Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab de Blida

Faculté des sciences

Département d'informatique

Mémoire Présenté par

Ghazi Sid Ali

En vue d'obtenir le diplôme de Master

Domaine : Mathématique et Informatique. MI

Filière : Informatique.

Option : Ingénierie des logiciels.

Titre :

Sécurité des images empreintes digitales par tatouage numérique pour la protection de propriété de l'identité et l'authentification du contenu.

Promoteur : Ait Saadi Karima

Encadreur : M.MASSIED

Organisme d'accueil : CDTA

CDTA

Soutenue le : devant le jury composé de :

-M Président

-M Examinateur

-M Examinateur

- promo 2012/2013 –

Remerciements

Je remercie ALLAH de m'avoir accordé santé, énergie et volonté pour réaliser ce travail.

Ce travail de recherche est sans doute l'aventure d'étude la plus enrichissante de ma vie, et n'aurait pas été aussi fructueuse sans l'aide des personnes qui m'ont soutenu tout au long de cette année de stage.

J'adresse mes remerciements les plus chaleureux à ma promotrice Mme. AIT SAADI KARIMA cadre de recherche au sein du (CDTA), qui s'est montrée à la fois dure, sérieuse et professionnelle durant la préparation de ce projet, mais aussi aimante et chaleureuse qu'une mère puisse l'être. Sa claire voyance, son tact pédagogique et les bénéfices des ses larges expériences nous ont étaient précieux.

Je tiens aussi à remercier Mlle BOUCHAIR IMENE, membre de l'équipe de recherche dirigée par Mme AIT SAADI, pour son aide et ses conseils qui ont permis à faire de ce travail un réel chalenge. Mes remerciements sont également adressés envers Mr le docteur ZEBBICHE KHALIL capitaine de la gendarmerie national pour ces éclaircissements apporté dans le domaine mathématiques et théorique de ce travail.

Aussi, je remercie Mlle HERMA Hadjer, une camarade de classe qui fut une grande inspiration de sérieux et de discipline, ainsi qu'une source de volonté et d'entraide inépuisable.

Ma grande reconnaissance va aussi aux professeurs de la faculté de SAAD DAHLEB de Blida, priant de trouver ici l'hommage de mon grand respect.

Ghazi Sid Ali .

Sommaire

References

[01] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Secure data hiding in wavelet compressed fingerprint images," in *Proc. of the ACM Multimedia Workshops 2000*, OCT. 2000, pp. 127–130.

[02] Hartung, F., Kutter, M.: Multimedia watermarking techniques. Proceedings of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[03] C.H. Lee and Y.K. Lee, «An Adaptive Digital Image Watermarking Technique for Copyright Protection», in Proceedings of the Ninth National Conference on Information Security, Taichung, Taiwan, May 14-15, pp. 1-7, 1999.

[04] E.KHELIFI, "image compression and watermarking in the wavelet transform domain ",Phd, Queen's university of Belfast, UK, Mai 2007

[05] Y. S. Kim, O-H. Kwon, R. H. Park, «A wavelet based watermarking method for digital images using the human visual system», Korea, 1998.

[06] A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, «Information Hiding – A survey» Proceedings of the IEEE, special issue of multimedia content, 87(7): 1062- 1078, July 1999.

[07] I.Cox, M, Miller, and J. Bloom digital watermarking; principale & practices Morgan Kaufmann Publisher, san Francisco, CA, USA,2002

[8] F . RAYNAL " études d'outil pour la dissimulation d'information: approches fractales, Protocol cryptographique" thèse de doctorat, université de Paris IX, mars 2002

[9] Vu Duc Minh et NGUYEN Thi Hoang Lan Maiti « tatouage des images dans un domaine fréquentiel » pp 6-14, 15 janvier 2006

[10] Norforna Corina « filigrane dans le domaine des ondelette » mémoire de diplôme pour obtenir le degré de M.Sc, l'univercité « politechnica » Timisoara, faculté .

[11] N. K. Ratha, M. A. Figueroa-Villanueva, J. H. Connell, and R. M. Bolle, "A secure protocol for data hiding in compressed fingerprint images," in *ECCV Workshop BioAW 2004*, OCT. 2004, pp. 205–216.

[12] I.J Cox, J Kilian, T Leighton and T Shamoon " secure spread spectrum watermarking for multimedia ",IEE trans, on image processing 6,12, 1673-1687. 1997)

[13] D. Kundur et D. Hatzinakos, "mistmatching perceptuals models for effective watermarking in the presence of compression », proceeding of SPIE, multimedia systems and application, Vol 3845, PP.22-42, September 199

[14] UE Analyse Multi resolution et ondelette " application de l'apprentissage parcimonieux en traitement d'image .

[15] O.R. Vincet Clausthal University of technology, Germany « A description algorithm for Sobel Image Edge Detection "

[16] www-fourier.ujf-grenoble.fr/~decauwer/hachage.pdf

[17] http://www.mscs.mu.edu/~mikes/icpc/nov1/hamming.htm

[18] Perceptual Image Hashing Based on Virtual Watermark Detection Fouad Khelifi, *Member, IEEE* and Jianmin Jiang

[19] www.iacr.org/phds/58_ThomasPeyrin_Analysedefonctionsdehachagecry.pdf

Liste des figures

Liste des tableaux

INTODUCTION GENERALE

L'usurpation de l'identité est devenue un problème fréquent, les fraudes et les falsifications de documents ont connu leurs apogées avec l'avancée informatique, La sécurité de l'information est devenue une des principales préoccupations des chercheurs et développeurs, un des sujets de développement les plus convoité de nos jours est la technologie biométrique. Elle démontre bien qu'elle peut diminuer les risques de fraude et améliorer grandement la sécurité des systèmes d'identification. Et bien que ces systèmes soient plus utilisés que d'autres, ils ne sont pas à l'abri des erreurs comme la plupart des gens le pensent.

Effectivement, ces systèmes sont vulnérables à plusieurs attaques. Ratha [01] a classé ces attaques en huit points : attaque sur le capteur, sur les canaux de transmission entre les différents modules, sur le module d'extraction des caractéristiques, sur la base de données et sur le module de comparaison et décision. Parmi celles-ci, nous trouvons l'attaque produite lors de l'acquisition et l'enregistrement de l'empreinte digitale et l'attaque ciblant la modification du contenu.

Pour prémunir contre ce type d'attaques, plusieurs méthodes de sécurisation ont vu le jour parmi ceux-ci, on trouve la Sécurisation des images d'empreintes basée sur le tatouage numérique pour protéger la propriété de l'identité de l'individu et les approches d'authentification pour assurer l'intégrité du contenu.

L'objectif de ce mémoire est de développer deux approches de sécurité des empreintes digitales : la première pour pallier au problème de perte d'identité et qui est basée sur le tatouage robuste, et la seconde pour vérifier l'authenticité du contenu de l'empreinte en appliquant les techniques du hachage perceptuel.

Ce projet s'inscrit dans le cadre du projet de recherche intitulé «***Sécurisation des documents multimédias par tatouage numérique***» initié conjointement par le Centre de Développement des Technologies Avancées (***CDTA***) et le Centre de Recherche-Développement de la Gendarmerie Nationale (***CRD-GN***).

Le mémoire sera structuré de la façon suivante :

Le chapitre I présentera des généralités sur le tatouage numérique, son principe, ses domaines d'utilisation, la classification de ses techniques. Il expliquera aussi comment le tatouage numérique peut être le meilleur moyen afin de sécuriser les systèmes d'authentification à base d'empreinte digitale.

Le second chapitre contiendra une étude détaillée sur le tatouage robuste, ses propriétés et son application dans la protection des images d'empreintes digitales pour développer la solution proposée. Aussi, nous donnerons les résultats des tests effectués et les performances de la méthode développée.

Dans le troisième chapitre, nous présenterons la méthode d'authentification du contenu de l'empreinte pour vérifier son intégrité. Pour cela, nous introduirons le concept du hachage perceptuel utilisé. Ainsi, ce chapitre comprendra les différents tests et résultats obtenus suite à l'évaluation de l'approche réalisée.

Dans le chapitre IV une présentation graphique de l'interface de l'application sera présentée, ainsi que la fonctionnalité offerte par celle-ci.

Et enfin, nous terminerons ce mémoire par une conclusion et les perspectives.

CHAPITRE I

LE TATOUAGE NUMERIQUE

I.1 Introduction :

Afin de sécuriser la circulation des œuvres « copyright » le tatouage des images à vu le jour, cela fut dans le début des années quatre-vingt-dix. Depuis ce temps, l'image a changé de forme et elle est passée au format numérique ce qui a grandement facilité son traitement et sa manipulation mais en même temps la numérisation de l'image a rendu celle-ci vulnérable aux attaques que peut subir n'importe quelle information numérique telles que : la modification, la distribution et la copie illégale. Face à ce changement, le tatouage des images est passé lui aussi au numérique pour devenir le tatouage numérique des images qui consiste à insérer une information invisible dite Marque dans l'image. Cette marque doit être suffisamment imperceptible pour ne pas infecter la qualité et le contenu de l'image, et doit être assez robuste pour être récupérée après une éventuelle manipulation de l'image.

I.2 Principe du Tatouage Numérique :

Le tatouage numérique, est l'une des applications les plus prometteuses de la stéganographie. Mais, avec ce concept, il ne s'agit plus de cacher une marque dans un document mais de le marquer d'une façon indélébile [02]. Le document peut être de diverses natures : texte, image, son, vidéo.

En général, un schéma de tatouage numérique comprend deux processus fondamentaux: le processus d'insertion et le processus d'extraction.

I.2.1 Insertion de la marque :

Cette phase d'insertion (**Figure I.1**) s'effectue dans les composantes perceptibles de la donnée (comme la luminance des pixels d'une image), et non dans l'entête d'un fichier. La marque insérée doit pouvoir être extraite et décodée, mais doit être imperceptible, c'est-à-dire que la déformation doit être suffisamment faible pour que l'être humain ne puisse pas différencier la donnée tatouée de la donnée d'origine, ni même savoir où chercher. Pour un tel résultat, on introduit dans cette fonction, en outre des deux paramètres « la donnée d'origine et la marque à insérer », un troisième paramètre qui est la Clé de chiffrement. Cette clé peut servir soit à la mise en forme de la signature soit pour localiser sur la donnée d'origine, la position des pixels où il va y avoir l'insertion. [01]

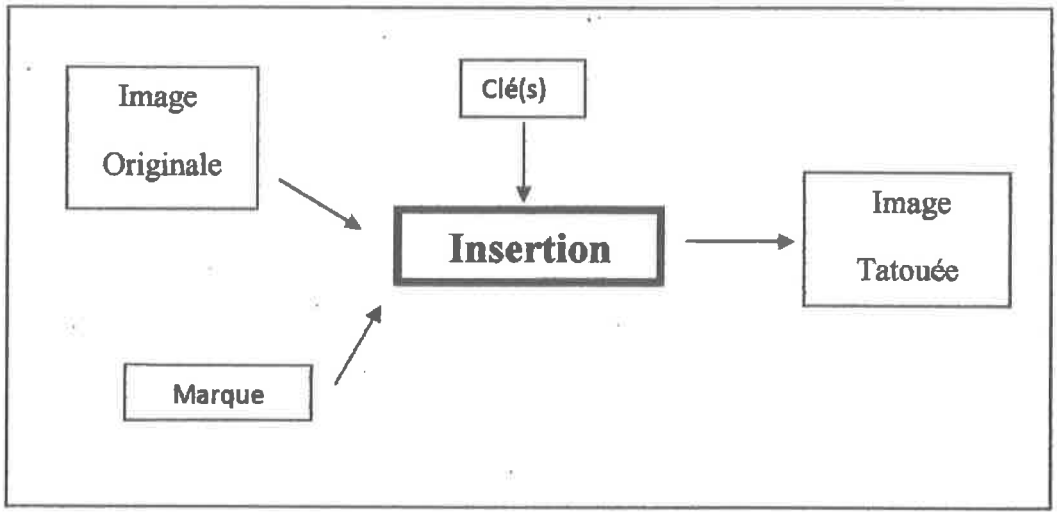


Figure I.1 Schéma général d'insertion de la marque

I.2.2 Extraction de la marque :

Cette phase (**Figure I.2**) permet d'extraire la marque, ceci peut être réalisé par extraction complète de la marque inséré ou par une simple détection. Pour ce faire, l'image tatouée et la clé de chiffrement sont nécessaires. [01]

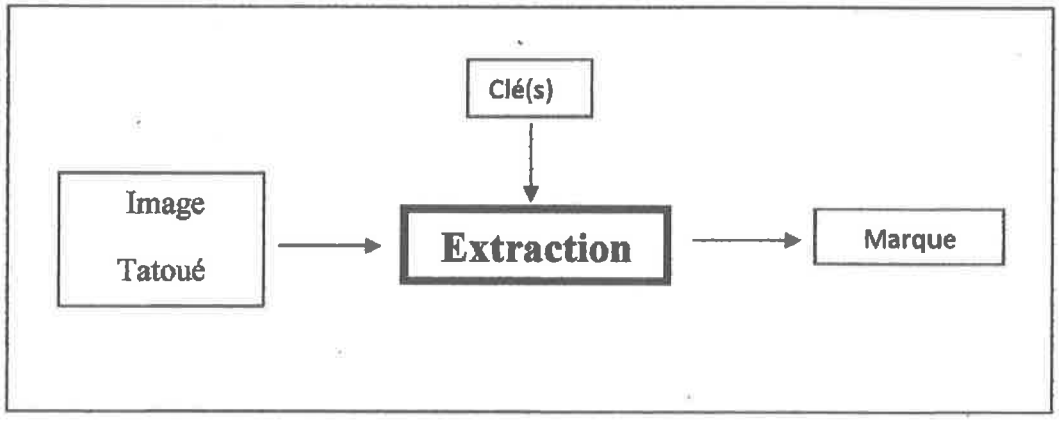


Figure I.2 Schéma d'extraction de la marque

I.2.3 Propriétés de la marque

Toute marque insérée doit satisfaire essentiellement trois contraintes : la capacité, l'invisibilité et la robustesse (**Figure I.3**).

- **Capacité :** elle représente la quantité d'information que l'on insère dans l'image hôte. La robustesse est liée directement à la taille de la marque, une marque qui comporte plus de bits qu'une autre aura plus de robustesse face aux attaques. Cette relativité n'est pas toujours vraie, en effet, une marque de très grande capacité peut dégrader la qualité de l'image hôte. ce qui la rend visible. [04]

- **Invisibilité** : la marque doit être invisible. En effet, une marque visible peut être aisément écrasée par une autre marque. De ce fait garantir l'invisibilité de la signature revient à respecter la qualité visuelle de l'image. Aucune dégradation ne doit être aperçue sur l'image tatouée. C'est pour cette raison que plusieurs algorithme de marquage existants ont tendance à effectuer l'insertion dans les zones d'intérêt les moins sensibles a l'œil humain (contour, zone texturé,...). [09]

- **robustesse** : Etre robuste c'est équivalent à pouvoir retrouver la marque insérée quelles que soient les modifications que peut subir l'objet tatoué. Ces modifications sont dues à plusieurs types de traitements (attaques) dont trois sont essentiels. Le premier concerne les attaques simples telles que la compression JPEG, le filtrage, l'addition de bruit, l'impression suivie par une numérisation à l'aide d'un scanner. Cette classe ne change pas la géométrie de l'image alors que la deuxième catégorie la modifie. On y trouve la rotation, le changement d'échelle et les transformations affines. La plupart des systèmes de marquage résistent à ces transformations simples mais ne supportent pas la combinaison de plusieurs d'entre elles.
  La troisième catégorie d'attaque vise à introduire une ambiguïté. Ceci peut être réalisé par une attaque de sur-marquage dans laquelle on insère d'autres marques pouvant créer un conflit pour décider quelle est la vraie marque d'origine.
  F. Petitcolas et al. Détaillent bien dans [04] ces différentes attaques.

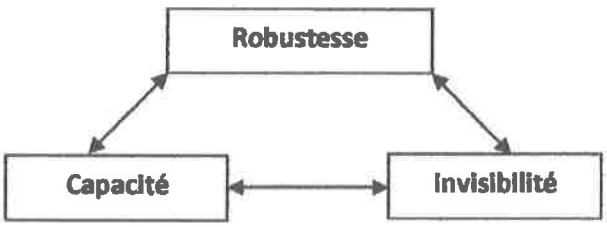


Figure I.3 : Propriété de la marque

I.3 Domaines d'application du tatouage numérique

Actuellement, le tatouage numérique est un domaine de recherche très actif. Il commence à être introduit dans différentes applications qui nécessitent d'être sécurisées. Parmi ces applications, on cite :

- **Protection des droits d'auteur** : la protection des droits d'auteur a été l'une des premières applications étudiées en tatouage numérique et elle reste cependant toujours d'actualité et concerne encore la majorité des publications dans ce domaine. L'objectif est d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce, même si le document concerné a suivi des modifications par rapport à l'original. Cet objectif peut être accompli par le tatouage car il offre des fonctionnalités d'insérer les droits d'auteur (information) dans le document, et par conséquent, ces droits deviennent une partie intégrante du contenu du document.
- **Authentification** : l'objectif de cette application est de détecter si un document a subi des manipulations, ceci peut être fait en utilisant une marque fragile, si celui-ci est modifié ou manipulé, la marque sera détruite et donc on déduit que le document a bien été modifié et qu'il n'est plus authentique.
- **Protection contre la copie illégale** : cette application consiste à intégrer une marque « intelligente » dans un document : et cela en utilisant un matériel particulier. En effet, les appareils doivent pouvoir détecter la marque et agir en conséquence, c.à.d. en permettant ou pas la lecture ou la copie de la marque.
- **Indexation** : l'indexation des fichiers ou documents consiste à classer de manière automatique ces documents selon leur contenu, et cela dans le but de faciliter la recherche et l'accès à ces documents. Les techniques classiques utilisées consistent à effectuer les traitements automatiques du document, de manière à dégager les composantes essentielles du contenu. Alors que le tatouage d'un document permet aussi d'insérer une information (contenant peu de bits) permettant de qualifier sommairement son contenu ou d'insérer un pointeur vers une description plus complète.

- **Transmission secrète** : pour échanger secrètement des messages, on peut les cacher dans une donnée porteuse (par exemple, image) de façon aussi discrète que possible. Quand on transfère cette porteuse, les messages cachés passent inaperçus pour une tierce partie.
- **Gestion des transactions** : dans ce type d'application, on insère l'identité du vendeur et celle de l'acheteur dans les documents multimédias. Les propriétaires successifs du document, et donc les sources de copie d'un document, peuvent ainsi être identifiés. Une application commerciale de ce type a été déployée par la société DiVX. L'une des mesures de sécurité mises en œuvre dans le matériel DiVX est d'insérer une marque qui pourrait être utilisé pour identifier une tentative de piratage. Si des copies illégales d'un film DiVX apparaissent sur le marché noir, DiVX pourrait utiliser les marque pour tracer jusqu'à la source.

I.4 Classification des systèmes du tatouage numérique :

Les systèmes du tatouage numérique sont classifiés selon plusieurs critères **[Figure I.4]**.

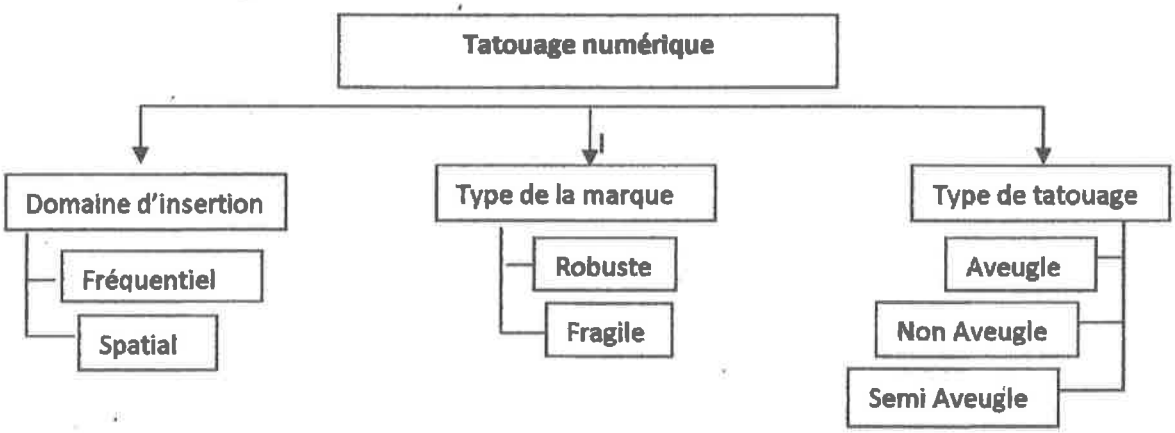


Figure I.4 : Schéma de classification du tatouage numérique.

Ces critères sont :

I.4.1 Domaine d'insertion :

L'insertion d'une marque peut être effectuée dans deux domaines différents, qui sont :

- **Domaine spatial** : les méthodes qui viennent en premier à l'esprit sont celle du domaine spatial, où elles modifient et agissent directement sur la luminance des pixels. Comme aucun traitement initial n'est requis, ses algorithmes sont très rapides et permettent de travailler en temps réel [8].
- **Domaine fréquentiel** : le domaine transformé ou domaine fréquentiel est obtenu du domaine spatial en appliquant une transformée en une ou deux dimensions. La transformée peut se réaliser sur toute la donnée ou sur des blocs obtenus par une subdivision de celle-ci [8]. Les transformées les plus utilisées dans le domaine du tatouage numérique sont : Transformée en Cosinus Discrète (TCD). Transformé de Fourrier discrète (TFD) et Transformée en ondelette Discrète (TOD). L'avantage principal de ce domaine par rapport au domaine spatial est que l'insertion de la marque se fait dans les coefficients de la transformée, ainsi, elle assure la propagation des modifications introduites sur un sous ensemble de ces coefficients, à tous les pixels dans le domaine spatial ; ce qui rend cette insertion imperceptible [9].

I.4.2 Type de la marque insérée :

- **Robuste :** la robustesse est mesuré à la résistance de la marque inséré face aux attaques contre la donnée tatoué [10], si celle-ci résiste et subsiste à ces attaque alors le tatouage est robuste. Ce type de tatouage a pour objectif de transmettre des informations même si un fraudeur modifie la donnée ou tente de l'altérer.

- **Fragile :** ce type de tatouage est très sensible aux modifications et aux traitements. Il est particulièrement utilisé pour vérifier l'intégrité du document marqué. Néanmoins, il serait intéressant de mentionner que certains systèmes de tatouage fragile sont tout de même résistant aux traitements les plus usuels, notamment la compression, ce type particulier est dit *semi-fragile* [10].

I.4.3 Type du tatouage :

Les techniques du tatouage peuvent être classées suivant les éléments nécessaires pour l'extraction de la marque [12], à savoir la présence/absence de la donnée originale pour effectuer l'extraction. On distingue trois cas, qui sont :

- **Tatouage aveugle** : pour ce cas, la donnée originale n'est pas nécessaire pour extraire la marque insérée. C'est le cas le plus favorable pour des applications pratiques.
- **Tatouage non aveugle** : pour ce cas, le processus d'extraction nécessite la donnée originale pour pouvoir lire correctement la marque insérée.
- **Tatouage semi-aveugle** : ce type de cas n'utilise pas la donnée originale mais il se base sur quelques caractéristiques dérivées de cette dernière. Ce type est de moins en moins étudié.

I.5 Attaque sur des systèmes de tatouage numérique :

On peut distinguer deux types d'attaques :

- **Attaques volontaire** : Ces attaques ont pour but de rendre la marque inefficace ; et cela par l'affaiblissement de ses caractéristiques. Telle que la robustesse et la sécurité. Ces attaques peuvent être de différentes natures, notamment : attaque géométrique, attaque par bruitage, attaque par filtrage.
- **Attaque involontaire** : Ces attaques sont des traitements effectuées sur l'image, dans la plus part du temps elles sont inévitables. Elles n'ont pour objectif ni d'enlever la marque insérée ni de la modifier. Ces attaques se produisent par opération de compression, scan, impression.

I.6 Conclusion

Dans ce chapitre, un aperçu global sur le tatouage numérique a été donné, en expliquant ses principaux concepts, ses différentes propriétés et ses critères de classification. Puis, on a vu l'apport du tatouage numérique comme solution au problème de sécurisation des systèmes d'identité à base d'empreinte digitale et les contraintes aux quelles il sera opposé. On s'est focalisé sur les images d'empreinte digitale mais ceci ne nie pas l'existence de technique adopté à d'autres types de documents multimédias (texte, son, vidéo...), la

référence [X] contenant diverse lien sur le tatouage numérique, montre bien que ce domaine est très riche en termes de publications. Le tableau 1 illustre cette idée vu la duplication du nombre de publications d'une année à une autre.

Année	1992	1993	1994	1995	1996	1997	1998
Nombre de productions	2	2	4	13	29	64	103

Tableau I.1 : Nombre de publication sur le tatouage numérique.

Chapitre II

Méthode de protection de l'information par tatouage numérique.

II.1 Introduction :

Les systèmes d'identification à base d'empreintes digitales gèrent des milliers de fichiers d'images dont chaque image correspond à une seule personne. Le seul lien entre une personne et son empreinte est le nom du fichier de celles-ci. Ce dernier est généré automatiquement du système AFIS, il correspond à l'identifiant de l'individu. Si celui-ci est modifié, d'une façon volontaire ou involontaire, le système ne pourra pas faire le lien entre la personne et son empreinte.

Une solution possible est d'utiliser les techniques du tatouage numérique pour insérer cet identifiant comme étant la marque, ce qui nous permettra de le restituer en cas de perte ou de modification de l'identifiant.

Dans ce chapitre nous présentons, la technique de tatouage numérique basée sur le contenu en s'inspirant de la méthode de N. Ratha [01], qui se trouve être la seule adaptée aux images d'empreintes digitales.

II.2 Conception du Système de tatouage numérique basée sur le contenu

Comme vu dans le chapitre précédent, le tatouage numérique propose deux types d'approche d'insertion, dans le domaine Spatial, et dans le domaine fréquentiel, Ratha a décrit deux approches dédiées pour chaque domaine [01]. Dans ce travail, nous nous sommes focalisés sur l'approche d'insertion dans le domaine spatial pour apporter une solution à notre problème.

La méthode comprend deux étapes essentielles : l'insertion (figure II.1) et l'extraction de la marque (figure II.2)

II.2.1 Processus d'insertion :

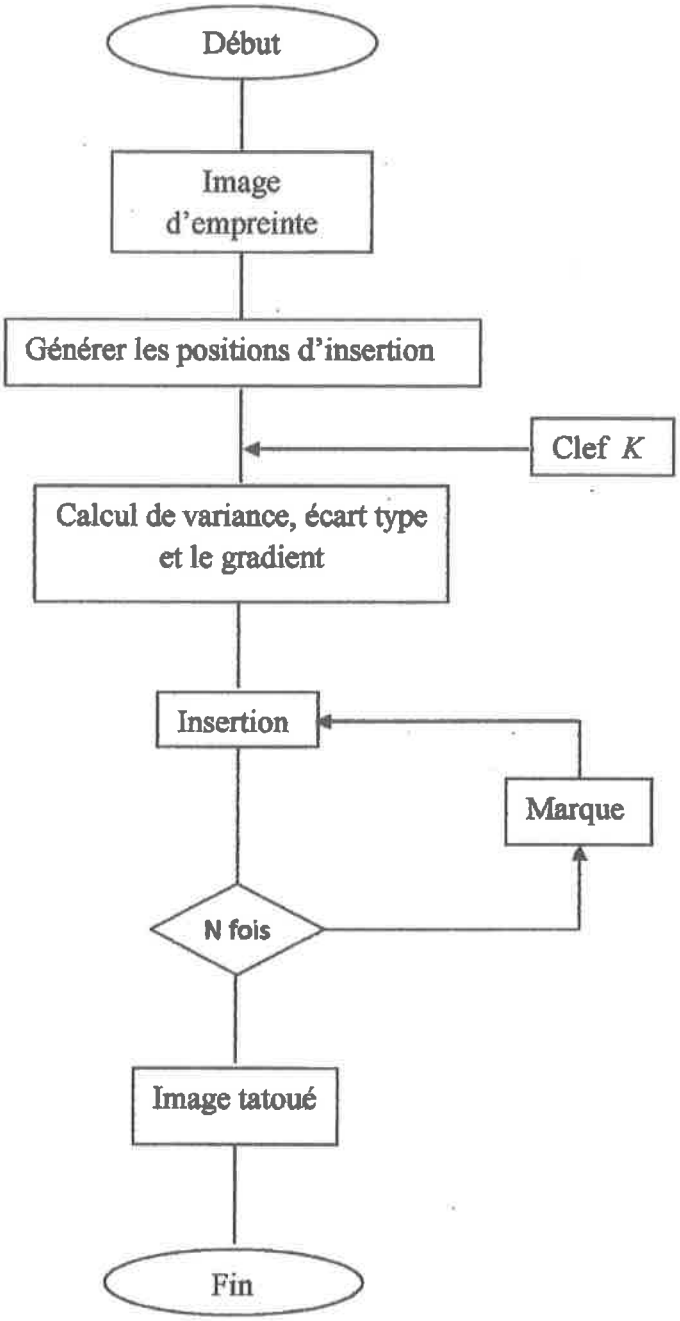


Figure II.1 : Processus d'insertion

L'insertion est effectuée dans les zones texturées selon une clef *K*. Pour ce faire, l'image en entrée est subdivisée en blocs de taille 3x3. Pour chaque bloc, un calcul de la moyenne *PAV (i, j)* ainsi que la déviation standard *PSD (i, j)* est fait selon les formules ci-dessous :

$$PAV(i,j) = Moy\left(bloc(i,j)\right) \quad \text{(II.1)}$$

$$Moy\left(bloc(i,j)\right) = \frac{\sum_{i-1;j-1}^{i+1;j+1} pixel(i,j)}{9} \quad \text{(II.2)}$$

$$PSD\ (i,j)^2 = Moy\left(\ bloc\ (i,j)\right)^2 - \ moy\ (bloc\ (i,j)) \quad \text{(II.3)}$$

Afin de déterminer les régions texturées et calculer le gradient *PGM (i, j)* on utilise le filtre de Sobel [15] pour la taille du bloc 5x5 selon les orientations horizontales et verticales respectivement.

$$PGM\ (i,j) = \sqrt{SobelH(i,j)^2 + SobelV(i,j)^2} \quad \text{(II.4)}$$

L'insertion des de la marque consiste à changer la valeur du pixel *P(i, j)* selon la formule :

$$P_{WM}\ (i,j) = P\ (i,j) + \quad (2S-1)PAV(i,j)Q *$$

$$\left[\left[1 + \frac{PSD(i,j)}{A}\right] * \left[\left[1 + \frac{PGM(i,j)}{B}\right]\right] * \beta(i,j)\right] \quad \text{(II.5)}$$

où les paramètres **A, B et Q** sont des constantes qui constituent la force de marquage.

β(i, j) est la position de minutie qui représente la caractéristique de l'individu. Elle est égale à 0 si la minutie est à cette position sinon, elle est égale à 1 ;
S : représente les bits de la marque en cours d'insertion et *Pwm(i, j)* représente la valeur du niveau de gris du pixel tatoué.

L'opération d'insertion est effectuée *N* fois pour chaque bit de la marque d'une manière pseudo aléatoire selon la clef *K*.

La clef K est utilisée pour générer deux séquences pseudo aléatoires, l'une pour désigner la position d'insertion le long des lignes et l'autre le long des colonnes.[01]

II.2.2 Processus d'extraction :

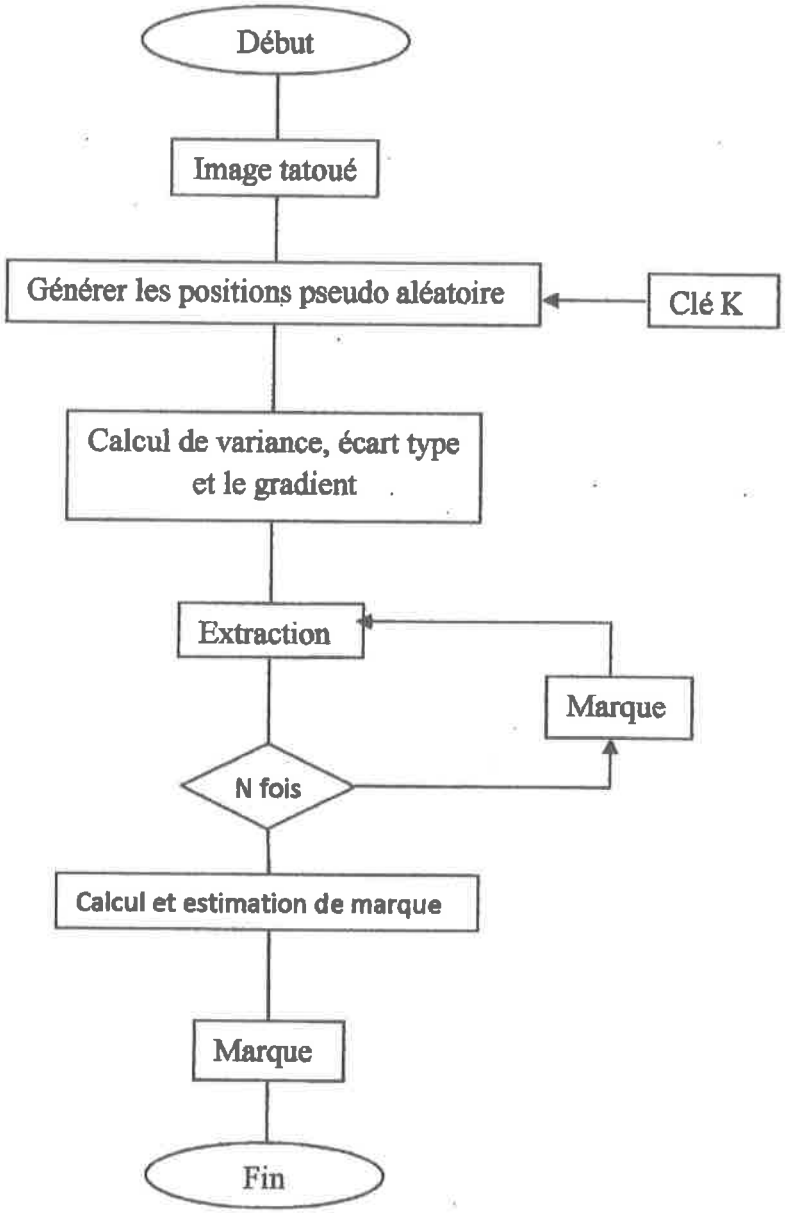


Figure II.2 : Processus d'extraction.

Le processus d'extraction est de type aveugle, il n'a pas besoin de l'image d'origine pour extraire la marque. Le principe suit les mêmes étapes que celles de l'insertion. C'est-à-dire calcul de la moyenne *PAV (i, j)*, la déviation standard *PSD (i, j)* et le gradient *PGM (i, j)* pour déterminer les régions texturées dans l'image tatouée [01]. L'opération d'extraction de la

marque est simple, il suffit de calculer une approximation $\acute{P}(i,j)$ de la valeur du niveau de gris d'origine dans un bloc. Celle-ci est donnée par :

$$\acute{P}(i,j) = \frac{1}{8}\left(\sum_{k=-2}^{2} P_{WM}(i+k,j) + \sum_{k=-2}^{2} P_{WM}(i,j+k) - 2P_{WM}(i,j)\right) \quad \text{(II.3)}$$

Avec δ la différence entre la valeur approximée du pixel et celle du pixel taboué :

$$\delta = \acute{P}(i,j) - P_{WM}(i,j) \quad \text{(II.4)}$$

Puisque l'insertion du même bit est effectuée N fois une moyenne de cette différence $\bar{\delta}$ est calculée pour chaque position d'insertion, ainsi, on estime les bits $\acute{S}$ de la marque extraite en utilisant la formule suivante :

$$\acute{S} = \begin{cases} 1 \text{ si } \bar{\delta} > \frac{\bar{\delta}_{R0} + \bar{\delta}_{R1}}{2} \\ 0 \text{ si non} \end{cases} \quad \text{(II.5)}$$

Où $\bar{\delta}_{R0}$ est la moyenne des bits de valeur 0 et $\bar{\delta}_{R1}$ la moyenne des bits de valeur 1 extraits.

- **Type de la marque :**

  La marque utilisée est suite de chaine de caractères alpha numérique, une conversion de celle-ci en binaire est appliquée **(Figure II.3).**

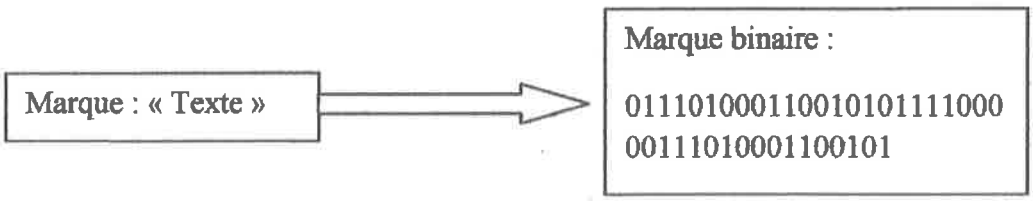


Figure II.3 Conversion de la marque en binaire

II.3 Inconvénients de la méthode :

La méthode de Ratha est de type fragile. Le changement d'un bit de marque extraite détruit la marque insérée. Donc le système AFIS ne pourra jamais identifier la personne correspondante à la marque d'origine. Pour remédier à cet inconvénient, nous avons proposé de convertir la marque du format alpha numérique au format image monochrome de type BMP. Ceci engendre l'augmentation de la capacité d'insertion.

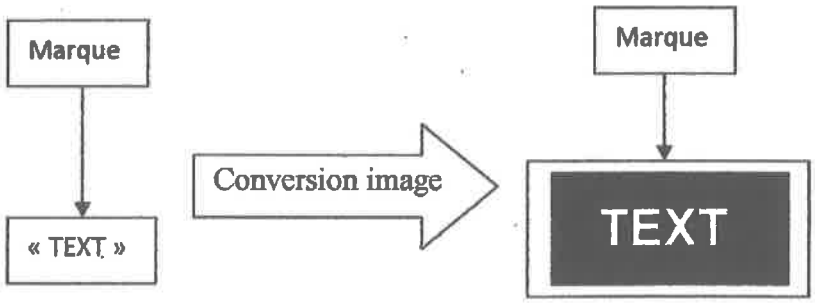


Figure II.4 Conversion de la marque en Image.

Le nom de fichier de l'empreinte digitale délivré par le système AFIS est généralement sous la forme suivante :

$$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}x_{16}yzt$$

avec :

$$x_i \in \{0,1,2,3,4,5,6,7,8,9\}, \qquad i = 1,2,\dots,16$$
$$y \in \{\_\}$$
$$z \in \{P,4,2\}$$
$$t \in \{G,D,1,2,3,4,5,6,7,8,9\}$$

Celle-ci est convertie en image BMP **(Figure II.5)**

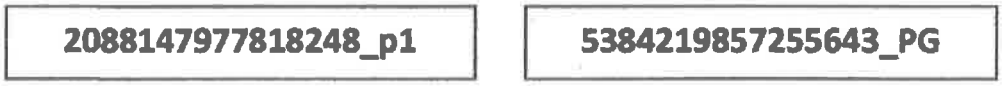


Figure II.5 Exemples de marque dans le Système AFIS

II.4 Tests et analyse des résultats

Dans ce paraphe, nous présentons les performances de la méthode développée et son évaluation aux critères de tatouage numérique tels que l'invisibilité, la capacité d'insertion et la robustesse face à certain nombre d'attaques tels que le Croping (Effacement d'une partie de l'image), le changement de luminosité, la compression WSQ (Wavelet Scalaire Quantization).

La taille des images d'empreintes digitales utilisées dans l'implémentation de notre application est de (740 x 580) pixels alors que la marque est de taille (14x137) pixels ce qui correspond à 1918 bits au lieu de 152 bits (marque en chaine de caractère).

Les paramètres qui constituent la force du marquage **A, B et Q** sont paramétrées à

A=100, B=1000 et Q= 0.1.

II.4.1 Analyse de l'imperceptibilité :

La métrique classique utilisée pour comparer deux images est le Peak-Signal-to-Noise (PSNR) [28], qui tente de déterminer le niveau de distorsion d'une image par rapport à sa source. A fin de mesurer la similitude entre l'image d'origine et celle tatouée, le PSNR est utilisé et se définit comme suit :

$$PSNR = 10\ log_{10}\left(\frac{255^2}{\sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}[I(i,j)-I'(i,j)]^2}{N*M}}}\right) \qquad \text{(II.5)}$$

où : I et I' représente respectivement, l'image D'origine et l'image tatoué, N x M est la taille de l'image.

Le tableau II.1 représente les résultats obtenus pour l'analyse d'imperceptibilité.

Tableau II.1 Résultat d'imperceptibilité

Image d'origine	Marque insérée	Image tatouée	PSNR (dB)

		51.54
		49.12

D'après les résultats obtenus, nous observons que la moyenne du PSNR est très satisfaisante [15] ceci indique que la marque est invisible.

II.4.2 Tests de Robustesse :

Après insertion de la marque, l'image tatouée est soumise à différente attaques à fin d'évaluer la robustesse de la méthode.

Cette robustesse sera estimer selon le taux de bits erroné (EBR : Bit-Error-Rate) ainsi que la Corrélation normalisé (NC) entre la marque inséré et celle extraite [15], et qui se définies par les équations suivantes:

$$EBR = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}(w[i,j]\ XOR\ w'[i,j])}{N*M} \qquad (II.6)$$

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M}W(i,j)W'(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{M}[W(i,j)^2]} \qquad (II.7)$$

où: w et w' représentent respectivement la marque insérée et la marque extraite de taille $(N*M)$.

Le tableau II.2 ci dessous représente les résultats de robustesse face aux attaques citées précédemment :

Tableau II.2 résultat d'extraction après les attaques.

Attaque	Image tatouée attaquée	Marque extraite	NC	EBR (%)
Effacement			0.92	1.5
			0.98	0.78
			0.92	5.26

compression WSQ			0.02	70.07
compression JPEG			0.09	83.56
Contraste (-5)			0.82	11.99
Contraste (-10)			0.85	10.11
Luminance (-10)			0.85	96.45

Tandis que les résultats obtenus face aux attaques de l'effacement partiel de l'image tatouée obtenus dans le tableau II.2, montrent une grande robustesse de la méthode, et que ceux de la

modification du contraste et de la luminance restent convenables au niveau visuel. La destruction de la marque face à la compression démontre clairement que la méthode utilisée n'est pas robuste.

II.5 Conclusion :

Dans ce chapitre, la méthode de Ratha a apporté une solution pour la problématique décrite. Aussi, la modification apportée à cette méthode de tatouage numérique s'est conclu par plus de robustesse par rapport à la marque. En effet, l'effacement partiel de l'image tatoué et les changements de luminance ou de contraste n'affectent en rien celle-ci, par contre elle reste fragile face aux traitements les plus rudes comme la compression WSQ ou JPEG.

CHAPITRE III

Méthode d'authentification du contenu de l'empreinte par Hachage Perceptuel

III.3.1 : Le Module d'extraction

On applique ici le procédé de l'algorithme de hachage perceptuel qui se résume par :

1) Prétraitements :
   - Application linaire d'un filtre passe-haut sur l'image acquise [19].
   - Diviser le filtre en N bloc chevauché.
   - Calculer les valeurs absolues de chaque coefficient de chaque bloc.

2) Extraction de signature :
   - Utiliser le model de la distribution de Weibull pour extraire les paramètres du vecteur caractéristique contenant les coefficients des blocs.
   - Génération d'une signature virtuel en utilisant une clé de chiffrement k, et dériver a partir de celle-ci N-1 autres signatures en utilisant une clé k'.
   - Application du processus d'extraction.

- **Prétraitement des images d'empreintes digitales :**

En premier lieu un filtre passe-haut linéaire simple de taille 3X3 est appliqué horizontalement et verticalement sur l'image ED [18] pour la détection de contour en utilisant le procédé suivant ;

Soit I l'image d'entrée et I_v et I_h les versions filtrées verticalement et horizontalement de I

On dénote $J_{(i,j)}$ la valeur du pixel de l'image I après le traitement ;

$$J_{(i,j)} = max\{abs(I_h(i,j)), abs(I_v(i,j))\} \qquad \text{(III.1)}$$

où $$I_h = \begin{bmatrix} -1 & 0 & +1 \\ -1 & 0 & +1 \\ -1 & 0 & +1 \end{bmatrix} * J_{(i,j)} \quad \text{and} \quad I_v = \begin{bmatrix} +1 & +1 & +1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{bmatrix} * J_{(i,j)} \qquad \text{(III.2)}$$

Des blocs de tailles N prédéfinies **[Figure III.3]** **[Figure III.4]** qui se chevauchent sont formés afin d'extraire le vecteur caractérisant de l'image d'entrée [19], on calcule la moyenne absolu de chaque bloc et on extrait les coefficients du vecteur.

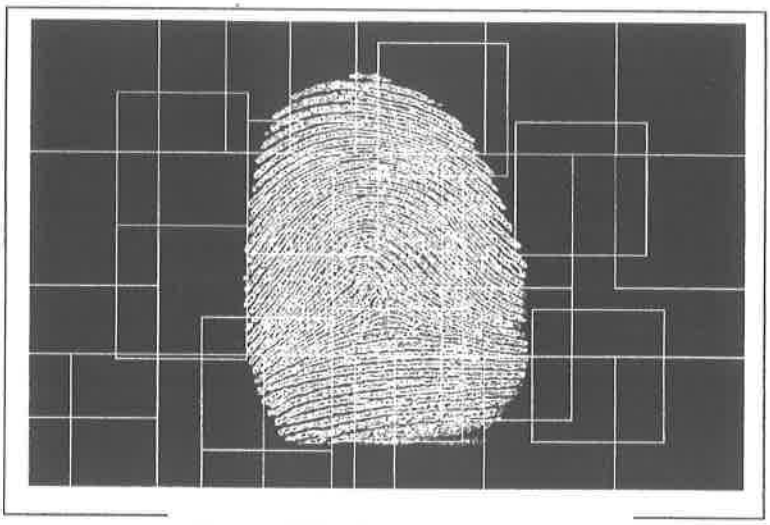


Figure III.3 Bloc Chevauchant

Figure III.4 Bloc Non Chevauchant

On extrait le vecteur *Vec* caractérisant l'image d'empreintes digitales en calculant la moyenne des coefficients de chaque bloc. Ce calcul se fait à l'aide de la formule suivante :

$$Vec[k] = Moy\ \frac{(\Sigma_0^N J_{(i,j)})}{N} \qquad \text{(III.3)}$$

- **Extraction de signature :**

Étant donné que les coefficients du vecteur caractéristique sont des nombres positifs, nous utiliseront la distribution de Weibull [18] afin de modéliser leurs comportements statiques. Ce modèle de distribution offre une bonne souplesse pour décrire les caractéristiques statistiques de la grandeur des coefficients.

$$f(x) = \frac{\beta}{\alpha}\left(\frac{x}{\alpha}\right)^{\beta-1} \exp\left[-\left(\frac{x}{\alpha}\right)^{\beta}\right] \qquad \text{(III.4)}$$

Où β est le paramètre de forme et α est le paramètre d'échelle de la distribution

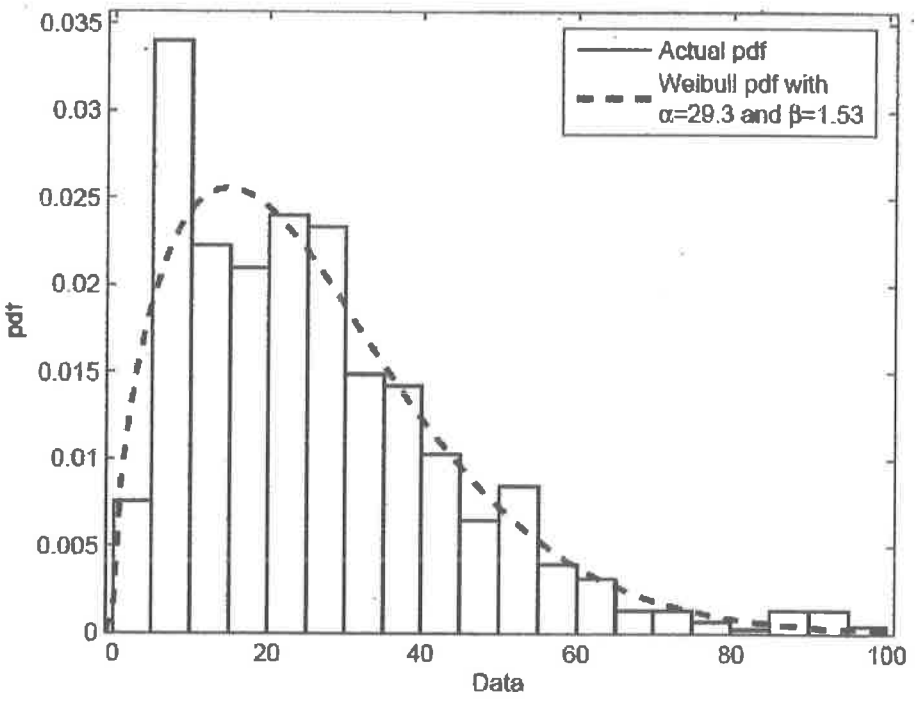


Figure III.5 Model de la distribution de données suivant la loi Weibull

A l'aide d'une clé k, une séquence pseudo aléatoire de taille N est générée, celle-ci est uniformément repartie dans l'intervalle [-1,1] et sera utilisé comme signature virtuelle. Afin d'obtenir N hash bits il nous faudrait N signature [18], une clé k' est utiliser pour

générer une séquence d'entier entre 1 et N pour produire d'autres signatures en décalant sur la première comme une permutation pseudo-aléatoire.

Chaque signature sera utilisée dans les calculs avec un des blocs pour extraire un des bits de la signature finale suivant les formules ci-dessous :

$$T^{(i)} = \sum_{j=1}^{N} \left(\frac{\left(1+\lambda W_j^{(i)}\right)^{\beta} - 1}{\left(1+\lambda W_j^{(i)}\right)^{\beta}} \right) \quad \text{(III.5)}$$

et

$$\emptyset^{(i)} = \sum_{j=1}^{N} y_j^{\beta} \left(\frac{\left(1+\lambda W_j^{(i)}\right)^{\beta} - 1}{\alpha^{\beta}\left(1+\lambda W_j^{(i)}\right)^{\beta}} \right) \quad \text{(III.6)}$$

où : $W_.^i$ dénote la i iéme signatures virtuelle: $0 < i < N$.

λ une constante désignant le facteur de similarité.

Y_l sont les valeurs du vecteur caractéristique

Le bit h^i de la signature prend la valeur suivant le conditionnement :

$$\begin{aligned} \emptyset^{(i)} \geq T^{(i)} &\Rightarrow h^{(i)} = 1 \\ \emptyset^{(i)} < T^{(i)} &\Rightarrow h^{(i)} = 0 \end{aligned} \quad \text{(III.7)}$$

III.3.2 Le module de comparaison :

Afin de déterminer la similitude de la signature obtenue, on calcule la distance de Hamming [17] avec (III.8,) entre l'empreint acquise et celle stocké dans la BD stockées dans la BD. Si la distance est inferieure au seuil d'acceptation prédéfini alors l'individu est authentifié, et si celle-ci est au delà du seuil, cela pourrait se traduire par une fraude.

$$D(a,b) = \sum_{i=0}^{n-1} (a_i \oplus b_i) \quad \text{(III.8)}$$

Dans la **[Figure III.4]** un résumée des différentes étapes de cette algorithme est décrit :

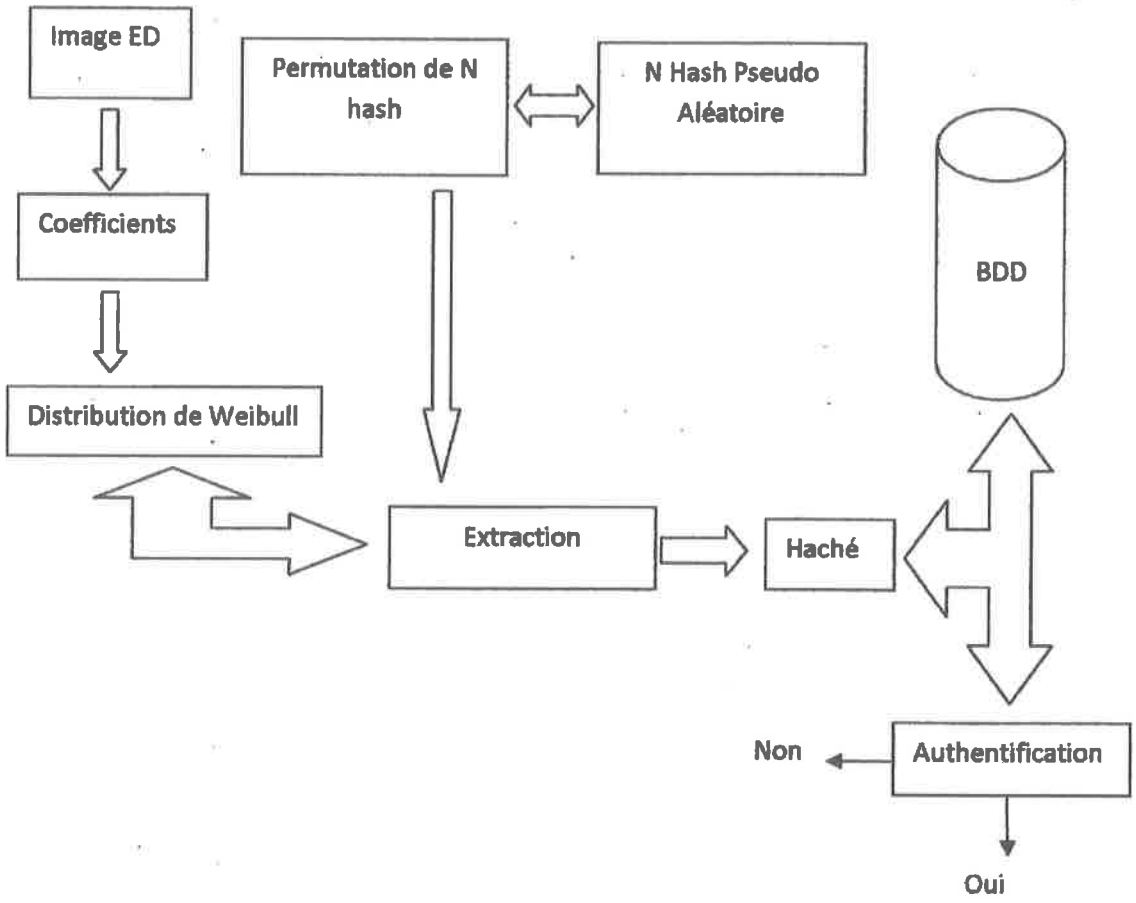


Figure III.6 Schéma résument l'authentification de l'empreinte en utilisant le hachage perceptuel

III.4 Tests et analyse

Le tableau III.1 représente les résultats de la méthode face à l'effacement de l'image d'empreinte

Image acquise	Image Stockée	Distance de Hamming
		6
		8
		+15

Les résultats obtenu montrent bien qu'un léger effacement de l'image peut être tolérer mais cela est relativement proportionnelle a la taille de l'effacement, c.-à-d. que si le taux d'effacement de l'image est grand, la distance sera grande entre les signatures obtenu, et si l'effacement couvre qu'une petite partiel de l'image, la distance sera assez petite pour authentifier l'individu. La distance dépassant les 10 implique un rejet de l'authentification.

Le tableau III.2 représente les résultats de la méthode face aux changements de luminance

	Image acquise	Image Stockée	Distance de Hamming
+20			3
+50			9

- Les résultats obtenus face aux changements de luminance sont très concluantes, la distance entre les signatures générées reste très convenable. Ainsi l'authentification de l'individu est validée par le système.

III.5 Conclusion:

Dans ce chapitre, une nouvelle technique basée sur le hachage perceptuel a été proposé pour la protection de l'intégrité de l'information, le concept est de générer N signatures dérivées afin d'avoir une similitude entre la signature calculée et celle stockée dans la BD, ceci en contrôlant la distribution de valeur au niveau de la forme binaire de la signature.

Les tests d'attaques, comme l'effacement partiel sont assez concluants. Mais une perte considérable de la donnée d'origine paralyse le système et l'authentification est rejetée. Pour ce qui du changement de luminance, celle-ci à donner de meilleurs résultats validant ainsi l'authentification de l'individu.

CONCLUSION GENERALE

CONCLUSION GENERALE :

Ce projet vise la protection de l'information de l'individu au niveau du système AFIS face à la tentative de modification de l'information et face aux tentatives d'usurpation d'identité, pour ce faire nous avons pris le choix de traiter séparément les deux problématiques en se fixant deux contraintes à respecter.

La première était d'utiliser une méthode de tatouage numérique sur les empreintes digitales basée sur le contenu pour la protection de l'information, Après une étude bibliographique des techniques de tatouage existantes. La méthode de Ratha fut la seule développée pour les images d'empreintes digitales, celle-ci avait comme inconvénient la fragilité de la marque insérée face aux attaques les plus répandues.

En proposant la conversion de la marque en format d'image, on a rendu celle-ci plus robuste face aux attaque de base, mais restait quand même fragile face a la compression WSQ ou JPEG.

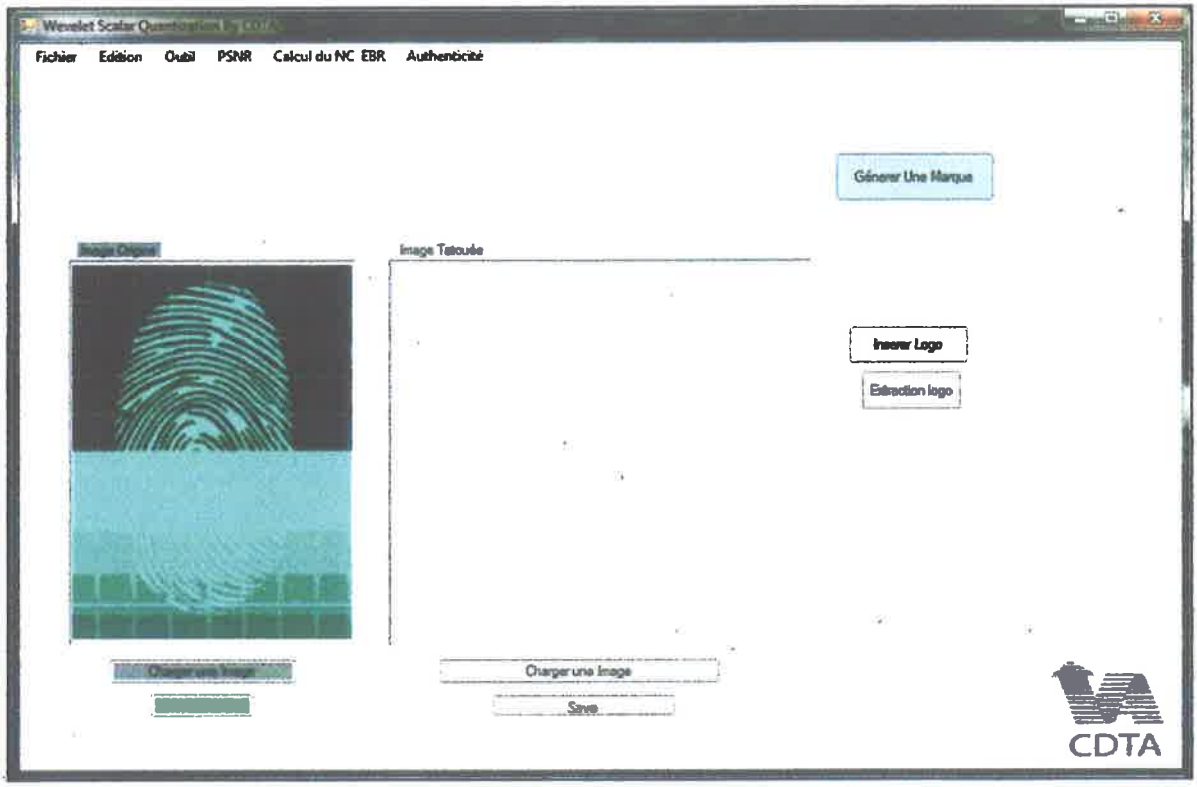
Une autre méthode développé en parallèle par **H.Hadjer & Bencouche Iméne** toujours dirigé par Mme **AIT SAADI KARIMA** intitulée : **Protection des images d'empreintes digitales par technique de tatouage numérique utilisant l'opérateur LBP,** a donné de meilleurs résultats face aux attaques utilisées, mais restait toujours fragile face à la compression WSQ.

En termes de perspectives de ce travail, nous proposons l'amélioration de la méthode de Ratha en utilisant un code correcteur d'erreurs sur la marque extraite. Rendant celle-ci plus robuste face à la compression.

Pour ce qui est de l'authenticité et l'intégrité de l'information par protection du contenu de l'empreinte en utilisant le hachage perceptuel, de bons résultats ont été obtenus, cependant les recherches dans ce domaine sont toujours d'actualité afin de perfectionner la méthode.

Aussi, plus de sécurité au niveau de la base de données pourrais amoindrir les risques d'attaques offrant ainsi plus de fiabilité au système.

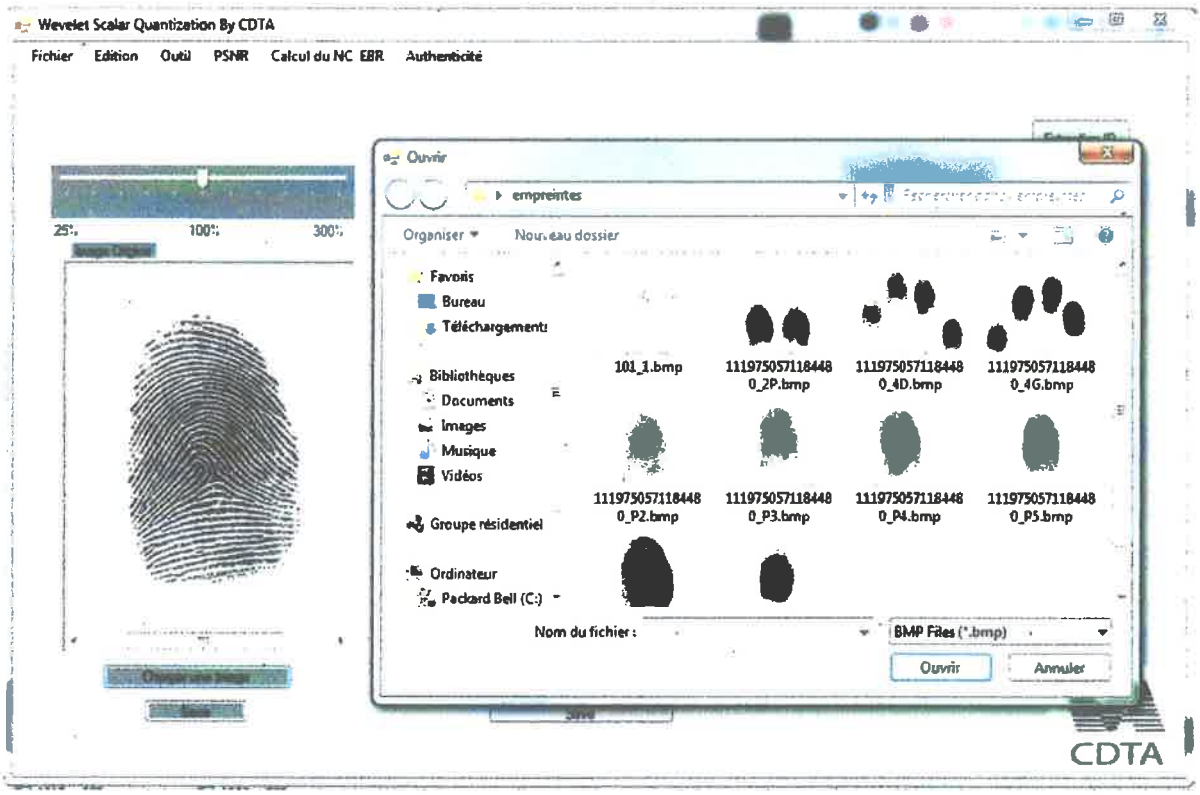
INTERFACE ET APLICATIONS



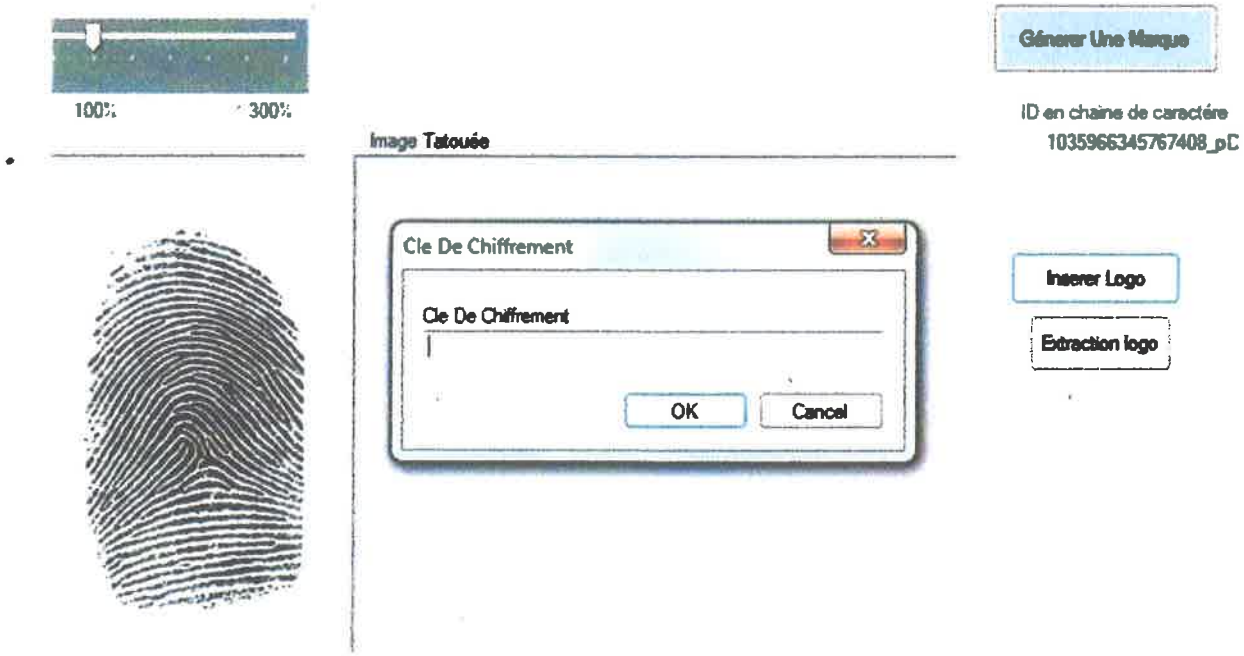
Interface V1.0 de l'application

L'application conçue est toujours en vois de développement, celle-ci offre une interface simple et visible, les différentes fonctionnalités qu'offre l'application sont :

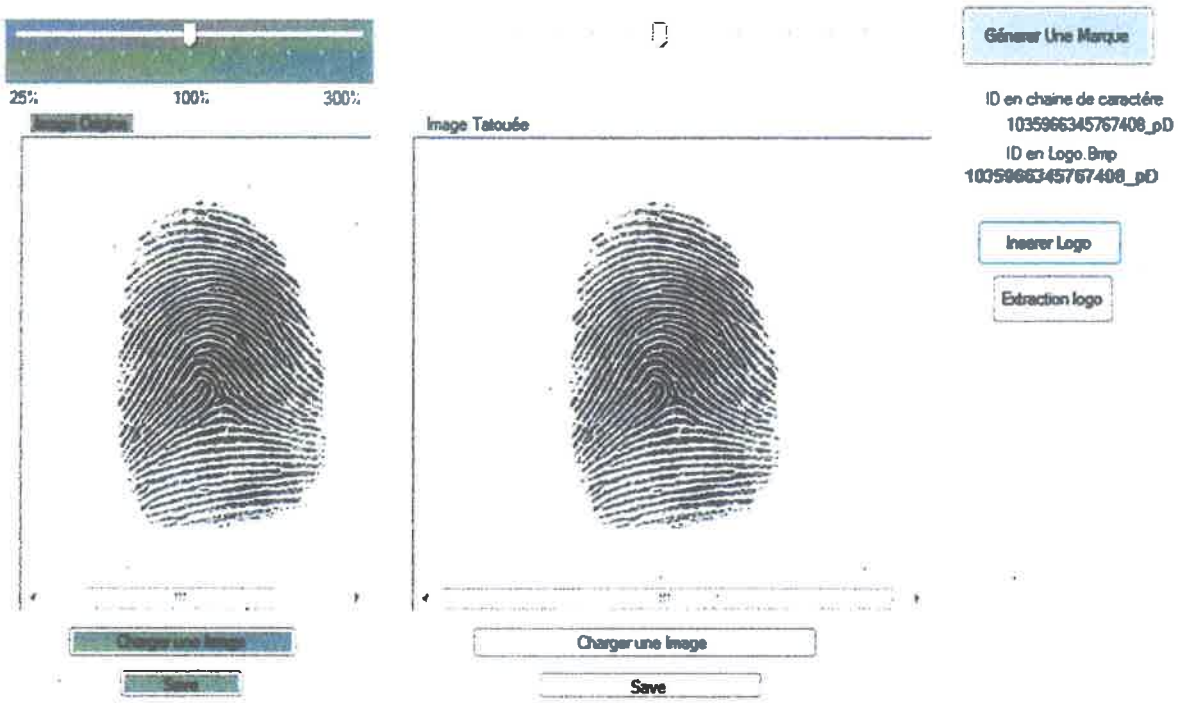
- Chargement d'images d'empreintes digitales
- Génération de matricule de l'empreinte.
- Conversion de la marque en BMP
- Insertion de la marque via clé de chiffrement
- Extraction de la marque
- Test d'imperceptibilité
- Calcul du taux de bits ratio et celui de la corrélation normalisé.
- Sauvegarde d'empreinte.
- Envoie d'empreinte via le réseau (utilisant les sockets)
- Divers attaque sur la marque sont proposer pour les tests.
- Authentification d'empreinte basée sur le hachage perceptuel.



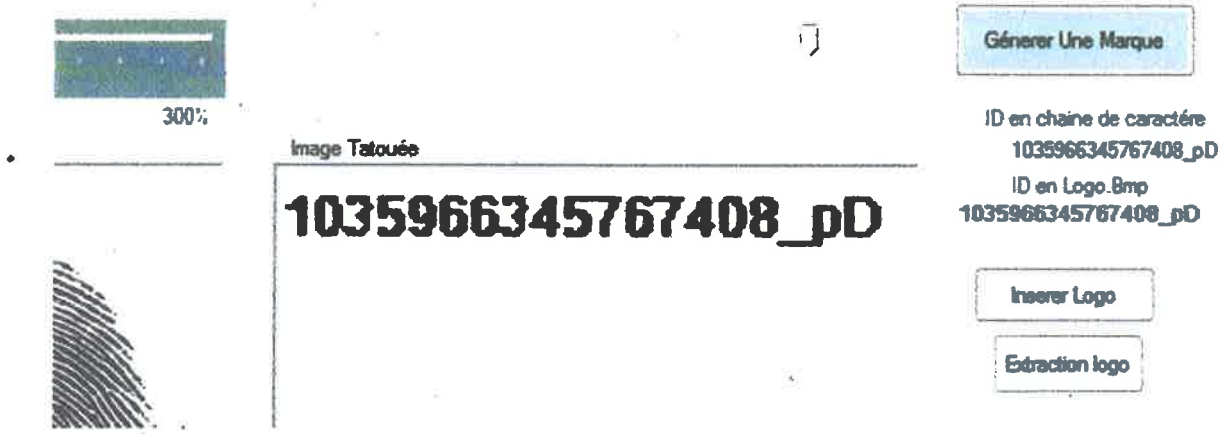
Chargement d'image d'empreinte



Demande de clé de chiffrement pour l'insertion



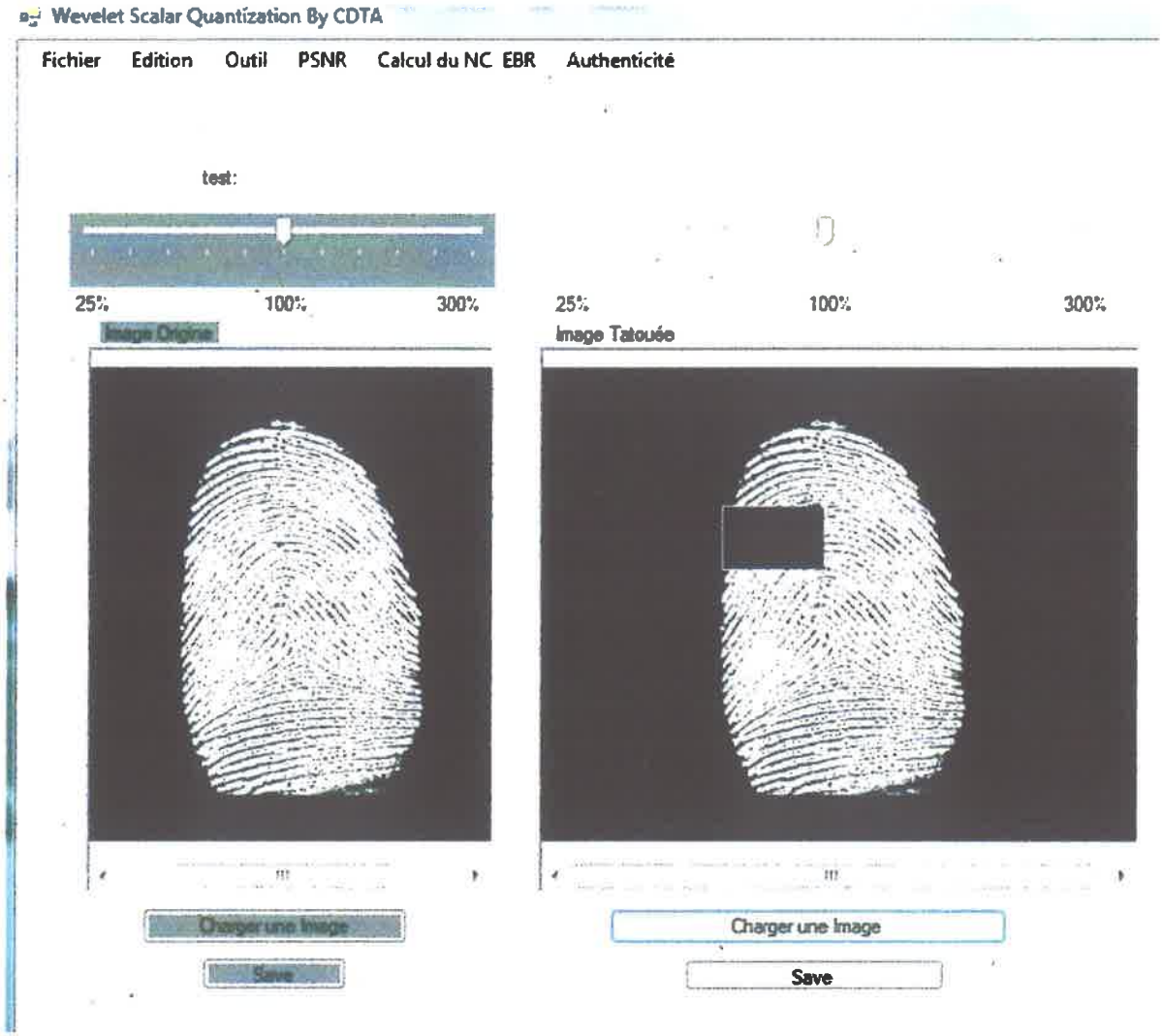
Similitude visuel de l'image tatoué (à droite)



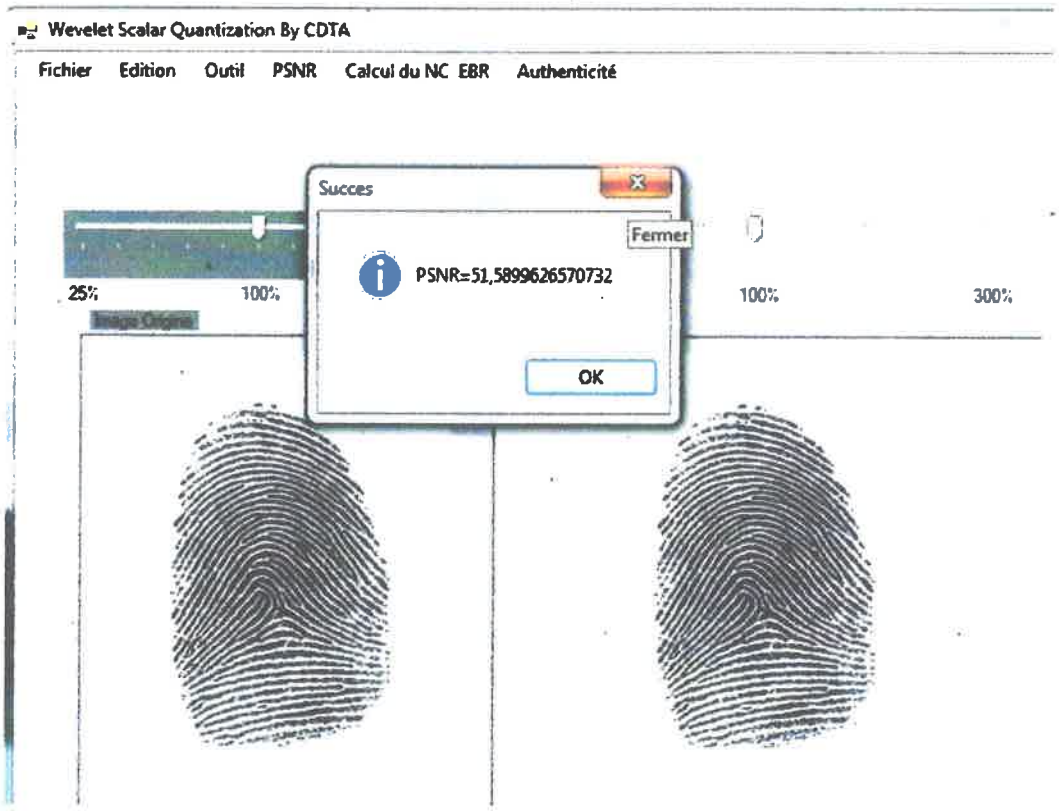
Extraction de la marque (sans attaque)

9663194524261490..29

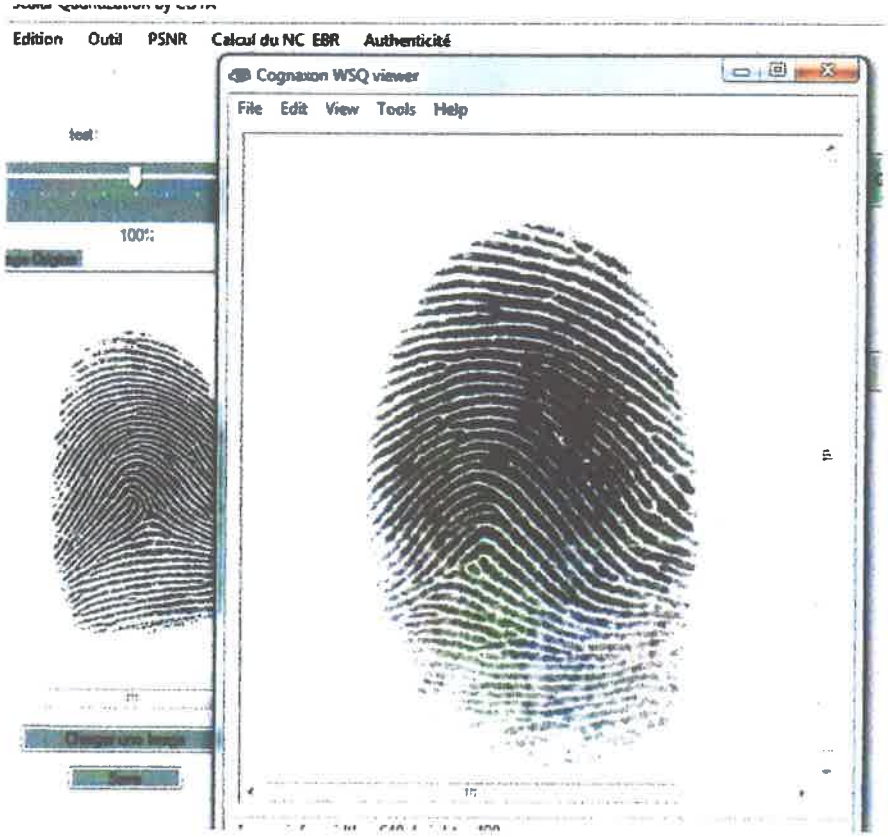
Extraction de marque avec (attaque)



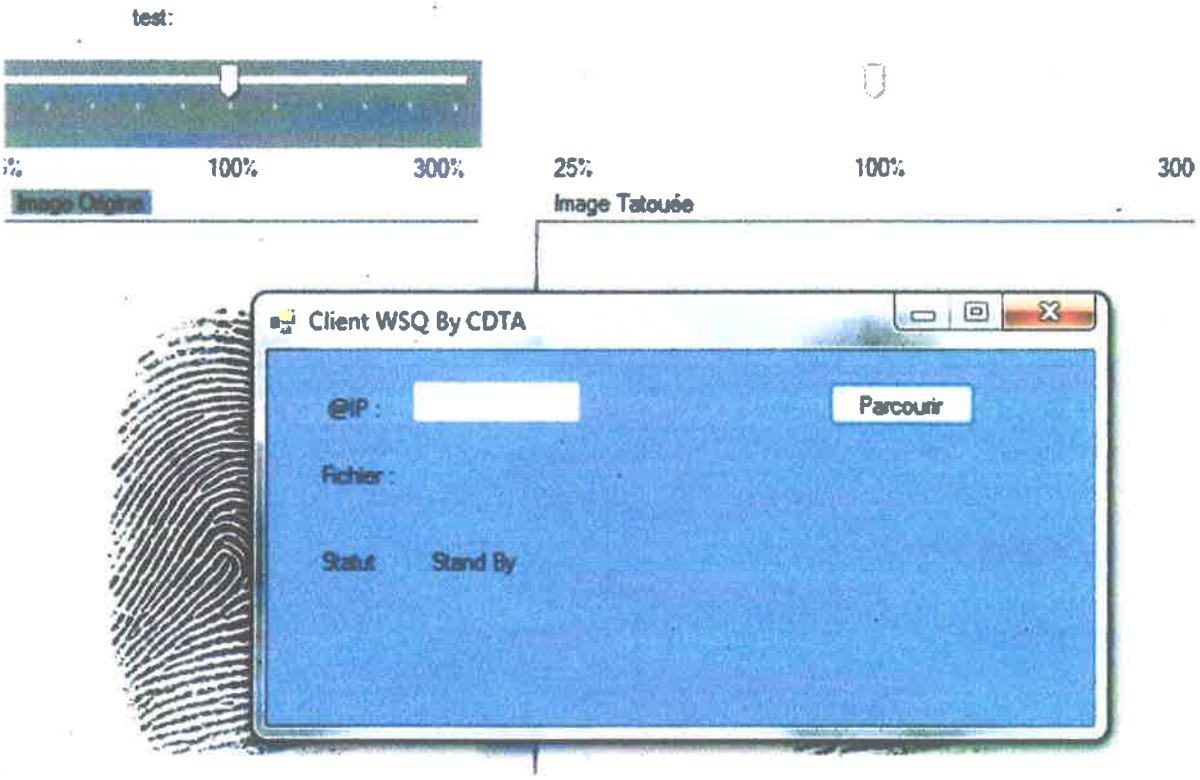
Filtre Prewit sur l'image d'empreinte



Calcul du PSNR pour l'impeccabilité de la marque insérée



Outil de conversion WSQ/JPEG



Envoie de données par réseau utilisant les sockets.

Le développement de cette nous a permet d'acquérir certaines connaissances :

- traitement d'images.
- les filtres servant à détecter les contours,
- les nombres pseudo aléatoires.
- la distribution de la loi de Weibull
- le transfert de données via sockets.
- Conversion format image BMP.
- Les fonctions de hachage.
- Interfaçage

Etc....

Résumé :

L'objectif de ce mémoire est d'appliquer les techniques du tatouage numérique sur les empreintes digitales pour la protection et l'intégrité de l'information de l'individu et renforcer la sécurité des systèmes automatiques d'identification par empreintes digitales. Ces technique consiste à cacher l'information de l'individu dans l'image de ses empreinte, pour y parvenir nous avons implémenté le module d'insertion et celui de l'extraction de la marque à l'aide du langage C#, et en s'appuyant sur la méthode développer par Ratha.

Aussi, nous avons réalisé un système d'authentification d'empreintes digitales en utilisant le concept du hachage perceptuel, un hachage plus tolérant au niveau des bits qui changent dans l'image d'entrée. Une signature plus similaire et plus proche en termes de distance par rapport à celle stocké dans la BD résulte de ce système.

Abstract:

The aim of this project is to apply the techniques of numerical tattooing on the digital image fingerprint to give protection and integrity of personal information of a person. And to boost the security of the Automatic Fingerprint Identification Systems, This technique consists in hiding secret information (name of the images) in the image from its fingerprints. To realize this, we have used Ratha's method based on fingerprint content in order to implement the insertion mechanism and the extraction one with the help of C# language.

Also, we realized an authentication fingerprint system using the concept of perceptual image hashing, this type of hash function give a similar signature, and closer to the one stocked in the data base, in term of Hamming distance.