Vérification de l'intégrité de l'image basée sur le contenu dans un système d'information médical

Mustapha .Machkour* – Youness Idrissi Khamlichi** – Karim Afdel***

*Laboratoire des Systèmes Informatiques et Vision LabSIV
Faculté des Sciences Ibn Zohr B.P.8106 Agadir
MAROC

machkourm@gmail.com

**Laboratoire des Systèmes Informatiques et Vision LabSIV
Faculté des Sciences Ibn Zohr B.P.8106 Agadir
MAROC

ykhamlichi@yahoo.com

***Laboratoire des Systèmes Informatiques et Vision LabSIV
Faculté des Sciences Ibn Zohr B.P.8106 Agadir
MAROC

kafdel@yahoo.fr

RESUME. Dans cet article, nous présentons l'architecture et l'implémentation d'un système sécurisé de gestion de base de données d'images médicales. Les termes de sécurité considérés sont l'intégrité et la confidentialité des données et des images médicales. Pour garantir l'intégrité, vis-à-vis des personnes non autorisées et surtout vis-à-vis de l'administrateur de la base de données nous utilisons le tatouage basé sur le contenu pour préserver les informations sensibles et intimes du patient. Pour assurer la confidentialité, nous combinons les moyens offerts par le SGBD Oracle en termes de droit d'accès et les techniques de cryptages.

ABSTRACT. In this paper, we present the architecture and the implementation of secured medical images database management system. The security terms, included here, are essentially the properties of the integrity and the confidentiality of the patient's data and his medical images. To guarantee the integrity, opposite the non-authorized people and especially opposite the database administrator that generally have all privileges, we use the watermarking content-based technique to preserve the patient's sensitive and intimate information. To assure the confidentiality of the data, we exploited the possibilities of securities offered by DBMS Oracle and the cryptography technique.

MOTS-CLES :Tatouage, sécurité des données, cryptographie, BLOB, CLOB, ORDImage de Oracle, images de mammographies.

KEYWORDS : Watermarking, data security, cryptography, BLOB, CLOB, Oracle ORDImage object, mammography images.

1. Introduction

La préservation de la confidentialité des données est devenue une priorité pour les citoyens ainsi que pour les administrations. Le besoin d'accumuler, de partager et d'analyser des données personnelles est multiple : pour l'amélioration de la qualité des soins grâce au dossier médical électronique. Partout dans le monde, les gouvernements adoptent des lois spécifiques pour cadrer l'utilisation de données personnelles. Il est cependant difficile de traduire ces lois en moyens technologiques convaincants garantissant leur application.

La sécurité des données comprend trois principales propriétés : la confidentialité, l'intégrité et la disponibilité. Grossièrement, la propriété de confidentialité évite les accès illégaux. La propriété d'intégrité garantie la détection d'une quelconque modification des données, qu'elle soit accidentelle ou malicieuse. Enfin, la propriété de disponibilité protège le système contre les attaques de déni de service.

Dans cet article nous présentons un système de gestion sécurisé de base de données médicale. La sécurisation mentionnée dans ce papier concerne essentiellement l'intégrité et la confidentialité des données. Dans le premier paragraphe, nous décrivons les fonctionnalités de ce système en particulier celle de tatouage utilisée comme un moyen supplémentaire pour garantir l'intégrité des images. Dans la seconde partie, nous présentons le schéma de la base de données. Enfin, le troisième paragraphe comprend une description de l'implémentation de ce système.

2. Fonctionnalités du système

Notre système comporte les fonctionnalités de base de tout système de gestion d'information à savoir l'insertion, la consultation et la mise à jour des données.

En plus, il doit permettre au praticien de réaliser les opérations suivantes :

- Construction de l'image tatouée,
- Stockage de l'image tatouée,
- Vérification de l'intégrité de l'image médicale
- Récupération des informations du patient à partir de l'image tatouée,
- Archivage des images origines.

2.1. Construction de l'image tatouée.

Pour garantir l'intégrité des images, nous avons utilisé la technique de tatouage où les informations et les images du patient constituent une seule entité. La construction de

l'image tatouée représente une des fonctions principales de notre système. Elle comprend les tâches suivantes :

– Restitution de l'image origine de la base de données ;

– Séparation du plan LSB de l'image ;

– Construction de la signature à base des moments de la carte du contour;

– Cryptage des données du patient et de la signature ;

– Intégration des données cryptées dans le plan LSB ;

– Formation de l'image tatouée ;

Le processus de réalisation de cette fonction est illustré sur une mammographie à la figure 1. Les informations saisies sont, en première étape, enregistrées dans la base de données sans aucun traitement et notamment sur l'image.

En deuxième étape, pour obtenir l'image tatouée, nous procédons à l'intégration des informations du patient et notre signature de sécurité basée sur la carte des contours **[**3**]** et les moments invariants **[**4**]**. L'image résultat est ensuite enregistrée dans la base de données. Pour des raisons de sécurité et de performance de la base de données, l'image origine sera sauvegardée sur un support externe, bande magnétique, DVD, etc.

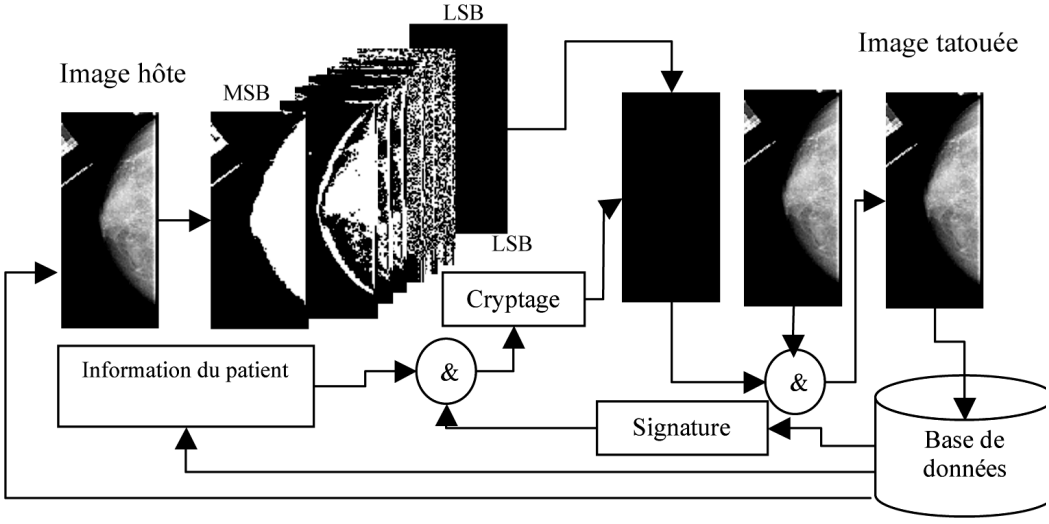

Figure 1 : *Processus de construction et stockage de l'image tatouée.*

2.1.1. Construction de la signature

La signature est composée à la fois d'une carte de contours et de la valeur moyenne des fonctions des moments. D'une part les moments de deuxième et de troisième ordre sont connus d'être des invariants de l'image. Autrement dit les valeurs de ces moments restent inchangées lors d'une modification d'échelle **[**5**]**, rotation et/ou transformations

orthogonales [6, 7, 8]. D'autre part la carte de contours caractérise de façon unique l'image. Toute modification intentionnelle ou accidentelle de l'image du patient affectera cette carte.

2.1.2. Création de la carte des contours

La carte des contours est obtenue en appliquant l'opérateur de Laplacien of Gaussian (LoG) [2] sur l'image d'origine sans le plan de bits LSB. Pour augmenter la capacité d'intégration et réduire l'espace occupé par cette carte dans le plan de bits LSB de l'image, nous avons réduit d'un facteur de 4 la taille de l'image d'origine avant la création de cette carte. La logique d'utilisation de la carte des contours est que toute modification effectuée sur l'image va affecter les contours et entraîner la modification de cette carte. Cette carte est aussi utilisée pour localiser la zone modifiée. La figure 2 montre les étapes de création de la carte des contours d'une image de mammographie.

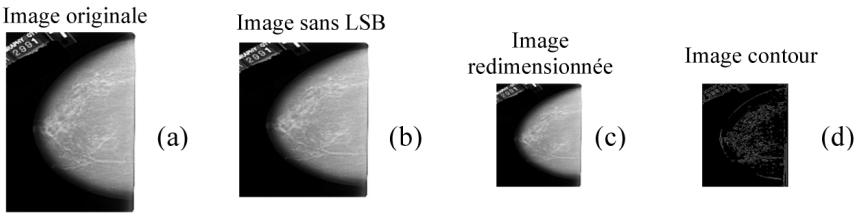

Figure 2 : *Création de la carte des contours d'une image mammographie*

2.1.3. Intégration de la signature

La première étape consiste à calculer la valeur moyenne des moments de deuxième et de troisième ordre sur l'image de mammographie sans le plan de bits LSB.

La deuxième étape commence par l'extraction de la carte de contours (figure 3 (a)), qui sera subdivisée en blocs de 6x6 pixels. Ces blocs sont répartis sur le plan de bits LSB de manière à rendre difficile la reconstruction de la carte pour des accès illégaux. La technique d'arrangement consiste à remplacer la partie droite du bloc par la partie gauche du bloc avoisinant et ceci le long d'un chemin circulaire bien défini (figure 3(b)).

Le plan de bits LSB de l'image est ensuite substitué par les données cryptées composé des informations du patient, de la valeur moyenne des moments du deuxième et du troisième ordre, et des blocs de contours.

Nous avons utilisé l'algorithme symétrique AES [1] pour le cryptage des données.

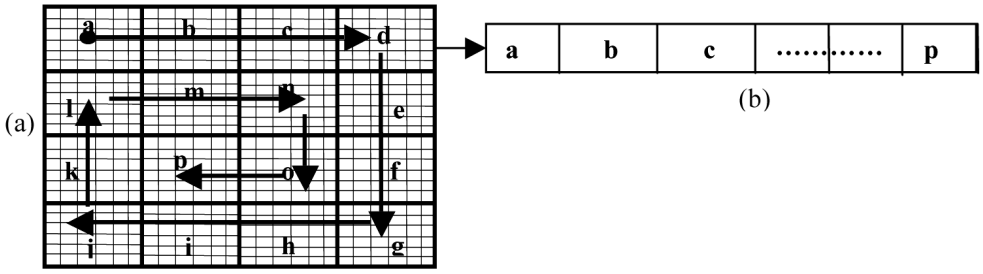

Figure 3 : *Réarrangement de la carte de contours en blocs de taille 6x6 pixels.* ***(a)*** *La carte de contour est divisée en blocs classés alphabétiquement le long d'un chemin circulaire ;* ***(b)*** *Les blocs sont arrangés en continue.*

2.2. Vérification de l'intégrité de l'image

La vérification de l'intégrité de l'image est une fonction cruciale dans notre système. Pour vérifier l'intégrité d'une image déjà stockée dans la base, nous commençons par extraire les données du patient et la valeur moyenne des moments précités à partir du plan de bits LSB de cette image. Ensuite, nous recalculons les moments invariants de cette image sans le plan de bits LSB. Si la valeur calculée des moments est identique à celle extraite du plan LSB, alors l'image restituée est intacte. Sinon, l'image a été altérée et son intégrité n'est plus préservée. Ce processus est schématisé à la figure 4

Dans le cas où l'image restituée est altérée, nous pouvons identifier la région altérée. Nous réarrangeons la carte des contours intégrée dans le plan de bits LSB en inversant les étapes décrites au haut. Nous comparons ensuite le résultat à la carte des contours de l'image restituée sans le plan de bits LSB. Une simple comparaison des deux cartes permet de localiser la région altérée (voir figure 4).

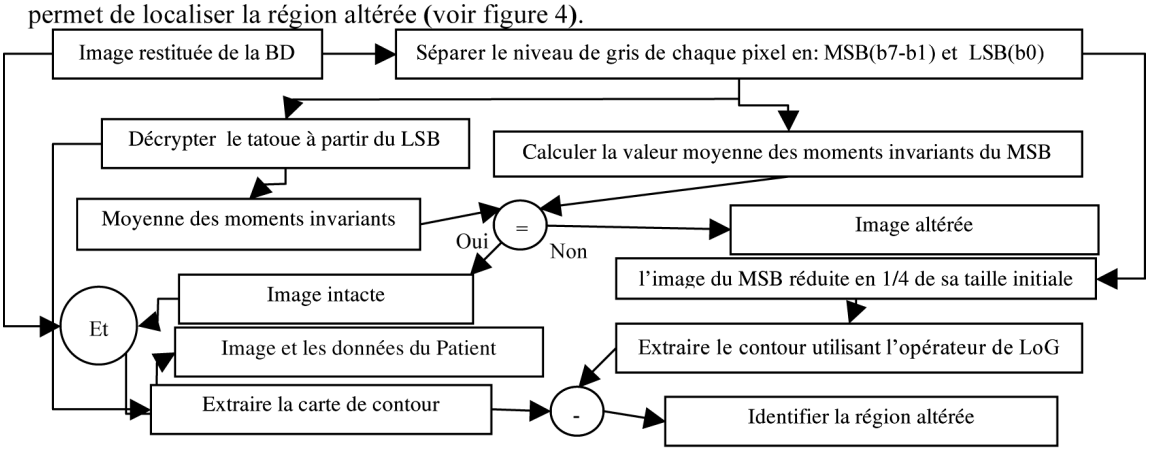

Figure 4 : *Processus de vérification de l'intégrité de l'image.*

Ce processus de vérification est aussi illustré à figure 5 par des valeurs expérimentales sur une image de mammographie.

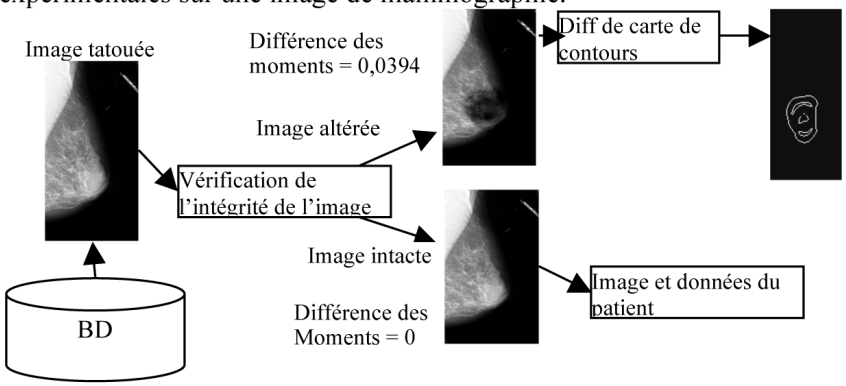

Figure 5 : *Processus de vérification de l'intégrité d'une image de mammographie.*

3. Implémentation du système

L'environnement de développement de notre système est essentiellement constitué du langage Java et du SGBD Oracle. Java a servi pour concevoir l'interface utilisateur "Swing et AWT" et implémenter les fonctionnalités du système. Le SGBD Oracle a été utilisé pour le stockage et la restitution des données.

3.1. Le langage JAVA

Nous avons utilisé le langage JAVA pour développer l'interface utilisateur d'une part, et implémenter les fonctionnalités du système d'autre part (voir figure 5). Nous avons opté pour ce langage pour la sécurité, la portabilité et son API très riche et particulièrement en classes de manipulation d'images.

3.2. Le SGBD Oracle

Oracle est un système de gestion de base de données qui permet de gérer des objets complexes en l'occurrence les images. Ces objets sont soit intégrés à la base (BLOB) soit à l'extérieur (BFILE) en stockant un descripteur du fichier image externe à la base (figure 1).

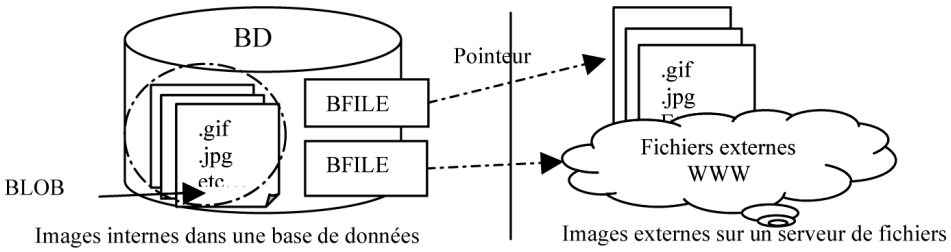

Figure 6 : *Image BLOB et BFILE*

Dans notre travail, nous nous sommes intéressés aux images BLOB qui permettent l'intégration des images au sein de la base de données et par suite bénéficier des avantages de système de base de données : partage, confidentialité…

3.3. L'interaction Java/ Base de données

L'intégration du code SQL dans le code Java permet la manipulation des données textuelles de la base de données (informations sur le patient) à partir de l'interface utilisateur. Cette manipulation est assurée par l'interface JDBC (Java DataBase Connectivity). En plus, grâce à la classe ORDImage (classe de JAVA) nous pouvons réaliser les opérations de base sur les images de type BLOB (insertion, extraction et modification). La figure suivante illustre l'interaction entreJava et base de données.

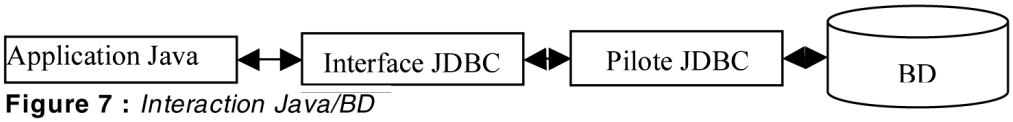

Figure 7 : *Interaction Java/BD*

3.4. Structure de la base de données image

Dans la figure suivante, nous présentons le schéma conceptuel simplifié de notre base de données médicale en termes de la notation UML(Unified Modeling Language).

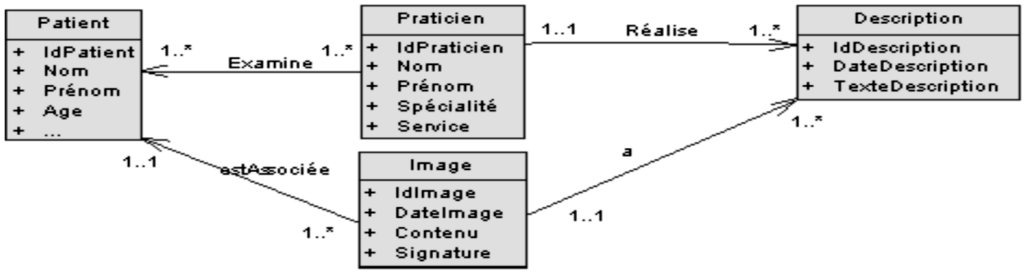

Figure 8 : *Schéma conceptuel de la base de données médicale*

4. Conclusion

Dans cet article nous avons mis en place une architecture sécurisée utilisant la technique de tatouage comme un moyen supplémentaire de sécurité assurant l'intégrité des images et des données. Pour garantir la confidentialité nous avons combiné les possibilités de sécurités offertes par SGBD Oracle et les techniques de cryptage.

5. Références

[1] J. Daemen, V. Rijmen, (1999, September 03). *AES Proposal Rijndael, Networks (2nd ed.)* [Online]. Available: http://csrc.nist.gov/CryptoToolkit/aes/index.html

[2] E. C. Hildreth, The Detection of Intensity Changes by Computer and Biological Vision Systems, *Computer Vision, Graphics, and Image Processing*, 22, 1-27, 1983.

[3] Y. I. Khamlichi, Y. Zaz, M. Machkour, K. Afdel. Authentication System for Medical Watermarked Content Based Image, *WSEAS TRANSACTIONS on SIGNAL PROCESSING*, Issue 5, Volume 2, May 2006, ISSN 1790-5022 (pp 826-830).

[4] Y. I. Khamlichi, M. Machkour, K. Afdel, A. Moudden. Multiple Watermark for Tamper Detection in Mammography Image, *WSEAS TRANSACTIONS on COMPUTERS*, Issue 6, Volume 5, June 2006, ISSN 1109-2750 (pp 1222-1226)

[5] A. G. Mamistvalov, n-dimensial moment invariants and conceptual theory of recognition n-dimensional solids. *IEEE Trans*. On PAMI, 20(8):819-831, Aug. 1998.

[6] H. Ming-Kuel, Visual pattern recognition by moment invariants. *IRE trans. Information Theory*, IT(8), 179-187, 1962

[7] C. Schmid, Appariement d'images par invariants locaux des niveaux de gris : application à l'indexation d'une base d'objets, Thèse de doctorat, INRIA, Juillet 1996.

[8] O. Tahri, F. Chaumette, "Determination of Moment Invariants and Their Application to Visual Servoing", Rapport de recherche no 4845 — Juin 2003, INRIA, 2003.