérification du droit d'auteur.
- ✓ Tatouage fragile : la marque doit être fortement sensible à toutes modifications ou manipulations quelque soit leur nature. Cette classe de tatouage sert en général à la vérification de l'authenticité et de l'intégrité des images.
- ✓ Le tatouage semi-fragile combine les caractéristiques du tatouage robuste et fragile pour détecter les manipulations malveillantes tout en demeurant robuste face aux attaques bienveillantes. Ce type de tatouage est aussi utilisé dans l'authentification des documents [9].

III-5-3-Classification des algorithmes de tatouage numérique selon le mode d'extraction :

Selon le mode d'extraction de la marque, on peut distinguer trois catégories : celles qui ont besoin de l'image originale lors de l'extraction et qui sont appelés algorithmes informés ou non aveugles. Les algorithmes qui n'utilisent pas l'image originale sont appelés algorithmes non informés ou aveugles.

La troisième catégorie est le tatouage semi-aveugle. Dans ce type on n'utilise pas l'image originale, mais on se sert uniquement de la marque et dans le cas échéant d'une clé qui a été utilisée lors de la phase d'insertion [9].

III-6-Algorithmes de tatouage :

-Les algorithmes introduis dans cette partie se divisent en deux classes : ce qui utilise la transformation de cosinus discret(DCT) et les autres, la transformation par ondelettes discret (DWT) [13].

III-6-1- Algorithmes DCT :

- **Algorithme de Cox :**

C'est un algorithme de type additif. C'est-à-dire la marque est "additionnée" à l'image. Il prend les idées d'étalement de spectrale est une technique utilisée dans les

télécommunications radio, pour disperser un signal sur une large bande de fréquence, de façon à le rendre discret et résistant aux Interférences [13].

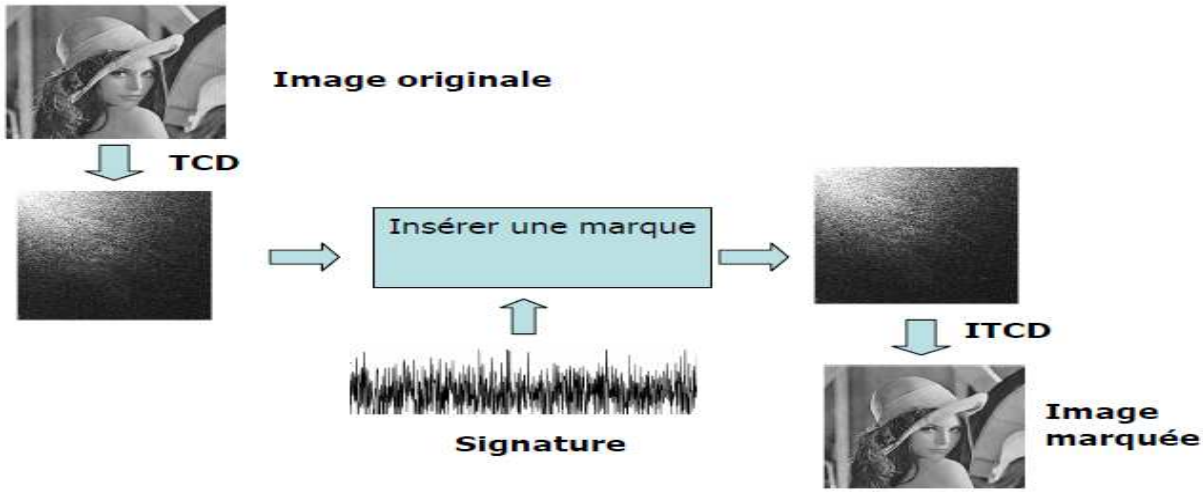


Figure 5 :Insertion de signature par DCT[13].

III-6-2- Algorithmes de DWT :

Ce sont les algorithmes utilisant la transformation DWT pour créer un domaine transformé, en suite, on exploite des caractéristiques du domaine et appliquer des techniques différentes pour implémenter la marque [13].

- **Algorithme de Chae :**

Cet algorithme de type fusion d'image est développé par J. J. Chae et B. S. Manjunath. Il permet une grande capacité de données et même la robustesse de la marque. C'est un algorithme de type fusion d'image [13].

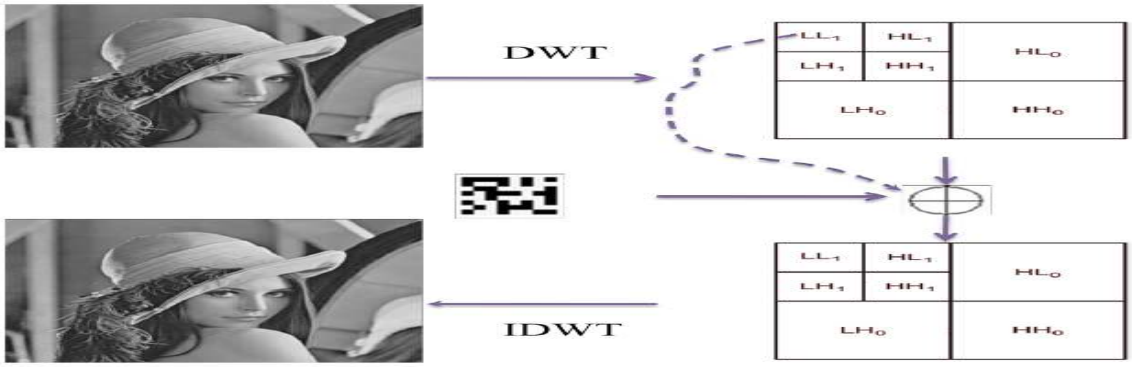


Figure 6:exemple d'insertion dans le domaine d'ondelettes DWT[13].

III-6-3-Algorithme de Walton:

L'algorithme proposé par Walton 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 des pixels sélectionnés, et sont ensuite insérées sous forme binaire au niveau des bits LSB [3].

III-7-Ondelette :

III-7-1- Définition d'ondelette :

Une ondelette est une forme d'onde de la durée limitée qui a une valeur moyenne zéro, ou les ondelettes sont des ondes localisées par temps court. Les ondelettes sont des fonctions générées partir d'une fonction mère Ψ par translations et dilatations. Grossmann et Morlet ont introduit cette fonction qui, dilatée d'un facteur d'échelle **a** et translatée d'un temps **b** permet d'analyser un signal, de le manipuler puis de le resynthétiser [14].

$$g(a,b) = \frac{1}{\sqrt{a}} \int_{t=-\infty}^{t=\infty} x(t)\ \psi_{a,b}(t)\ dt \quad (1)$$

La fonction Ψa , b (t) est obtenue par translation et dilatation d'une fonction particulière appelée ondelette mère

$$\Psi_{a,b}(t) = a^{-1/2}\,\Psi\left(\frac{t-b}{a}\right) \qquad a > 0 \quad (2)$$

IV-Conclusion :

Dans ce chapitre, nous avons défini ce que c'est un tatouage d'images ainsi qui différents types de tatouage utilisée.

Nous nous sommes intéressés aux terminologies et notions liées aux techniques du tatouage des images numérique

I-Introduction:

Le marquage fragile des images est utilisé pour l'authentification stricte des données de ces images. En d'autres mots, ce type de marquage vise à prouver l'intégrité des données de l'image. Une image et dite authentique si et seulement si tous ses pixels sont restés intacts.

Les techniques de marquage fragile utilisent la cryptographie qui se résume dans les fonctions de hachage, la signature numérique, et les systèmes à clés privées/publiques. Ces techniques agissent soit sur l'image entière, ou bien sur des blocs, des lignes ou des colonnes [11].

Les algorithmes de tatouage invisible sont nombreux comme le DCT,DWT,SLT, patchwork. Dans ce chapitre on va détailler l'algorithme de Walton qui va être la méthode àimplémenter.

Le tatouage d'image par image sa sera notre méthode à implémenter pour le tatouage visible, en effet qu'il y a d'autre méthode à citer comme le tatouage d'image par texte.

II-Tatouage invisible :

II-1-Walton :

Algorithme proposé par Walton en 1995 .Walton calcule un checksum de tous les pixels de l'image en se limitant, pour chaque pixel, à ses 7 premiers bits. Ce checksum est simplement calculé en additionnant les valeurs des pixels sans tenir compte des bits de débordement.
La longueur du checksum n'est pas fixée. Plus celle-ci sera importante, plus le risque d'avoir fortuitement deux checksums identiques pour deux images différentes sera faible. Ensuite, le résultat du checksum est inséré dans les bits de poids faible de certains pixels de l'image (suivant une clé)[15].

II-2- Algorithme de Walton :

Figure 1 : Image original

1) Choix d'un nombre entier suffisamment grand N.

2) Diviser l'image en blocs de 8x8 pixels.

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

(C)

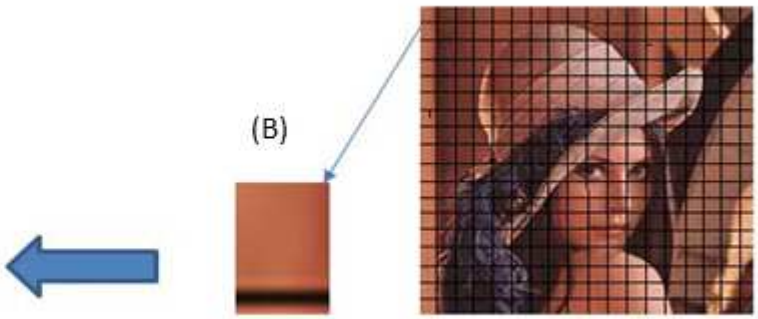


Figure 2 : présentation des bloc

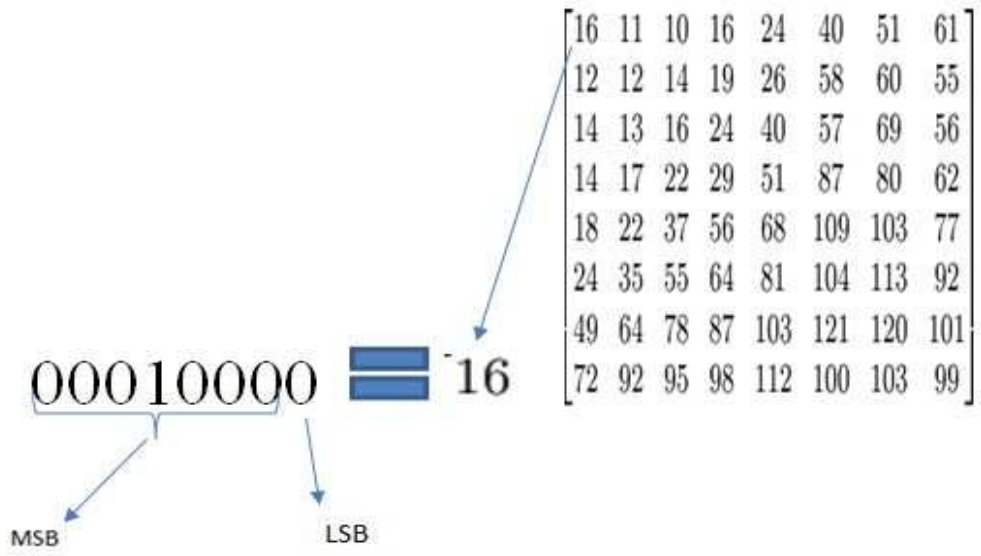
3) Pour chaque bloc B :

a. Mettre à zéro le bit de poids faible de chaque pixel du bloc. Noter les 64 pixels résultants du bloc comme suit (p1, p2, …, p64).

b. Générer une séquence pseudo-aléatoire de 64 nombres entiers (a1, a2, ...) comparables dans la taille à N. Utiliser une clé secrète K.

c. Calculer la somme (check-sum) à l'aide de :

$$S = \sum_{j=1}^{64} a_j g(p_j) \bmod N \quad \text{où g } (p_j) \text{ est le niveau de gris du pixel } p_j \text{ (déterminé par les 7 bits les plus significatifs)} \qquad (1)$$



$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Figure 3 : présentation du LSB et MSB .

4) Encrypter la forme binaire de S. Une autre clé est requise.

5) Insérer la séquence encryptée au niveau des 64 bits de poids faible (LSB) de chaque pixel du bloc considéré[11].

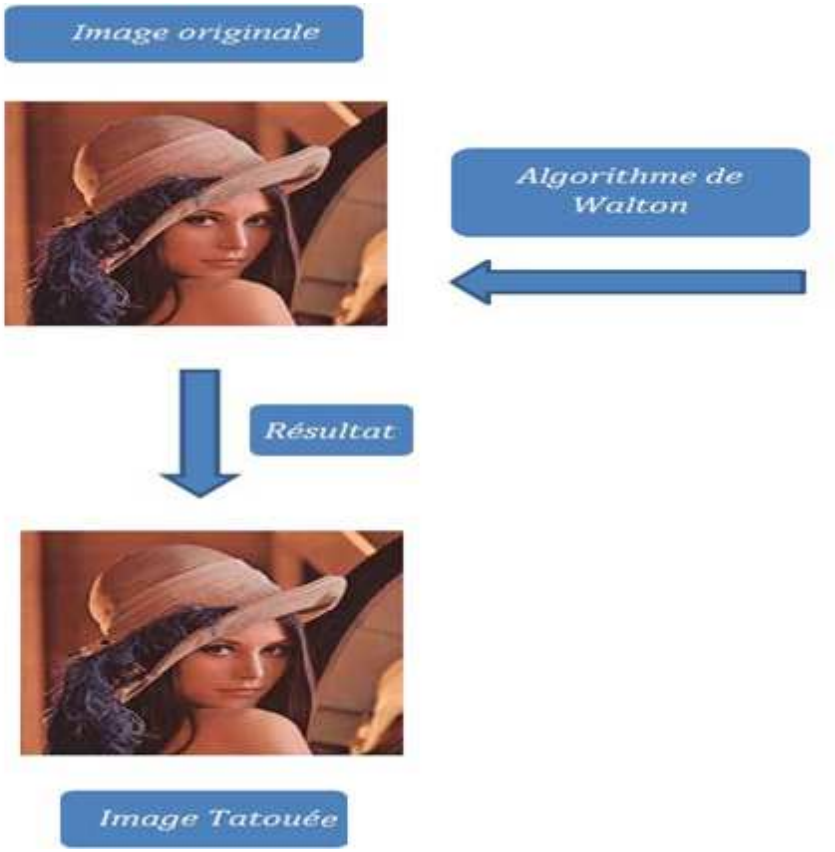


Figure 4 : Exemple de tatouage invisible par la méthode de Walton.

II-3-La somme de contrôle (Checksum):

On transmet une donnée supplémentaire. Cette donnée est la somme d'un bloc de données (par exemple 255 données). Le récepteur fait le même calcul et compare.

Si les checksums sont différents, le récepteur peut demander la retransmission [16].

II-4-Algorithmes de checksum :

- **Parity byte/parity word**: on calcule l'ou-exclusif des octets ou des mots du message. Le résultat est ajouté à la liste de données à transmettre.
- **Modular sum**: on additionne les nombres en tant que nombres entiers non signés en ignorant les dépassements éventuels. Le complément à deux de cette somme est ajouté aux données originales à transmettre.

- **Fletcher, Adler-32 et CRC** (Cyclic Redundancy Check) sont des algorithmes plus performants et largement utilisés. Ils considèrent non seulement les valeurs des données mais aussi leur position dans la séquence pour calculer la valeur de contrôle [17].

II-5-Algorithme de vérification :

L'algorithme de vérification 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.

Avec d'autre manière on peut dire :

Le processus de détection et de vérification d'authenticité de l'image consiste à comparer, pour chaque bloc, la *check-sum* calculée à partir de l'image testée avec la *check-sum* extraite des bits de poids faible [2].

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

Avec cette méthode, il est possible d'intervertir deux blocs homologues (i.e., de même position) de deux images protées 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 [3].

II-6-La faille de Walton :

La méthode de Walton a une faille importante. Il suffit en effet de remplacer une zone de l'image par une autre zone, mais ayant un checksum identique, pour effectuer une modification non détectable. Pour parer à ce problème, Walton propose de rendre le calcul du checksum dépendant de la clé en soustrayant certains pixels, ou encore en les multipliant par les valeurs de la clé [15].

III-Tatouage visible :

III-1-Tatouage d'image par image :

Le tatouage d'image par image est notre méthode pour le tatouage visible qui se réalise en plusieurs étapes :

- Chargement d'image à traiter (B)
- Choisir une position aléatoire dans l'image et la lire
- Chargement l'image de tatouage et lire (A)
- Définir (K)

$$image\ resultat = image\ tatouée + \left(\frac{image\ de\ tatouage}{le\ facteur\ de\ luminosité}\right) \quad (2)$$

- C=A+B/K
- Affichage du résultat(C : image tatouée)

Exemple :

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

K : Facteur de luminosité

Figure 5 : présentation de traitement matriciel pour la méthode du tatouage visible.

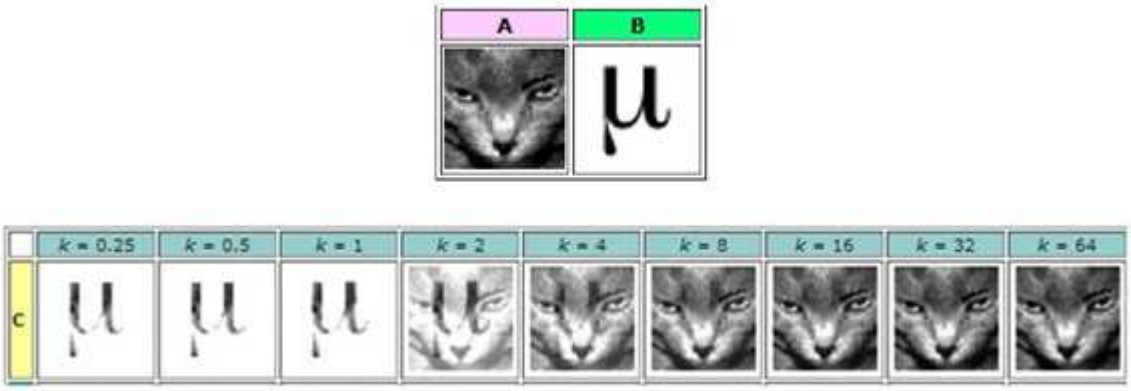


Figure6 : Exemple de tatouage image par image dissimilée

Et le facteur de luminance varie en fonction du choix de l'utilisateur.

En mettant en œuvre cet algorithme nous allons rencontrer deux problèmes majeurs :

- Deux images de taille différente.

- Débordement des couleurs.

Le premier problème est résolu par le redimensionnement de la zone tatouée de l'image camouflée selon deux conditions, l'une, si l'image camouflée est plus grande que celle camouflant, le tatouage aura lieu sur toute l'image camouflée. Deux, nous avons le cas opposé, l'image du tatouage sera redimensionnée selon l'image qui va être tatouée.

Le deuxième problème est cependant un peu délicat, étant donné qu'il s'agit des valeurs des couleurs qui sont dans un intervalle de 0 à 255. Ainsi, afin de résoudre ce problème la solution suivante sera appliquée :

$$la\ couleur\ (rouge, vert\ ou\ bleu)\ dans\ un\ pixel\ (i,j) > 255$$
$$couleur\ =\ couleur\ \%\ 255$$

Finalement le tatouage sera implémenté en utilisant la formule mathématique mentionné ci-dessus.

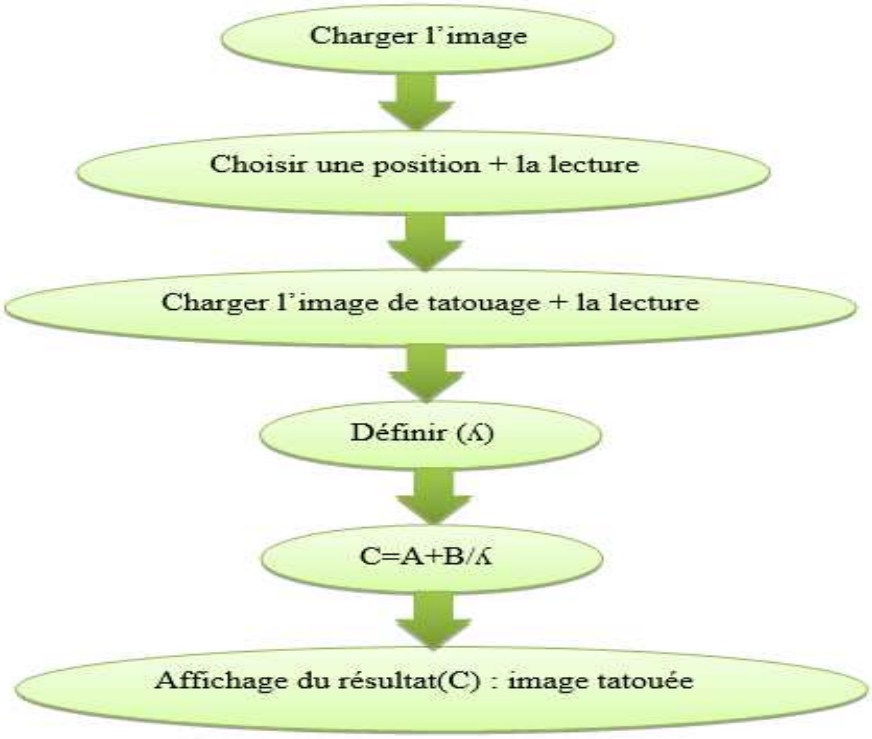


Figure 7: les étapes de tatouage visible

VI-Conclusion :

Dans ce chapitre on a présenté les méthodes de tatouage qu'on va implémenter dans le chapitre 4 d'abord nous avons commencé par la méthode invisible de Walton qui se base sur la somme de checksum et puis on a présenté les étapes de tatouage d'image par image « image dissimulée »pour le tatouage visible.

I-Introduction :

Après avoir pris connaissance dans le chapitre précédent des différentes méthodes de tatouage, ce chapitre porte sur la construction de l'application.

L'application a pour but de tatouer les images numériques d'une manière invisible par La méthode de Walton et de tatouer les images par l'insertion d'image pour le tatouage visible.

II- Ressources utilisées :

II.1. Ressources matérielles :

- Processeur : Intel(R) Core(TM) i5CPU @ 2.53GHz 2.53GHz .
- Mémoire : 4096MB RAM (4GO).

II.2. Resourceslogicielles: Windows 8 Pro 64-bit,C++ Builder

II-3-Outil de développement : C++ Builder

II-3-1-Définition :

Un outil logiciel BORLAND, basé sur le concept de programmation orientée objet, permet à un développeur, même non expérimenté, de créer assez facilement une interface homme/machine d'aspect « WINDOWS ». Le programme n'est pas exécuté de façon séquentielle comme dans un environnement classique. Il s'agit de programmation « événementielle » ; des séquences de programme sont exécutées, suite à des actions de l'utilisateur (clique, touche enfoncée etc).

Au début, C++ Builder a visé seulement la plateforme Windows. Des versions plus récentes ont incorporé Borland une bibliothèque de composants supportée par Linux. En 2003, Borland a sorti le C++ BuilderX (**CBX**), qui avait été écrit avec le même Framework que JBuilder et un peu de ressemblance avec C++ Builder ou Delphi. Ce produit avait visé le développement de larges programmes pour les entreprises. En 2006, Borland a lancé C++ Builder 2006, qui fournit des améliorations considérables et des corrections de bugs. Cette version fait partie de Borland Développer Studio, une seule collection contenant Delphi, C++ Builder et C# Builder [18].

II-3-2-Interface :

L'interface peut paraître déroutante car elle est composée de différentes fenêtres qui ne recouvrent pas tout l'écran. Les applications qui ont été préalablement lancées sont toujours visibles.

On peut distinguer plusieurs zones distinctes :

1-La barre de menu

2-La barre d'outils qui se décompose elle-même en deux parties :

- La palette d'outils pour les opérations classiques
- La palette de composants rangés par catégories (onglets)

3-Une fiche ou Form en Anglais qui représente l'interface en cours de création. Si l'application comporte plusieurs fiches, elles sont cachées et disponibles par le menu et le raccourci clavier F12. Du fait de l'environnement RAD, elles représentent à l'identique les composants à l'exécution (en dehors des composants non visuels).

4-L'inspecteur d'objets qui donne les caractéristiques de l'objet sélectionné dans la fiche, tant au niveau des propriétés (attributs) que des événements.

5-L'éditeur de code avec affichage automatique du code lié à l'objet sélectionné dans la fiche. A chaque fiche correspond deux fichiers : un fichier entête (.h) et un fichier code (.cpp) éditables [18].

II-3-3-Composants de C++ Builder :

Par défaut, C++ Builder utilise un compilateur C++, un éditeur de liens, un compilateur de ressources et un gestionnaire de projets intégrés.

Il est toutefois possible de spécifier la volonté d'utiliser les outils en ligne de commande livrés avec C++ Builder ou bien d'autres outils tiers. Cette dernière possibilité est très utile lorsque l'on veut utiliser des modules compilés avec d'autres langages. Il est fortement conseillé de lire les chapitres correspondants dans le manuel du développeur [18].

III-Domaines de tatouage :

Toute type d'information a besoin d'être sécurisée, ce projet s'intéresse au fait à la manière d'authentifier l'image numérique par tatouage numérique (visible, invisible et hybride) qui peut être appliqué sur plusieurs domaines, parmi ces derniers on cite les suivants :

- Imagerie médicale.
- Imagerie aérienne.
- Imagerie numérique.
- Imagerie astronomique.
- Production cinématographique.
- Photographie.
- Imagerie satellitaire.

IV-Conception :

Le but de notre application est d'implémenter une authentification des imagesnumériques par un tatouage (visible,invisible,hybride) ce travail est réalisé comme suite :

IV-1-Tatouage invisible :

- Charger l'image originale
- Convertir l'image en matrice
- Appliquer l'algorithme de tatouage invisible
- Convertir la matrice résultante en image
- Afficher le résultat (image tatouée)
- Enregistrer l'image tatouée

IV-2-Tatouage visible :

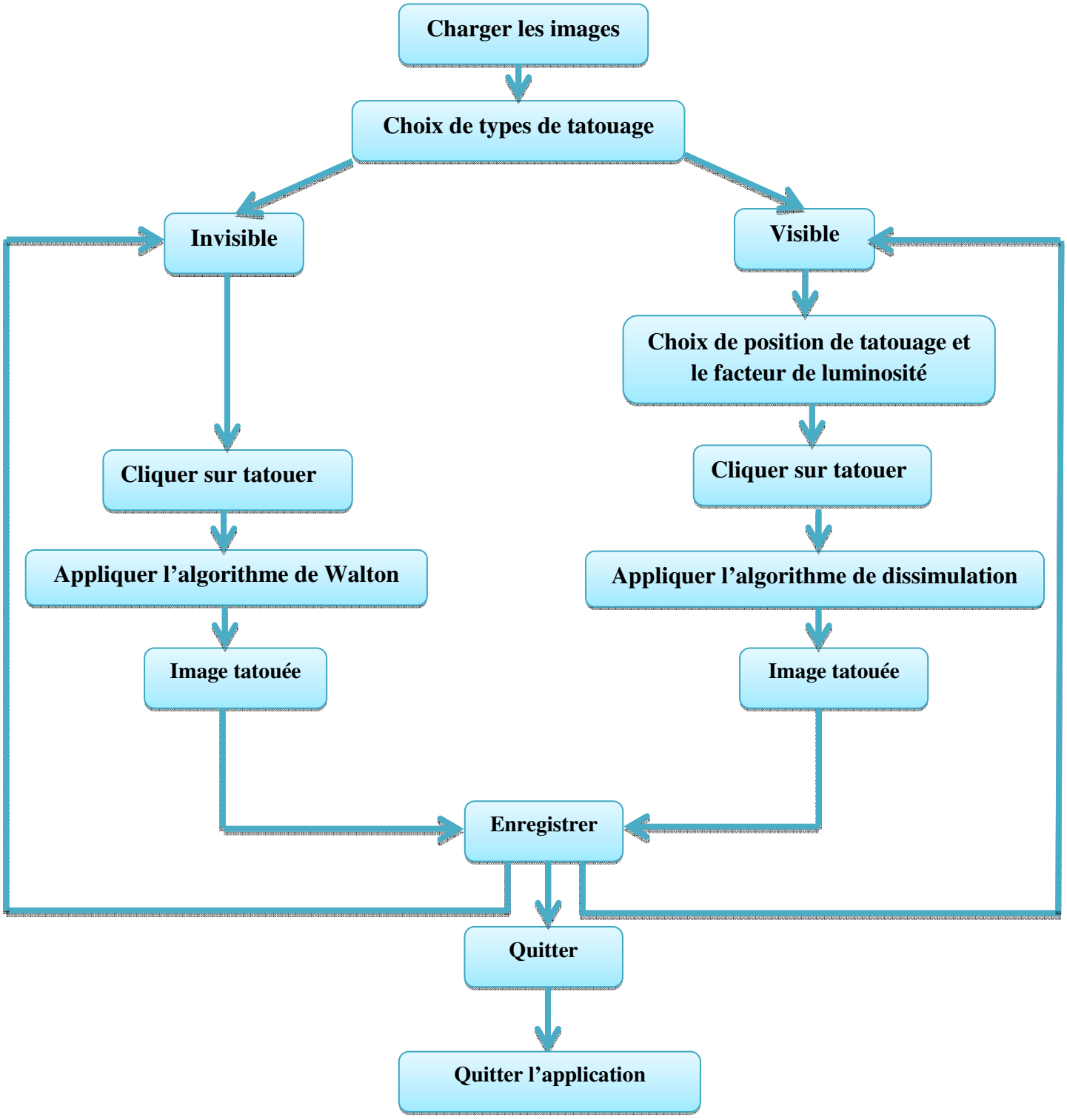
- Charger l'image originale et l'image tatouage.
- Convertir chaque image en matrice.
- Appliquer l'algorithme de tatouage.
- Convertir la matrice résultanteen image.
- Affichage du résultat (image tatouée).
- Enregistrer l'image tatouée.

IV-3-Tatouage hybride :

Dans cette étape on va commencer par l'un des tatouages et on va enregistrer l'image résultantepuis on vaappliquer le deuxième tatouagenon fait dans la première partie sur cette image. On obtient alors une image tatouée par un tatouage hybride.

V- Organigramme d'application :

Ces étapespeuvent être représentées par l'organigramme suivant :



FigureIV.1 : organigramme de l'application

VI-Présentation d'application :

A propos de notre application :

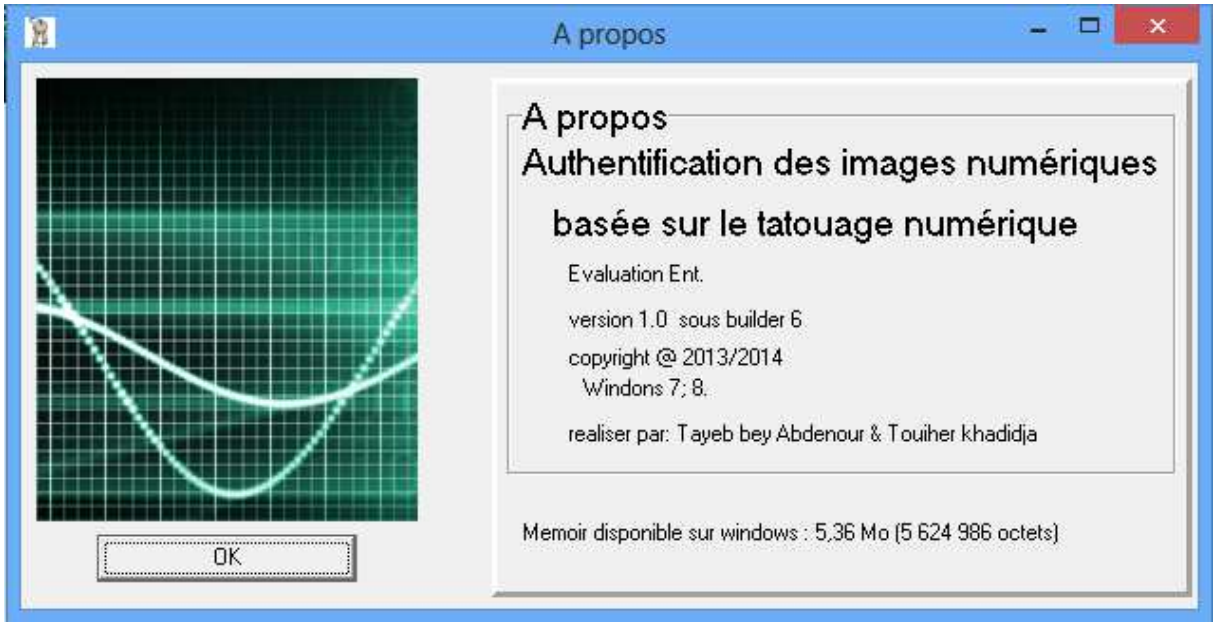


Figure IV.2 : A propos.

On commence la présentation de notre application par l'interface d'accueil.

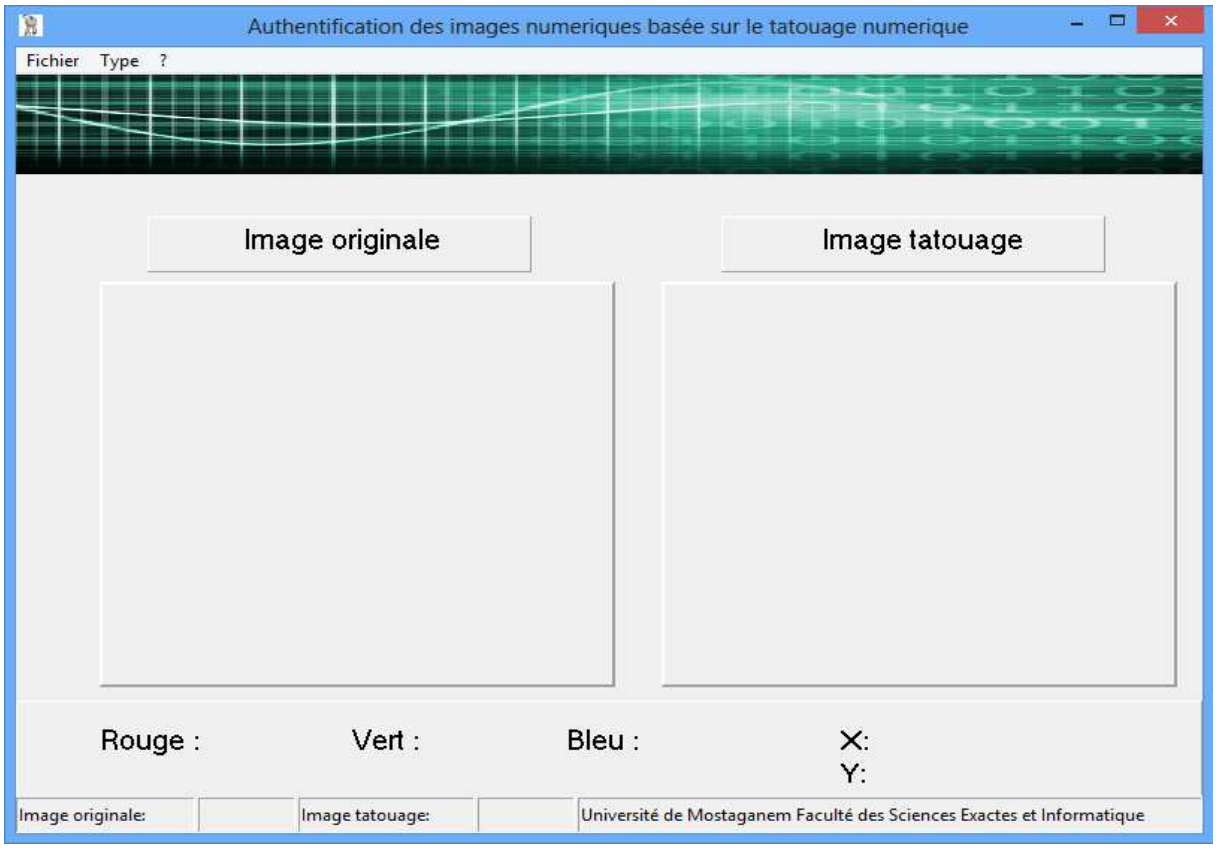


Figure IV.3 : Interface d'accueil.

On charge les images (image originale et image tatouage).

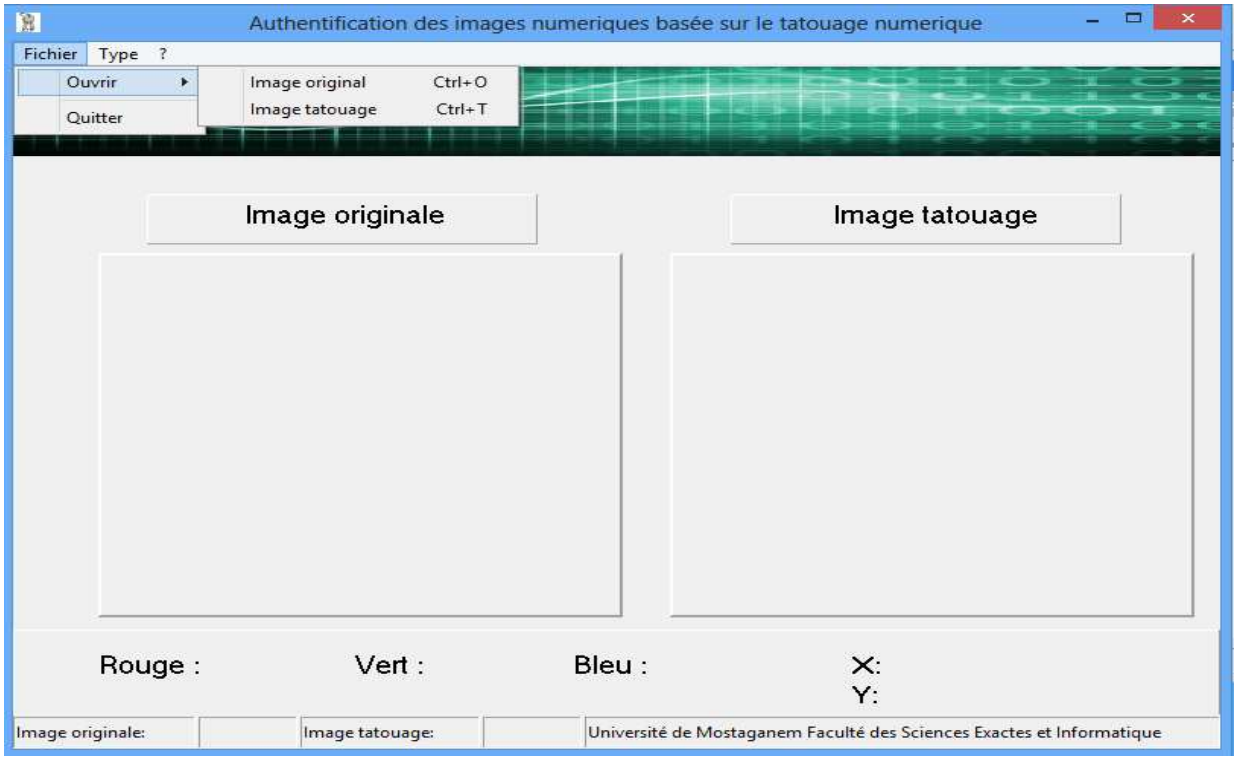


Figure IV.4 : Chargement des images.

Après le chargement des Images on va avoir cette figure.

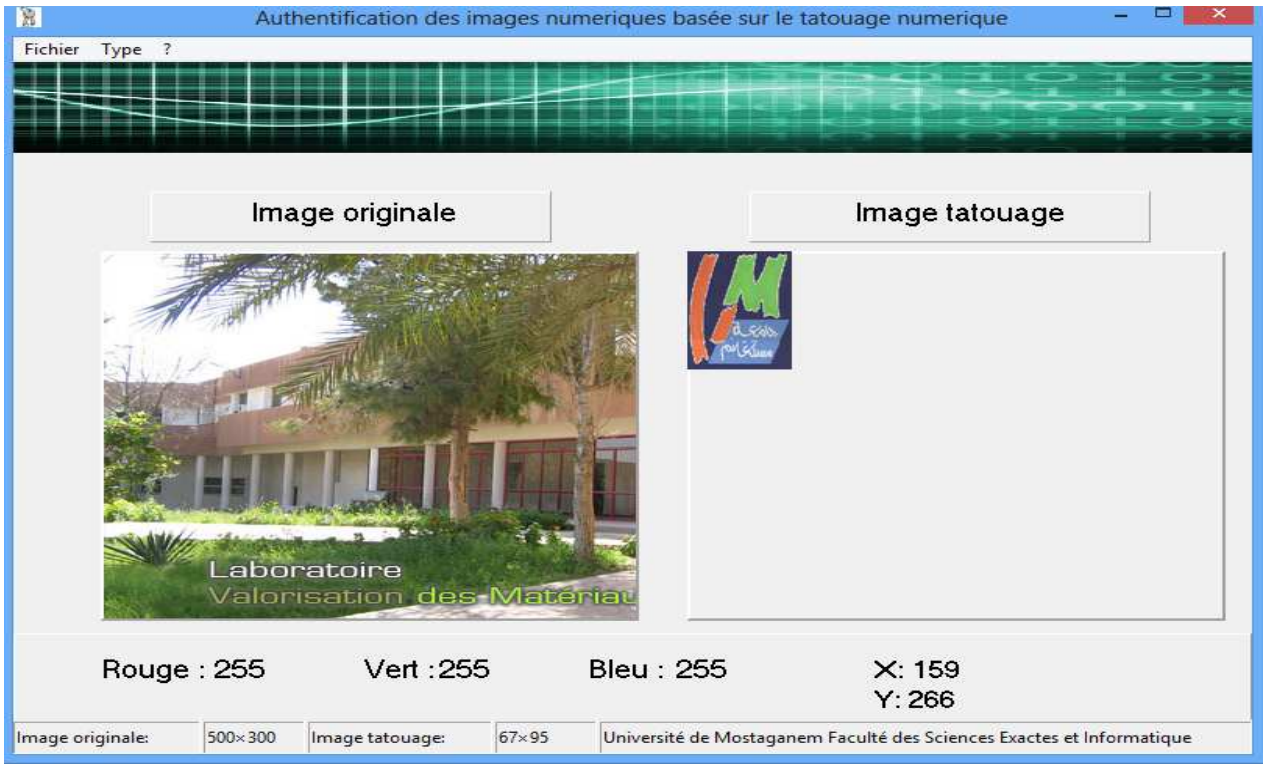


Figure IV.5 : Interface des images charger

Après on fait le choix du tatouage, en cliquant sur type pour choisir le type du tatouage.

VI-1- Tatouage visible :

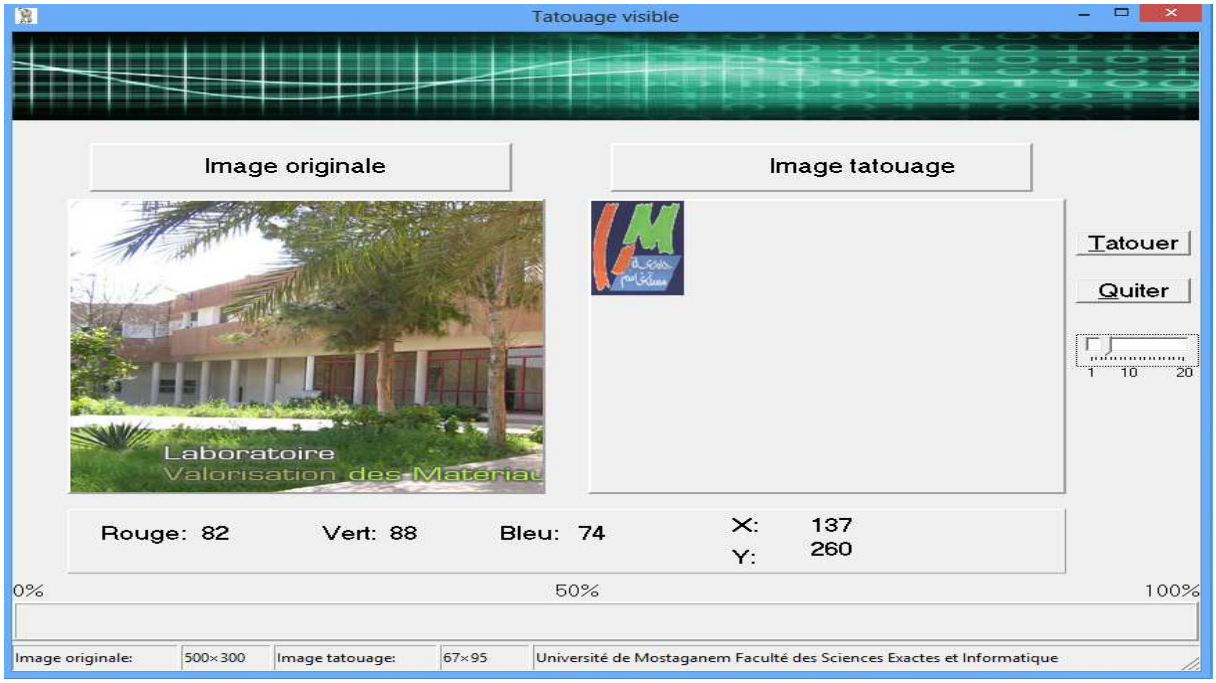


Figure IV.6 : Interface de tatouage visible.

Dans ce cas, on doit choisir la valeur de K ainsi que la position d'insertion du tatouage , voici le résultat du tatouage visible :

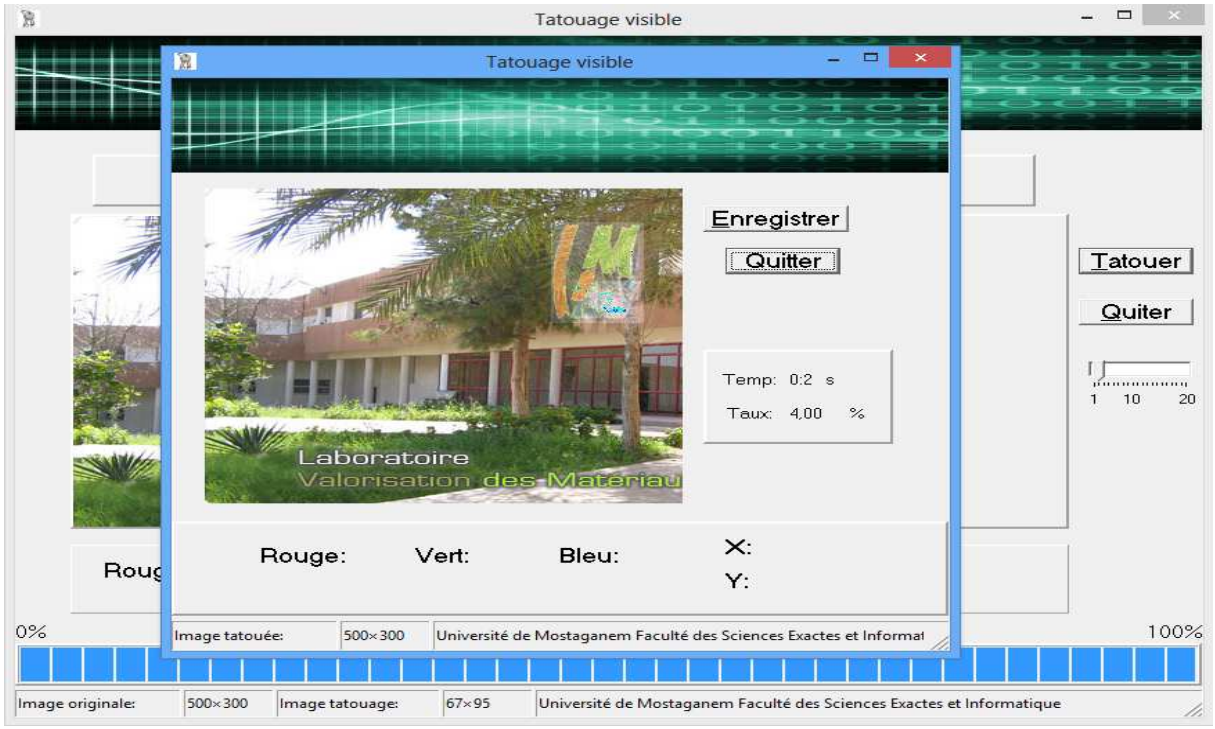


Figure IV.7 : Interface de résultat du tatouage visible.

VI-2-Tatouage invisible :

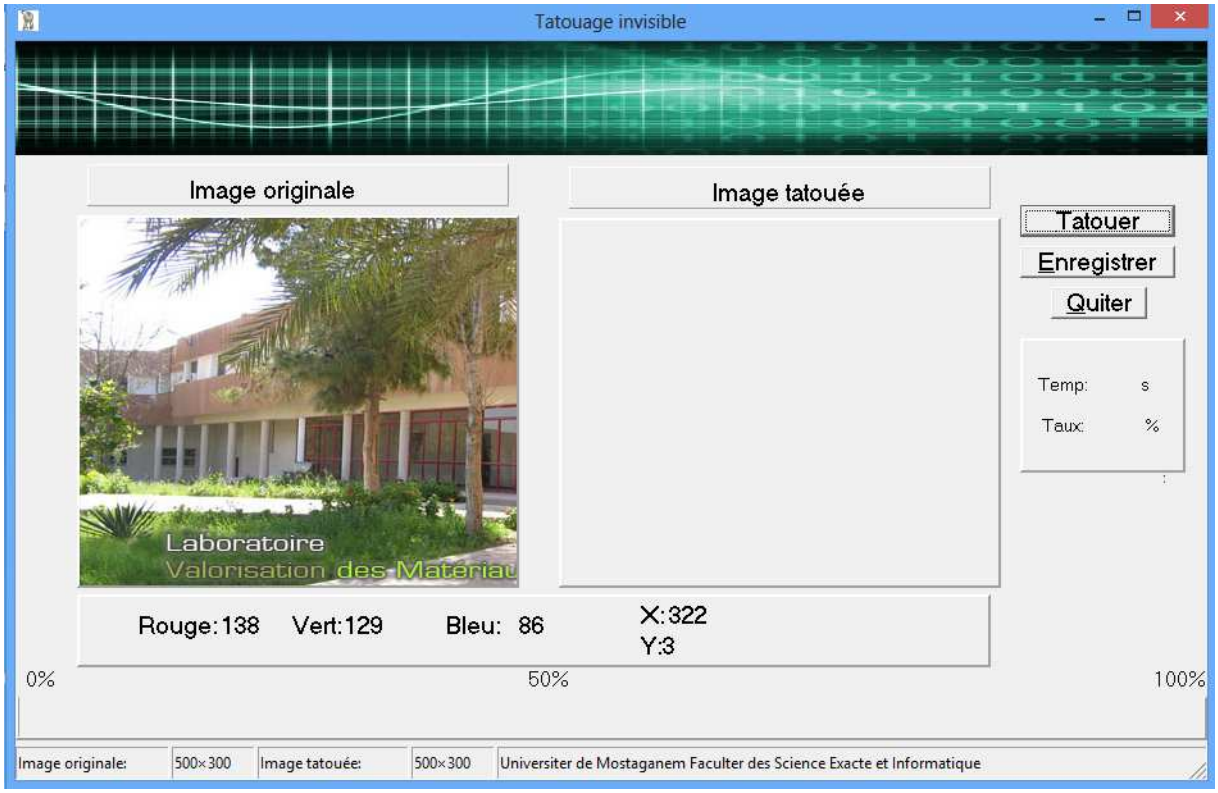


Figure IV.8 : Interface de tatouage invisible.

On clique directement sur tatouer et voici le résultat :

Figure 8 : Interface de résultat du tatouage invisible.

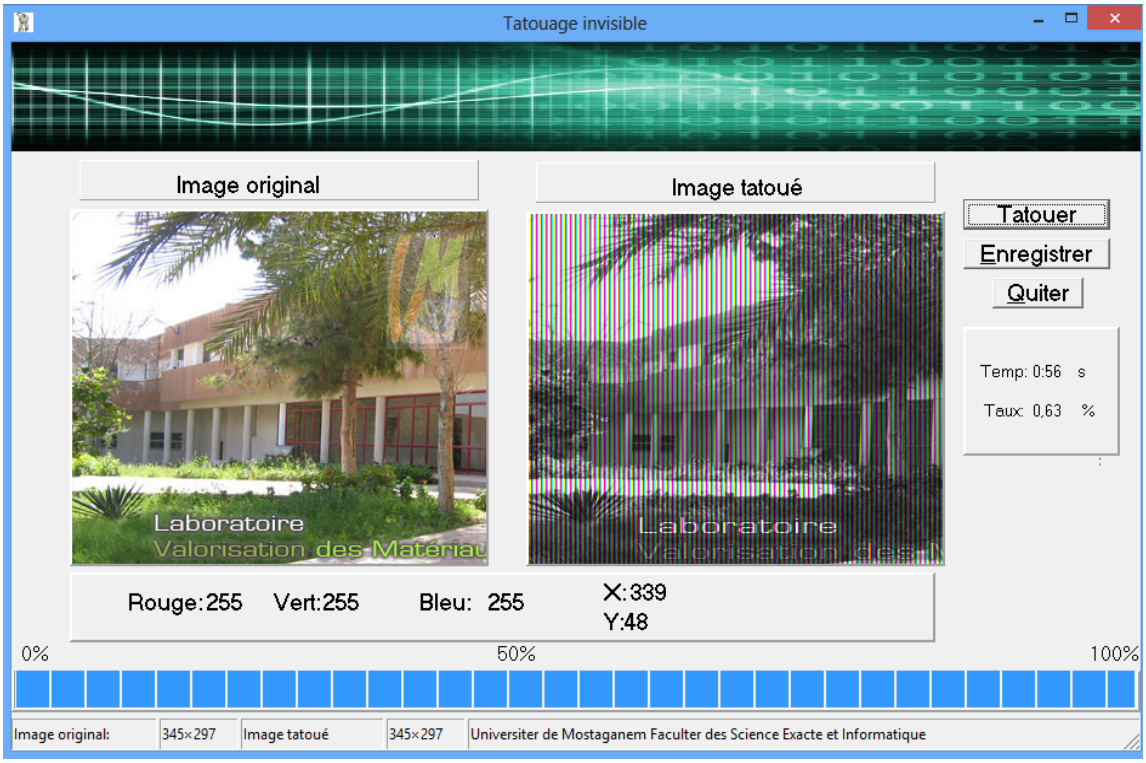
VI-3-Tatouage hybride :

Notre problématique est de réalisé un tatouage hybride pour avoir une authentification efficace et robuste alors on a proposé deux méthodes :

VI-3-1-Premier méthode (visible +invisible) :

- On commence par un tatouage visible on fait l'enregistrement du résultat.

- On applique un tatouage invisible sur le résultat(obtenu par le tatouage visible).



VI-3-2-Deuxièmeméthode (invisible +visible) :

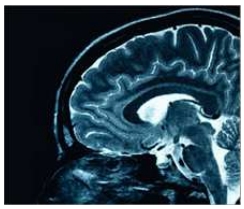
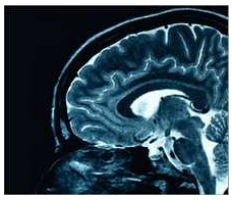
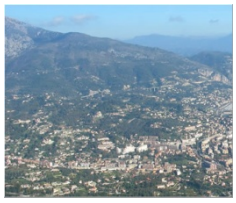
- On commence par un tatouage invisible on fait l'enregistrement du résultat.

- On applique un tatouage visible sur le résultat(obtenu par le tatouage invisible)

VII-Résultats :

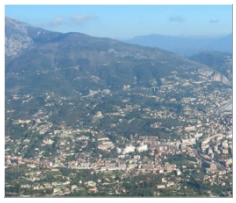
Après l'implémentation de notre application sur plusieurs exemples on obtient les résultats suivants :

VII-1-Tatouage invisible :

Image originale	Image tatouée	temps	taux
Image médicale : 	Image médicaletatouée : 	0 :56 s	0,48%
Image photographique : 	Image photographique tatouée : 	1:0 s	0,53%
Image aérienne : 	Image aérienne tatouée : 	1:39s	0,39%

VII-2-Visible :

Image originale	Image tatouage	Image tatouée	temps	taux
Image médicale : 			0:2 s	6%

Image photographique : 			0:2 s	4%
Image aérienne : 			0:2 s	31%

VII-3-Hybride :

VII-3-1-Premier méthode (visible +invisible) :

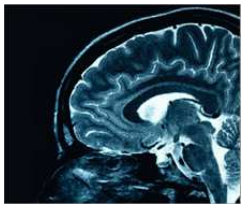
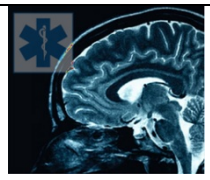
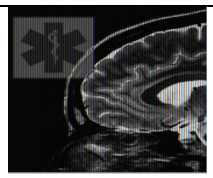
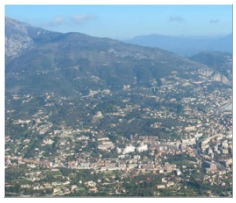
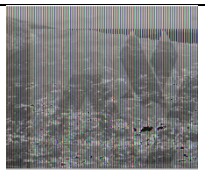
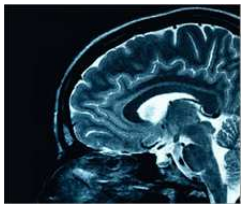
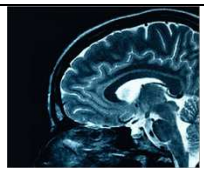
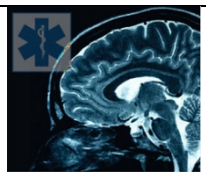
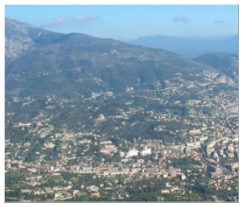
Image originale	Image tatouage	type	Image tatouée	temps	taux
Image médicale 		Tatouage visible		0:2s	6%
		Tatouage invisible		0 :56 s	0,48%

Image photographique : 		Tatouage visible		0 :2 s	4%
		Tatouage invisible		1:0 s	0,53%
Image aérienne : 		Tatouage visible		0 :2s	31%
		Tatouage invisible		1 :39	0,39%

- **Deuxième méthode (invisible +visible) :**

Image originale	Image tatouage	type	Image tatouée	temps	taux
Image médicale 		Tatouage invisible		0 :56 s	0,48%
		Tatouage visible		0:2s	6%

Imagephotographique : 		Tatouage invisible		1:0 s	0,53%
		Tatouage visible		0 :2 s	4%
Image aérienne : 		Tatouage invisible		1 :39	0,39%
		Tatouage visible		0 :2s	31%

VIII-Discussions :

Après les résultats trouvés,on obtient les remarques suivantes :

- Si on applique le tatouage visible sur une image, le tatoue sera clair à l'œil humain est vraiment facile à détecter.
- Le tatouage invisible nécessite un scanner pour savoir qu'il y a une modification sur l'image puis que la contrainte d'imperceptibilité existe dans ce type de tatouage.

- On a aussi appliqué le tatouage hybride avec ses deux modes où on a obtenu des résultats déférents :
  - Le premier est l'application du visible puis l'invisible qui nous a donné une grande perte d'information.
  - Le deuxième est l'application de l'inverse (invisible puis visible) on obtient une image tatouée robuste.
- Si on compare les résultats de tatouage en fonction de temps ,on remarque que le visible est plus rapide que l'invisible puisque le premier est une opération d'addition entre deux images mais le deuxième fait un changement de pixel plus une comparaison qui se base sur la somme de check-sum en fin de traitement, il faut noter que de temps est lié aussi avec un autre facteur qui est la taille d'image.

- Si on fait la même chose une autre comparaison en fonction du taux qui est le nombre des pixels changés par rapport au nombre total dans l'image on constate que cetélément est plus grand si on applique le tatouage visible puisqu'il y a une autre image qui va être ajouté à l'image originale (c.-à-d. un nouveau ensemble de pixels), et comme la taille d'image influence sur le temps donc elle influence de la même manière sur le taux.

IX-Conclusion :

Dans ce chapitre on a vu trois implémentations du tatouage numérique et leur fonctionnement par la conversion ainsi que l'application de l'algorithme de tatouage ,au début on a réalisé un tatouage visible qui est l'addition entre image originale et image tatouage avec un facteur de luminosité et puis un tatouage invisible qui est le traitement de pixel avec la méthode de Walton (la somme de checksum) et on a terminé par l'inclusion du tatouage hybride et robuste qui est le tatouage invisible puis le tatouage visible afin de renforcer l'authentification de l'image donc du droit d'auteurmalgré le temps et le taux sont élevés mais le plus important est d'avoir une bonne sécurité de l'image numériques.

.

Conclusion générale :

Dans ce mémoire, nous avons abordé la problématique de l'authentification des images numériques, problème qui a pris de plus en plus d'importance depuis le développement d'internet et des réseaux d'échange et la dématérialisation des contenus multimédias, où on a implémenté un tatouage visible, invisible et hybride pour résoudre ce problème.

Pour réaliser notre projet nous somme passé par les chapitres suivants :

ChapitreI :on a présenté une introduction sur les images numériques où on a donnéun ensemble de définitions pour connaitre le plus possible dans le domaine des images numériques.

ChapitreII : on a présenté une introduction sur le tatouage numérique qui nous aide à comprendre cette nouvelle technique de sécurité.

Chapitre III : on a présenté lesméthodesà implémenter.

Chapitre IV : on a présenté une implémentation de l'application qui se compose en trois méthodes : le tatouage visible, invisible et l'hybride.

Puis que la sécurité 100% en informatique reste toujours impossible, c'est comme la cryptographie qui perd son efficacité si quelqu'un réussità déchiffrer le document,donc le tatouage est devenu comme une nouvelle technique de protectionpour empêchertoute évènement non autorisé sur les documents multimédias mais le problème qui se pose est le détatouage,malgré les méthodes de ce dernier sonten cours d'être réalisable donc après plusieurs essais ,ils vont devenir une réalité et un grand problème .

Mais si on compare la cryptographie et le tatouage donc le dernierest plus performant que la première technique puis que le détatouage est plus difficile et prend plus de temps par rapportau décryptageet même dans les types de tatouage il y a un qui donne une sécuritésupplémentaire que les autresoù on trouve le tatouage hybride (invisible puis visible)qui reste le meilleure entre les 3 types.

Enfin suggérons pour des travaux futurs :le détatouage légal en connaissant l'algorithme utilisé pour le tatouage malgé on ne voit pas son utilité car si on doit tatouer une information est pour la garder authentique par contre le détatouage illégal comme une attaque est plus approprié à le faire. On propose aussi une hybridation entre le tatouage et la crypto pour garantir plus de sécurité.