شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

HANAA ALY

Computer Science Department
Faculty of Computer and Information Sciences
Ain Shams University

Protecting Patients' Privacy using Medical Images Watermarking

Thesis submitted as a partial fulfillment of the requirements for the degree of
Master of Science in Computer and Information Sciences

By

Alaa Hussein Ibrahim El-Saadawy
Teaching Assistant at Computer Science Department,
Faculty of Computer and Information Sciences,
Ain Shams University

Under Supervision of

Prof. Dr. Mohamed Ismail Roushdy
Professor of Computer Science,
Faculty of Computer and Information Sciences,
Ain Shams University

Dr. Maryam Nabil Al-Berry
Lecturer at Scientific Computing Department,
Faculty of Computer and Information Sciences,
Ain Shams University

Dr. Ahmed Salah El-Sayed
Lecturer at Computer Science Department,
Faculty of Computer and Information Sciences,
Ain Shams University

Acknowledgment

First of all I thank Allah, the most merciful and gracious, who gave me the knowledge, patience and strength to complete this thesis, and blessed me with his inspired gifts to overcome the obstacles I encountered.

I would like to express my deep gratitude to my supervisors who I am very lucky to work under their supervision; Prof. Dr. Mohamed Roushdy for his usual support, patience, encouragement and guidance. Dr. Maryam Al-Berry and Dr. Ahmed Salah for their usual support, motivation and guidance, I extend my utmost gratitude and appreciation for your technical and scientific help, continuous supportive guidance in both technical and non-technical issues. I am deeply thankful.

Special thanks for my sister Hadeer for her continuous technical support.

I would like to thank the world best gift, the most supportive family. I would like to thank Mum and Dad who have devoted themselves to support me in my whole life, not just this work for their endless passionate support and encouragement and the sleepless nights they spent to make it easier for me, this thesis dedicated to you, to make you proud. Without you, everything is nothing. And my sisters Mahitab, Hadeer and Esraa for always being by my side in the downs and ups. Thanks my sisters for your usual moral support.

My family, thanks for being the shoulder I can always depend on and for constantly pushing me to become the person I want to become and create the life I want for myself.

I would like to thank my fiancée Mahmoud for being by my side. Thanks for your motivational encouragement and support, believing in me and pushing me to continue working on my thesis.

Also I would like to thank Engineer Amir Alfoly for his support and encouragement and provide me with everything to facilitate working on my thesis.

Last but not least, I would like to thank all my professors, colleagues and students who kept on encouraging me, and special thanks for my friend Dina Hassanien for her constant encouragement and support. Thank you for being in my life.

Abstract

As a result of modern communication technology, the transmission of medical images among different specialists in different medical institutes has become popular. Accordingly, protecting patients' data and authenticity against any unauthorized access or modification is a must.

Watermarking the images technique before transmission has became a main step to protect patient's information integrity, copyright, authentication and to protect patients' information against any signal processing or geometric attacks.

This thesis proposes a fragile reversible watermarking scheme. The proposed scheme is based on embedding a Quick Response (QR) code that contains the patient's data into the medical image followed by encrypting the image using Rivest-Shamir-Adleman (RSA) and finally compressing the encrypted image using Huffman encoding algorithm.

The proposed scheme can detect various types of geometric and signal processing attacks and localize tampering caused by copy-paste, text addition and content removal attacks in the extraction steps. For evaluating the proposed scheme, two different datasets were used which are OPENi and MURA as host images and QR code as a watermark image. Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM) and Bit Error Rate (BER) were used as evaluation metrics .

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	**Stands for**
AE	**A**rithmetic **E**ncoding
AES	**A**dvanced **E**ncryption **S**tandard
BER	**B**it **E**rror **R**ate
BP	**B**inary **P**attern
CA	**A**pproximation **C**oefficients
CD	**D**iagonal **C**oefficients
CH	**H**orizontal **C**oefficients
CT-Scan	**C**omputed **T**omography **Scan**
CV	**V**ertical **C**oefficients
CW	**C**omposed **W**atermark
DCT	**D**iscrete-**C**osine **T**ransform
DES	**D**ata **E**ncryption **S**tandard
DFT	**D**iscrete **F**ourier **T**ransform
DTCWT	**D**ual-**T**ree **C**omplex **W**avelet **T**ransform
DWT	**D**iscrete-**W**avelet **T**ransform
ECC	**E**lliptic-**C**urve-based encryption
EMR	**E**lectronic **M**edical **R**ecord
EPR	**E**lectronic **P**atient **R**eport
EZW	**E**mbedded **Z**erotree **W**avelet
HF	**H**igh **F**requency
HS	**H**ierarchical **S**egmentation
ICA	**I**mperialistic **C**ompetition **A**lgorithm
IWT	**I**nverse **W**avelet **T**ransform

LBP	**L**ocal **B**inary **P**attern
LSB	**L**east **S**ignificant **B**it
MD5	**M**essage **D**igest **5**
MRI	**M**agnetic **R**esonance **I**maging
MSE	**M**ean **S**quare **E**rror
MURA	**MU**sculoskeletal **RA**diographs
NCC	**N**ormalized **C**ross-**C**orrelation
PNN	**P**robabilistic **N**eural **N**etwork
PSNR	**P**eak **S**ignal to **N**oise **R**atio
QR	**Q**uick **R**esponse
RLE	**R**un-**L**ength **E**ncoding
ROI	**R**egion **O**f **I**nterest
RONI	**R**egion **O**f **N**on-**I**nterest
RSA	**R**ivest-**S**hamir-**A**dleman
SR	**S**imilarity **R**atio
SSIM	**S**tructural **S**imilarity **I**ndex **M**atrix
SVD	**S**ingular **V**alue **D**ecomposition
US	**U**nited **S**tate
WGN	**W**hite **G**aussian **N**oise

Chapter 1

Introduction

Chapter 1. Introduction

1.1 Thesis Motivation

Using shared medical images in some services like telemedicine, telediagnosis, and teleconsultation has been facilitated after the availability of computer networks. Sharing patient information among specialists in different hospitals is a must to understand diseases and avoid misdiagnosis [1] [2] [3]. One of the available techniques and approaches to protect medical images, while transferred through the internet, against any corruption or unauthorized access is the watermarking techniques [4].

Hiding the patient's data into the medical image without distorting it during transmission is essential to ensure the confidentiality of the transmitted data. Recovering the hidden data and the original medical image without errors is the priority in Electronic Patient Record (EPR) data hiding [5] [6]. Since making any modifications on medical images may lead to misdiagnosis, authenticity, which ensures that the source is valid and belong to the right patient, and integrity control, which checks that the image has not tampered, are the major purposes of medical images watermarking [7] [8] [9].

Since securing the patient's data is our main purpose, encrypting the medical image is considered as one of the main steps. There are several encryption techniques [10], such as, International Data Encryption Algorithm (IDEA) [11], private key encryption standard, Data Encryption Standard (DES) [12] Advanced Encryption Standard (AES) [13], Elliptic-Curve-based encryption (ECC) [14], and public key standards such as Rivest-Shamir-Adleman (RSA) [15].

Medical image compression is also a necessary step since storing a large number of images requires huge long-term storage space. There are two types of image compression algorithms, namely, lossless and lossy algorithms. For achieving a high compression rate, lossy algorithms are used, while lossless algorithms are used in case that we need to restore the original data without any loss [16].

Attacks are one of the most popular challenges of watermarking techniques. The two common attacks are signal processing attacks (like image compression, adding noise and different filters) and geometric attacks (such as rotation, translation and scaling) [17] and tampers like (copy-paste, text addition and content removal).

Medical image watermarking has many advantages: 1) The storage space required for the image and the patient record will be reduced by embedding the data in the corresponding images; 2) The additional bandwidth which is required for the transmission of an image by hiding data in the image itself can be avoided; 3) If the disease is clandestine, normally a patient does not like to expose his medical report to the public [18].

Besides the advantages of watermarking there are challenges associated with watermarking in Electronic Medical Record (EMR) systems such as 1) Some fields in EMR are more relevant in the diagnosis process; as a result, small variations in them could change the diagnosis; 2) A misdiagnosis might not only result in a life-threatening scenario but also might lead to significant costs of the treatment for the patients [19].