

UNIVERSITÉ CONSTANTINE 2

**Faculté des Nouvelles Technologies de l'Information et de la
Communication**

Département de l'Informatique Fondamentale et ses Applications

N° d'ordre

Thèse de Doctorat en Sciences en Informatique

Thème :

**Sécurisation d'images médicales par méthodes
hybrides : cryptage et insertion de données
cachées**

Présentée par :

BRAHIMI Zahia

Devant le Jury Composé de :

Mme BOUFAIDA Zizette	Professeur - Université de Constantine2	Présidente
M. KHOLLADI Mohamed-Khireddine	Professeur EL OUED	Rapporteur
M. BESSALAH Hamid	Docteur - CDTA, Alger	Co-Rapporteur
M. MOUSSAOUI Abdelouahab	Professeur - Université de Sétif 1	Examineur
M. CHIKHI Salim	Professeur - Université de Constantine 2	Examineur
M. SERIDI Hamid	Professeur - Université de Guelma	Examineur

TABLE DES MATIÈRES

<i>Remerciements</i>	<i>i</i>
<i>Résumés</i>	<i>ii</i>
<i>Liste des figures</i>	<i>iii</i>
<i>Liste des tableaux</i>	<i>iv</i>
Introduction Générale	1
Chapitre 1. Le Cryptage	
1.1 Introduction	4
1.2 Généralités sur la Cryptographie	4
1.2.1 Objectifs de la Cryptographie	4
1.2.2 Principe de Kerckhoffs	5
1.2.3 Définition	5
1.3 Cryptosystèmes Classiques	5
1.3.1 Cryptage Par décalage (Shift Cipher)	6
1.3.2 Cryptage par Substitution.....	6
1.3.3 Fonctions Affines	6
1.3.4 Chiffrement de Vigenère	7
1.3.5 Chiffrement de Hill	7
1.3.6 Chiffrement par Permutation	7
1.4 La Cryptographie Moderne	7
1.4.1 Chiffrement symétrique	8
1.4.2 Chiffrement par bloc	8
1.4.2.1 Architecture générale	8
1.4.2.2 Principaux algorithmes de chiffrement symétriques par bloc	10
a. DES et 3-DES (Data Encryption Standard)	10
b. AES (Advanced Encryption Standard)	11
1.4.3 Algorithmes de chiffrement par flot.....	12
1.4.3.1 Chiffrement de Vernam (One-time pad)	12
1.4.3.2 Chiffrement synchrone	13
1.4.3.3 Chiffrement asynchrone	14
1.4.4 Cryptographie asymétrique	14
1.4.4.1 Algorithme RSA	15
1.5 Modes opératoires de chiffrement	16
1.6 La Cryptanalyse	18
1.6.1 La cryptanalyse différentielle	18
1.6.2 La cryptanalyse linéaire	19
1.7 Conclusion	20

Chapitre 2. Techniques d'Insertion de Données Cachées

2.1 Introduction	21
2.2 Généralités, Concepts et Définitions	21
2.2.1 Définition	22
2.2.2 Catégories	23
2.2.3 Règles en stéganographie	23
2.2.4 Architecture	23
2.2.5 Liens avec d'autres technologies	24
2.3 L'Insertion de Données Cachées	25
2.3.1 Le principe de l'IDC	25
2.3.2 Les applications de l'IDC	27
2.3.3 Contraintes techniques de l'IDC	27
2.4 Techniques d'Insertion de données cachées	28
2.4.1 Les techniques de l'IDC dans le domaine Spatial	28
2.4.1.1 Les techniques basées LSBs	29
2.4.1.2 Les techniques basées expansion de différences	30
2.4.1.3 La technique BPCS	32
2.4.2 Les techniques de l'IDC dans le domaine fréquentiel et multirésolution	33
2.4.3 L'insertion de données cachées dans le flux compressé.....	34
2.5 Les Techniques d'évaluation des méthodes d'IDC	35
2.5.1 Evaluation de la robustesse	35
2.5.2 Evaluation de la qualité des images	36
2.6 Conclusion	38

Chapitre 3. Le Codeur JPEG 2000

3.1 Introduction	39
3.2 JPEG 2000 : une norme à douze parties	39
3.3 Fonctionnalités de JPEG 2000	43
3.3.1 Meilleures performances à faible débit	43
3.3.2 Compression avec et sans pertes dans un même algorithme.....	43
3.3.3 Transmission progressive par résolution ou qualité	43
3.3.4 Accès aléatoire aux données	45
3.3.5 Région d'intérêt (RI)	45
3.3.6 Détection d'erreurs en milieu bruité	45
3.3.7 Traitement d'une large variété d'images	45
3.3.8 Architecture ouverte	45
3.4 Domaines d'application	45
3.5 Processus de codage dans JPEG 2000	47
3.5.1 Modèle d'image utilisé	49
3.5.2 La grille de référence	49
3.5.3 Prétraitement	51
3.5.3.1 Le Tiling	51
3.5.3.2 DC Level Shifting	

3.5.3.3 La transformée couleur	52
3.5.4 La décomposition en ondelettes « DWT »	53
3.5.5 La quantification	54
3.5.6 Le codage entropique	55
3.5.7 Allocation de débit	56
3.5.8 Organisation du codestream	58
3.6 Codage de la Région d'Intérêt (RI)	59
3.7 Kakadu : Implémentation Software de JPEG 2000	61
3.8 Conclusion	62

Chapitre 4. Le Cryptage Sélectif

4.1 Introduction	63
4.2 Stockage et Transmission Sécurisés des Images Médicales	65
4.3 Le Cryptage Sélectif : Définition et Intérêts	65
4.4 Théorie de l'Information et Cryptage sélectif	66
4.5 Critères d'évaluation	69
4.6 Cryptanalyse des cryptosystèmes d'images	70
4.6.1 Attaques utilisées dans les cryptosystèmes à chiffrement sélectif	71
4.7 Cryptage Sélectif et Compression	72
4.8 Les Scénarios d'Application du Cryptage Sélectif	73
4.9 Les techniques de cryptage sélectif des images fixes.....	76
4.9.1 Techniques dans le domaine spatial et fréquentiel	76
4.9.2 Techniques de Cryptage Sélectif dans Jpeg 2000	77
4.10. Discussion et Conclusion	78

Chapitre 5. Techniques de Cryptage Sélectif implémentées: Tests et Résultats

5.1 Introduction	80
5.2 Rappel de la structure du codestream	81
5.3 Schémas Proposés pour le cryptage sélectif du Codestream JPEG2000	82
5.3.1 Chiffrement sélectif par precincts	82
5.3.2 Chiffrement sélectif Basé sur la permutation des entêtes des Paquets de Données (Packets Headers)	87
5.3.3 Chiffrement sélectif de la région d'intérêt (RI) d'une image médicale	91
i. Cryptage sélectif de la RI basé sur une fonction de permutation de bits-plans les plus significatifs	92
ii. Chiffrement sélectif de la RI basé sur une fonction d'inversion des bits-plans les plus significatifs	94
iii. Chiffrement sélectif de la RI en combinant les fonctions de permutation et d'inversion des bits-plans les plus significatifs	95
5.3.4 Evaluation de la sécurité du schéma Permutation-inversion	98
5.4 Conclusion	99

Chapitre 6. Techniques d'IDC implémentées:tests et résultats

6.1 Introduction.....	100
6.2 les approches développées	100
6.2.1 L'approche de katsutoshi	100
6.2.2 Processus d'insertion et d'extraction basé sur la DE	103
6.2.3 L'approche par expansion de différence modifiée	108
6.2.4 L'approche par BPCS	112
6.2.5 L'approche hybride BPCS et DE.....	119
6.3 Conclusion	121
<i>Conclusion Générale</i>	122
<i>Bibliographie</i>	124

RESUME

L'utilisation de plus en plus excessive de réseaux de soins impose la préservation de l'intégrité et l'authenticité des informations médicales, concernant les patients. La transmission d'informations médicales, et particulièrement les images à travers des réseaux publics, n'est pas sans poser des problèmes de sécurité et de confidentialité. Pour répondre à ce double besoin de sécurité, deux grandes familles de technologies complémentaires se développent. La première s'appuie sur une protection via le cryptage des images. La seconde famille base la protection sur l'insertion de données cachées (IDC) dont le but est d'insérer de manière secrète un message à l'intérieur d'un média, dans notre cas l'image médicale et les données médicales auxiliaires.

Le cryptage sélectif est une manière d'adapter le niveau de sécurité des données à chiffrer au niveau de protection désiré. Il permet de réduire les ressources informatiques utilisées et le temps de traitement des données surtout pour des applications sensibles. C'est en effet le cas des images médicales prises depuis un appareil médical et devant être envoyées sur le réseau afin d'établir un diagnostic à distance. Cette image doit être transmise rapidement et sûrement : un cryptage sélectif est alors la meilleure solution répondant au compromis (temps/sécurité).

Comme nous nous intéressons au chiffrement sélectif dans le domaine compressé, les techniques proposées doivent répondre à quelques propriétés notamment une compressibilité équivalente et la sécurité.

L'IDC est une technique qui permet d'insérer une capacité très élevée de données dans une image numérique de manière imperceptible. Elle peut être utilisée dans plusieurs domaines et en particulier en imagerie médicale.

Dans le cadre de cette thèse, nos travaux de recherche ont conduit à la création de nouvelles techniques de chiffrement sélectif, dans le codeur JPEG 2000, basées sur des fonctions cryptographiques ne nécessitant parfois pas, la transmission de la clé de chiffrement.

De même, nous avons développé de nouvelles techniques réversibles pour l'Insertion de Données Cachées permettant d'assurer la protection des données sans dégrader l'image. Ces techniques s'adaptent aux fonctionnalités de la norme JPEG 2000.

Mots Clés : Cryptographie, Stéganographie, Cryptage/Chiffrement Sélectif, Compression, JPEG 2000, Insertion de Données Cachées, images médicales, fonctions cryptographiques.

ملخص

إنّ الاستعمال المتزايد لشبكات العلاج يستلزم الحفاظ على سلامة و مصداقية المعلومات الطبية المتعلقة بالمرضى، حيث يطرح إرسال المعلومات الطبية، لاسيما الصور، عبر الشبكات العمومية، مشاكل تتعلق بالأمن و السرية.

و بغية التكفل بهذا الانشغال، يتم تطوير مجموعتين واسعتين و متكاملتين من التكنولوجيات؛ تقوم المجموعة الأولى على الحماية من خلال تشفير الصور و تركز المجموعة الثانية على الحماية على إدماج بيانات مخفية (IDC) عن طريق إدراج، ضمن وسيط من الوسائط، رسالة سرية، تتمثل، فيما يخص بحثنا هذا، في الصورة الطبية و البيانات الطبية التكميلية.

يعد التشفير الانتقائي طريقة لتكثيف مستوى تأمين المعطيات المشفرة مع مستوى الحماية المرجوة. فهو يسمح بتقليص الموارد المعلوماتية المستعملة و مدة معالجة المعطيات، لاسيما بالنسبة للتطبيقات الحساسة.

و هذا هو فعلا حال الصور الطبية المأخوذة من جهاز طبي و التي ينبغي إرسالها على الشبكة من أجل القيام بكشف عن بعد، إذ ينبغي إرسال هذه الصورة بسرعة و بأمان: فالتشفير الانتقائي هو إذا أفضل حل يستجيب لضرورة التوفيق بين عامل الوقت و مقتضيات الأمن.

و بما أننا نهتم بالتشفير الانتقائي في المجال المضغوط، ينبغي للتقنيات المقترحة أن تستجيب لبعض الخصائص، لاسيما الانضغاطية المتكافئة و الأمن.

يعد إدماج البيانات المخفية (IDC) تقنية تسمح بإدراج نسبة عالية جدا من البيانات في صورة رقمية بشكل غير محسوس. ويمكن استخدامها في مجالات عديدة لاسيما في التصوير الطبي.

في إطار هذا البحث، أفضت أعمال بحثنا إلى إيجاد تقنيات جديدة للتشفير الانتقائي، ضمن المشفر JPEG 2000، القائم على الوظائف المشفرة التي لا تقتضي، أحيانا، إرسال مفتاح التشفير. كما أننا طورنا تقنيات انعكاسية جديدة من أجل إدماج البيانات المخفية التي تسمح بضمان حماية البيانات دون تخريب الصورة. و تتماشى هذه التقنيات مع وظائف معيار JPEG 2000.

المصطلحات الأساسية: الترميز، إخفاء المعلومات، التشفير/ التشفير الانتقائي، الضغط، JPEG 2000، إدماج البيانات المخفية، صور طبية، وظائف تشفيرية.

ABSTRACT

The increasingly use of health care networks requires the preservation of the integrity and authenticity of the medical information about patients. The transmission of medical information, particularly images through public networks, is not without problems of security and confidentiality.

To address this dual need for security, two large families of complementary technologies are being developed. The first is based on protection via encryption images. In the second family, the information security is based on the data hiding (DH), whose goal is to insert in a secret message within a medium which is the medical image in this case.

Selective encryption is a way to adjust the level of data security to encrypt the desired level of protection. It reduces the resources used and the time of data processing especially for sensitive applications. Indeed, it is the case of medical images taken from a medical device and should be sent over the network to establish a remote diagnosis. This image must be transmitted quickly and surely: a selective encryption is then the best solution to meet the compromise (time/security).

As we focus on selective encryption in the compressed domain, the proposed techniques must satisfy some properties including equivalent compressibility and security.

The Data Hiding is a technique that allows you to insert a very high capacity data in a digital image in an imperceptible way. It can be used in many fields, especially in medical imaging.

In this thesis, our research led to the creation of new selective encryption techniques in JPEG 2000 encoder based on cryptographic functions not requiring sometimes, the transmission of the encryption key.

Similarly, we have developed new techniques for reversible Data Hiding to ensure data protection without degrading the image. These techniques can be adapted to the features of the JPEG 2000 standard.

Keywords: Cryptography, Steganography, Encryption / Selective Encryption, Coding, JPEG 2000, Data Hiding, medical images, cryptographic functions.