République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

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	Examinateur
M. CHIKHI Salim	Professeur - Université de Constantine 2	Examinateur
M. SERIDI Hamid	Professeur - Université de Guelma	Examinateur

TABLE DES MATIÈRES

Chapitre 2. Techniques d'Insertion de Données Cachées

Chapitre 3. Le Codeur JPEG 2000

Chapitre 4. Le Cryptage Sélectif

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

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

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 السرّية.

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 لتكييف 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.