

نموذج ترخيص

أنا الطالب: نور حسين عبد الله محمد عبد الله أُمّح الجامعة الأردنية و /
أو من تفوضه ترخيصاً غير حصري دون مقابل بنشر و / أو استعمال و / أو استغلال و /
أو ترجمة و / أو تصوير و / أو إعادة إنتاج بأي طريقة كانت سواء ورقية و / أو إلكترونية
أو غير ذلك رسالة الماجستير / الدكتوراه المقدمة من قبلي وعنوانها.

Exploring Encryption and Watermarking
Techniques for Secure Telemedicine.

وذلك لغايات البحث العلمي و / أو التبادل مع المؤسسات التعليمية والجامعات و / أو لأي
غاية أخرى تراها الجامعة الأردنية مناسبة، وأُمّح الجامعة الحق بالترخيص للغير بجميع أو
بعض ما رخصته ليا.

اسم الطالب: نور حسين عبد الله محمد عبد الله.

التوقيع: [Signature]

التاريخ: 2013/8/6

**EXPLORING ENCRYPTION AND WATERMARKING
TECHNIQUES FOR SECURE TELEMEDICINE**

By
Noor Hussein Haj-Abdullah

Supervisor
Dr. Gheith Abandah, Associate Prof.

Co-Supervisor
Dr. Ali Al-Haj, Associate Prof.

**This Thesis was Submitted in Partial Fulfillment of the Requirements for the
Master's Degree of Science in Computer Engineering**

**Faculty of Graduate Studies
The University of Jordan**

تعتمد كلية الدراسات العليا
هذه الترسية من الرسالة
التوقيع..... التاريخ.....

August, 2013


COMMITTEE DECISION

This Thesis/Dissertation (Exploring Encryption and Watermarking Techniques for Secure
Telemedicine) was Successfully Defended and Approved on 4/8/2013

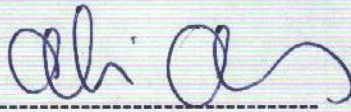
Examination Committee

Signature

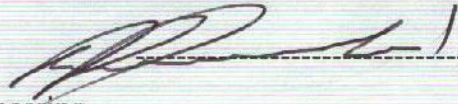
Dr. Gheith Abandah, (Supervisor)
Associate Professor of Computer Engineering



Dr. Ali Al Haj, (Co-Supervisor)
Associate Professor of Computer Engineering
Princess Sumaya University for Technology



Dr. Andraws Swedan, (Member)
Associate Professor of Computer Engineering



Dr. Iyad Jafar, (Member)
Associate Professor of Computer Engineering



Dr. Ahmad Tawayha, (Member)
Associate Professor of Electrical Engineering
Princess Sumaya University for Technology



تعتمد كلية الدراسات العليا
 هذه النسخة من الرسالة
 التوقيع: التاريخ: 4/8/2013

**EXPLORING ENCRYPTION AND WATERMARKING
TECHNIQUES FOR SECURE TELEMEDICINE**

By
Noor Hussein Haj-Abdullah

Supervisor
Dr. Gheith Abandah, Associate Prof.

Co-Supervisor
Dr. Ali Al-Haj, Associate Prof.

**This Thesis was Submitted in Partial Fulfillment of the Requirements for the
Master's Degree of Science in Computer Engineering**

**Faculty of Graduate Studies
The University of Jordan**

August, 2013

COMMITTEE DECISION

This Thesis/Dissertation (Exploring Encryption and Watermarking Techniques for Secure Telemedicine) was Successfully Defended and Approved on 4/8/2013

Examination Committee

Signature

Dr. Gheith Abandah, (Supervisor)
Associate Professor of Computer Engineering



Dr. Ali Al Haj, (Co-Supervisor)
Associate Professor of Computer Engineering
Princess Sumaya University for Technology



Dr. Andraws Swedan, (Member)
Associate Professor of Computer Engineering



Dr. Iyad Jafar, (Member)
Associate Professor of Computer Engineering



Dr. Ahmad Tawayha, (Member)
Associate Professor of Electrical Engineering
Princess Sumaya University for Technology



تعتمد كلية الدراسات العليا
 هذه النسخة من الرسالة
 التوقيع: التاريخ: ٢٠١٣/٨/٤

DEDICATION

To my Parents,

Hussein Abdullah Haj-Abdullah

&

Najla Mahmoud Yassin

To my Husband,

Ali Saleem Al-Rabi

To my Children,

Kareem &

Ghena (baby to come)

ACKNOWLEDGMENT

I would like to express my sincerest gratitude to my advisers Dr. Gheith Abandah and Dr. Ali Al-Haj for their invaluable advice and continuous assistance throughout the work in this research. I am grateful to express my special thanks to Dr. Ali Al-Haj for his endless support, time, and motivations throughout the course. Under his guidance and encouragement I successfully surpassed many difficulties and learned a lot.

It is a pleasant task to thank my collegous, my friends, and all those who contributed in many ways to the success of this thesis and made it an unforgettable experience for me.

Table of Contents

Committee Decision.....	ii
Dedication.....	iii
Acknowledgment.....	iv
Table of Contents.....	v
List of Tables.....	viii
List of Figures.....	ix
List of Abbreviations.....	xvi
Abstract.....	viii
Chapter 1 Introduction.....	1
1.1 Importance of Telemedicine.....	1
1.2 Telemedicine Security Requirements.....	3
1.3 Current Approaches and Limitations.....	4
1.4 Proposed Approaches.....	6
1.5 Thesis Organization.....	7
Chapter 2 Cryptography: Fundamentals and Application in Telemedicine....	9
2.1 Introduction to Encryption and Cryptography.....	9
2.2 Symmetric Encryption.....	11
2.3 Asymmetric Encryption.....	15

2.4 Data Hashing.....	18
2.5 Digital Signatures.....	20
2.6 Cryptography in Telemedicine.....	22
2.7 The DICOM Standard	23
2.8 Literature Review.....	29
Chapter 3 Watermarking: Fundamentals and Application in Telemedicine....	36
3.1 Watermarking Systems.....	36
3.2 Watermarking Requirements.....	38
3.3 Classification of Watermarking Techniques.....	41
3.4 Relevance of Watermarking with Telemedicine	51
3.5 Literature Review	54
Chapter 4 Proposed Crypto-based Secured Telemedicine Algorithm.....	64
4.1 Proposed Algorithm I.....	64
4.2 Proposed Algorithm II.....	70
4.3 Implementations of the Algorithms.....	74
4.4 Performance Evaluation of the Algorithms.....	79
Chapter 5 Proposed Watermarking-based Secured Telemedicine Algorithm..	92
5.1 Watermarks Generation Module.....	92
5.2 Image Preprocessing.....	94

5.3 Watermarks Embedding/Extraction in RONI.....	96
5.4 Watermarks Embedding/Extraction in ROI.....	103
5.5 Performance Evaluation of the Algorithm.....	105
Chapter 6 Proposed Watermarking-Encryption based Secured Telemedicine Algorithm.....	118
6.1 Watermarks Generation Module	118
6.2 Image Preprocessing.....	121
6.3 Watermarks Embedding/Extraction in RONI.....	121
6.4 Performance Evaluation of the Algorithm.....	128
Chapter 7 Discussion and Conclusions.....	143
7.1 Attributes of the Proposed Algorithms.....	143
7.2 Limitations of the Proposed Algorithms.....	144
7.3 Future Research.....	144
References.....	145
Abstract in Arabic.....	152

List of Tables

	Page
Table 1 Symmetric key systems (Stallings, 1999)	13
Table 2 Commercial public key systems (Stallings, 1999)	17
Table 3 Basic application level confidentiality profile attributes	27
Table 4 Comparison study related encryption techniques	30
Table 5 Comparison study related watermarking schemes	55
Table 6 Comparison study related encryption and watermarking schemes	60
Table 7 A summary of the properties of GCM	76
Table 8 Entropy values for original image and ciphered ones	85
Table 9 Correlation and PSNR between original plain and encrypted images	86
Table 10 Time in seconds required for encryption and decryption	87
Table 11 Robustness against statistical attacks	88
Table 12 A comparison results in terms of entropy, PSNR, correlation, and time	90

List of Figures

	Page	
Figure 1	System block diagram for the encryption approach	4
Figure 2	System block diagram for the watermarking approach	5
Figure 3	System block diagram for the hybrid approach	6
Figure 4	Types of cryptography	10
Figure 5	Encryption and decryption process	11
Figure 6	Keys needed for privately communicating with each other	12
Figure 7	key-based asymmetric algorithm	16
Figure 8	Digital signature signing and verifying algorithm	21
Figure 9	Signing and encryption process	34
Figure 10	Decryption and verification process	35
Figure 11	Watermarking Processes	37
Figure 12	Generic watermarking scheme	37
Figure 13	Watermarking properties	39
Figure 14	Watermarking classification	42
Figure 15	Least significant bit substitution technique	43
Figure 16	Wavelet analysis	46
Figure 17	Wavelets transform types	47

Figure 18	1-level DWT decomposition process	47
Figure 19	One-Level DWT decomposition	49
Figure 20	One-Level DWT decomposition of MRI image	49
Figure 21	Three-Level DWT decomposition	50
Figure 22	Three-Level DWT decomposition of MRI image	50
Figure 23	Wavelet decomposition (4-level DWT) of an image	58
Figure 24	Proposed approach for data encryption	65
Figure 25	Proposed approach for data retrieval and verification	65
Figure 26	Signing and encryption process	66
Figure 27	Decryption and verification process	68
Figure 28	Signing and encryption process	70
Figure 29	Decryption and verification process	73
Figure 30	AES-GCM vs. other (NIST) Authenticated Encryption	77
Figure 31	Histogram of plain and cipher image related to the proposed algorithm I	80
Figure 32	Histogram of plain and cipher image related to the proposed algorithm II	82
Figure 33	Decryption using correct key related to the proposed algorithm I	83
Figure 34	Decryption using incorrect key related to the proposed	83

	algorithm I	
Figure 35	Decryption using correct key related to the proposed algorithm	84
	II	
Figure 36	Decryption using incorrect key related to the proposed	84
	algorithm II	
Figure 37	Total execution time needed for the schemes	90
Figure 38	Encryption time needed for AES-GCM, Whirlpool, and ECDSA	91
Figure 39	Decryption time needed for AES-GCM, Whirlpool, and ECDSA	91
Figure 40	Image of the patient information watermark	93
Figure 41	Fragile watermark image	94
Figure 42	ROI selection and RONI separation from polygon shape of ROI	95
Figure 43	Dividing the image into blocks and determining ROI/RONI	96
	blocks	
Figure 44	Embedding procedures for ROI and RONI	97
Figure 45	Three level DWT decomposition of each block	98
Figure 46	A block diagram of RONI embedding procedure	98
Figure 47	Choosing the sub-bands	99
Figure 48	The extraction procedures for ROI and RONI	101
Figure 49	A block diagram of RONI extraction procedure	102

Figure 50	A block diagram of ROI embedding procedure	103
Figure 51	A block diagram of ROI extraction procedure	104
Figure 52	(a) The original image, (b) the watermarked image	107
Figure 53	(a) Original watermark, (b) extracted watermark	108
Figure 54	Watermarked image cropping with different values of block size	108
Figure 55	Extracted watermark (patient information) after cropping	109
Figure 56	(a) Correlation vs. block size and (b) PSNR vs. block size; after cropping	109
Figure 57	Gaussian attack with different mean values on the watermarked image	110
Figure 58	Extracted watermark (patient information) from HL3 after Gaussian attack	111
Figure 59	(a) Correlation values vs. mean and (b) PSNR vs. mean; after Gaussian attack	111
Figure 60	Compression attack of different quality values on the watermarked image	112
Figure 61	Extracted watermark (patient information) from HL3 after compression attack	113
Figure 62	(a) Correlation vs. quality and (b) PSNR vs. quality ; after	113

	compression attack	
Figure 63	Dithering attack of different Q_e values on the watermarked image	114
Figure 64	Extracted watermark (patient information) from HL3 after dithering attack	115
Figure 65	(a) Correlation vs. Q_e and (b) PSNR vs. Q_e ; after dithering attack	115
Figure 66	(a) Original fragile watermark, (b) extracted watermark	116
Figure 67	Gaussian attack on the fragile watermark image	117
Figure 68	Image of the patient information watermark	119
Figure 69	Embedding procedures for RONI	122
Figure 70	A block diagram of RONI embedding procedure	123
Figure 71	The extraction procedures for RONI	126
Figure 72	A block diagram of RONI extraction procedure	127
Figure 73	(a) The original image, (b) the watermarked image	130
Figure 74	(a) Original watermark, (b) extracted watermark	131
Figure 75	Watermarked image after cropping attack	132
Figure 76	Extracted watermark (patient information) after cropping attack	133
Figure 77	(a) Correlation vs. block size and (b) PSNR vs. block size; after	134

	cropping attack	
Figure 78	Gaussian attack of different mean values on the watermarked image	134
Figure 79	Extracted watermark (patient information) from HL3 after Gaussian attack	135
Figure 80	(a) Correlation vs. mean and (b) PSNR vs. mean; after Gaussian attack	136
Figure 81	Compression attack of different quality values on the watermarked image	136
Figure 82	Extracted watermark (patient information) from HL3 after compression attack	137
Figure 83	(a) Correlation vs. quality (b) PSNR vs. quality; after compression attack	138
Figure 84	Compression attack of different quality values on the watermarked image	138
Figure 85	Extracted watermark (patient information) from HL3 after dither attack	139
Figure 86	(a) Correlation vs. Q_e (b) PSNR vs. Q_e ; after dither attack	140
Figure 87	Computed and extracted hash comparison	140

Figure 88 Comparison of CRC values; (a) extracted one, (b) computed one 141

List of Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CDMA	Code Division Multiple Access
CFB	Cipher Feed Back
CT	Computed Tomography
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
DWT	Discrete Wavelet Transform
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EPR	Electronic Patient Record
GCM	Galois Counter Mode
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HVS	Human Visual System
ICT	Information and Communication Technology

IDEA	International Data Encryption Algorithm
IDWT	Inverse Discrete Wavelet Transform
IV	Initialiazation Vector
JPEG	Joint Photographic Expert Group
LSB	Least Significant Bit
MAC	Message Authentication Code
MD5	Message Digest Algorithm
MRI	Magnetic Resonance Imaging
MSE	Mean Square Error
NESSIE	New European Schemes for Signatures, Integrity and Encryption
NIST	National Institutes of Standards and Technology
OFB	Output Feed Back
PACS	Picture Archiving and Communication System
PSNR	Peak Signal to Noise Ratio
ROI	Region of Interest
RONI	Region of Non Interest
SHA	Secure Hash Algorithm
UID	Instance Unique Identification
US	Ultrasonic

EXPLORING ENCRYPTION AND WATERMARKING TECHNIQUES FOR SECURE TELEMEDICINE

By
Noor Hussein Haj-Abdullah

Supervisor
Dr. Gheith Abandah, Associate Prof.

Co-Supervisor
Dr. Ali Al-Haj, Associate Prof.

ABSTRACT

Health care institutions need to exchange medical data and cannot work separately without sharing medical information. Telemedicine plays an important role in providing solutions to these challenges. It must be secured so that no modifications are allowed to the medical information during the transfer process over networks. Any implementation in secured telemedicine must meet the following requirements: confidentiality, integrity, and authentication.

Current implementations in secured telemedicine fall into two categories: encryption-based secured telemedicine and watermarking-based secured telemedicine. But the encryption-based techniques do not include embedding the patient information inside the image and the watermarking-based techniques do not provide confidentiality requirement since the image itself is not hidden.

In this thesis, three types of techniques are implemented to meet the secured telemedicine requirements. For the encryption approach, two algorithms are proposed which cipher the header and the image, and achieved the requirements. For the watermarking approach, an algorithm is proposed that hides the data and achieves the security requirements. A third approach is a hybrid technique which combines the two methods, encryption and digital watermarking together to increase the security.

The proposed approaches were implemented and compared with algorithms from the literature in terms of satisfying the three requirements. Comparisons have been made with regard to detecting the attacks, and evaluating the correlation, entropy, peak signal to noise ratio, and execution time performance measurements.

The results showed that the three proposed algorithms achieved the security requirements for secured telemedicine application. However, as an attractive point, the proposed encryption-based

algorithms satisfied the requirements for the header level and the image level. For the execution time, the watermarking technique proved to be superior over the other two approaches. As for the attacks detection, all schemes proved to possess a tamper detection property. In addition, the hybrid algorithm possesses the tamper localization attribute. The results have shown that the developed encryption-based algorithms have the best performance among the three proposed schemes. It also has specificity similar to that of the hybrid algorithm and better than that of the watermarking algorithm.

Chapter 1

Introduction

Since most physicians rely entirely on many types of medical images to diagnose their patients accurately, this led healthcare centers and hospitals to produce continuously a huge amount of medical images. To this end, effective health information management systems are directed by medical field professionals to handle the great amount of information inherited in medical images and this calls out for the need to protect these objects. Research is now focused on finding methods to solve issues related to medical images security. This chapter introduces the importance of telemedicine and its current security tools in addition to different scenarios of the necessary requirements for such a system to be accepted by medical crew. It provides a review of the current approaches in the area of medical image encryption and watermarking techniques and how they are used to secure message transmission. After that, hybrid techniques that allow using encryption and watermarking for the telemedicine operation are presented. We also introduce and present a complete view and discussion of the security issues. a comparison study is presented in the related work between many tested experiments and compared with the proposed project.

1.1 Importance of Telemedicine

The most common form of medical information is medical images such as x-rays, magnetic resonance imaging (MRI), computed tomography (CT scan) and ultrasonic (sonography) (US) imaging. An x-rays medical image is an electromagnetic radiation obtained by placing the patient body in front of the x-ray pulse detector (Jerrold, 2002). MRI is a medical image that uses the property of the nuclear magnetic resonance (NMR) to visualize specific internal structure of the

body in details (Sheil and W. C., 2012). On the other hand, CT scan is a medical imaging modality where slices of specific areas of the body are got from a series of x-ray images taken in different directions (Diffen, 2012). Ultrasonic imaging is used to produce pictures of the inside of the body using high frequency sound waves (Neis et al. 2000).

Medical images play a crucial and important role in the medical applications and need a special safety and acceptable level of confidentiality. This is mainly because serious decisions are done on the information provided by medical images. This research has a primary focus in providing special requirements for medical images that are transmitted from one location to another.

Nowadays, there are many health care institutions such as hospitals and clinics that need to exchange medical data and cannot work separately without sharing medical information. At this point, telemedicine is vital. It combines medicine and information and communication technology (ICT) in the medical world provided that no modifications are allowed to the medical information during the transfer process over networks. The prefix 'tele' is a Greek word that means 'distance', and so, telemedicine is medicine at a distance (Craig and Patterson, 2005). At this point, telemedicine has increased the number of ways in which healthcare can be available and delivered throughout the world instead of the tradition way that the provider and the recipient must be physically present in the same place.

The secure management of electronic medical information or electronic patient record (EPR) that is digitally stored may have an impact on the quality of medical care. Due to high speed growth of computer networks and the internet, this had made sharing digital multimedia objects (images, videos, etc.) very easy. Although recent advances in ICT provide new means to access, handle and move medical information, they disclose their security because of their ease of manipulation

and replication (Flor and Alexander, 2012). For instance, Physicians and radiologists can make decisions about the patient care if they have access to the patients' medical information. On the other hand, disability to access data may affect adversely on the clinical management decisions.

Because secure storage and transmission is crucial in medical image security, many approaches have been developed to protect the medical information from being misused.

1.2 Telemedicine Security Requirements

In general, patient's medical records consist of very sensitive information that should not be accessible to unauthorized people in order to ensure the patient privacy. At the same time patient information should be available whenever required by authorized persons in order to use it for authentication purposes (Ashley, 2002).

The transfer procedure is not easy to achieve since it is governed by three special requirements:

Confidentiality: is to ensure that only the authorized user has access to the information.

Integrity: is to ensure that the data received without any modification as sent by the sender.

Authentication: is to guarantee that the information belongs to the correct patient and from the right source.

Since it is easy to distribute and duplicate digital multimedia objects, this calls out for the need to protect these objects and this is done using encryption and/or digital watermarking techniques.

1.3 Current Approaches and Limitations

The classical way for securely transferring the medical images with the patient report is encryption. Encryption is the process that encodes information in such a way that unauthorized people cannot read it and it is a good choice to solve the problems related to the exchange transaction as shown in Figure 1. A few approaches in the literature used various encryption algorithms in order to ensure secure telemedicine. The image data sent by a sender cannot be understood by people other than a purposed party. However, encryption does not achieve embedding the patient information inside the image.

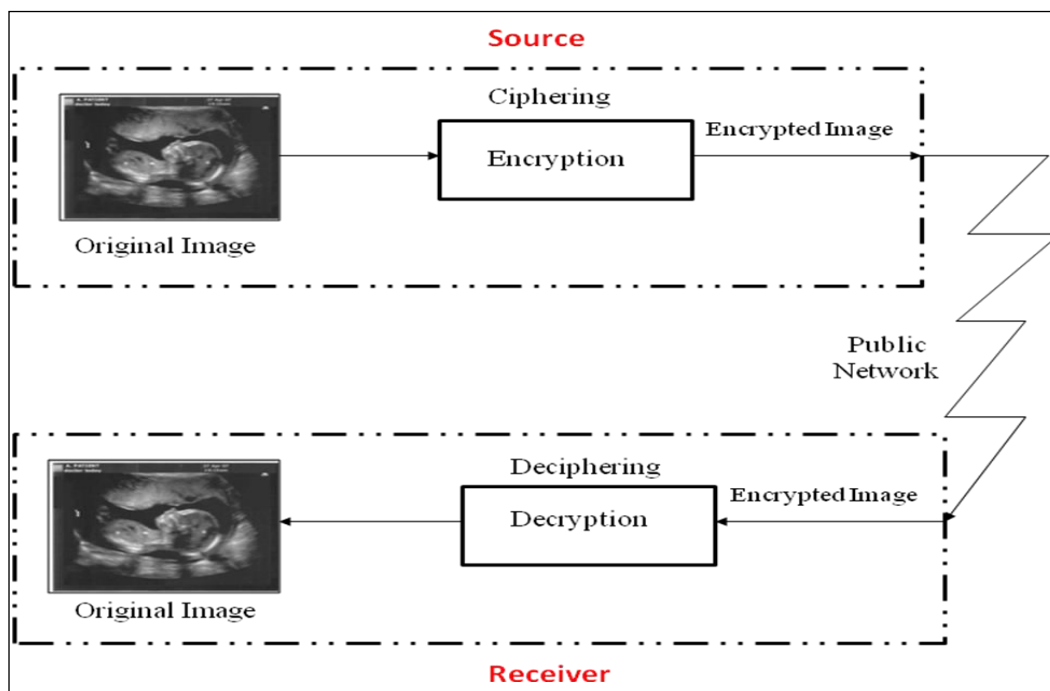


Figure 1. System block diagram for the encryption approach

A modern technique used to hide data is the digital watermarking technique; it achieves integrity and authenticity proofs and shows the identity of its owner while the image contains similar information about the medical report. Digital watermarking is the process that embeds (hides)

data called watermark, into a multimedia object such that the watermark can be detected and extracted from that multimedia object to make sure that this object belongs to a specific party(person, company,...etc). There are many schemes based on different methods of watermarking as shown in Figure 2. The disadvantage of this technique, it does not provide confidentiality requirement since the image itself is not hidden.

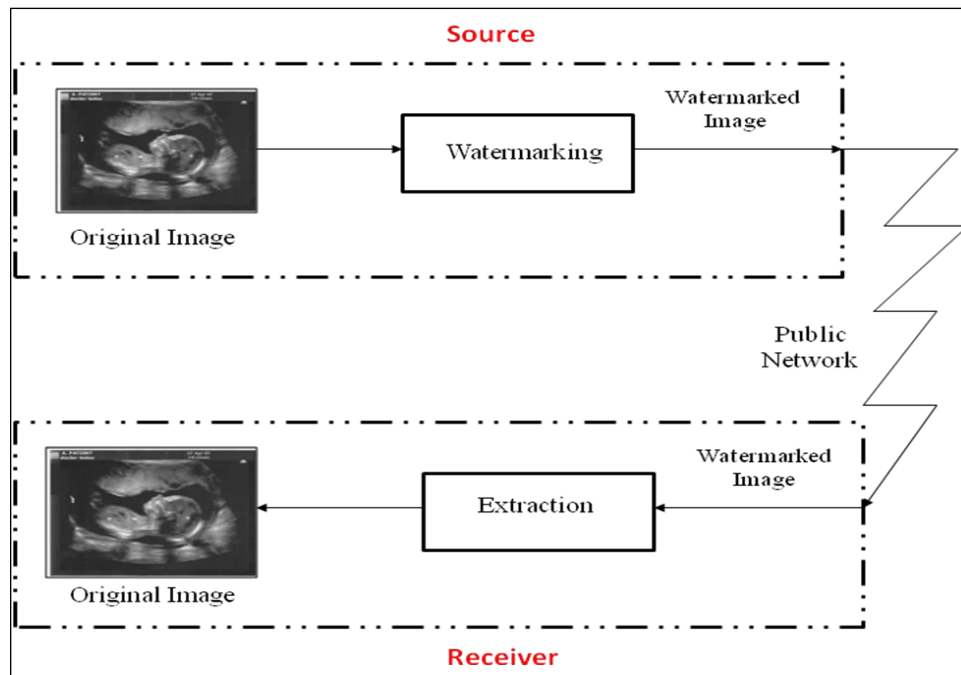


Figure 2. System block diagram for the watermarking approach

The third approach is the hybrid technique which combines the two methods, encryption and digital watermarking together in order to increase the security. In this technique, a cryptographic watermark and the medical information are embedded and hidden in the cover image then the watermarked image is transferred over a public network as shown in Figure 3. On the receiver side, the watermarked image is delivered and passed to the extraction process in order to extract the cryptographic watermarks and the medical information.

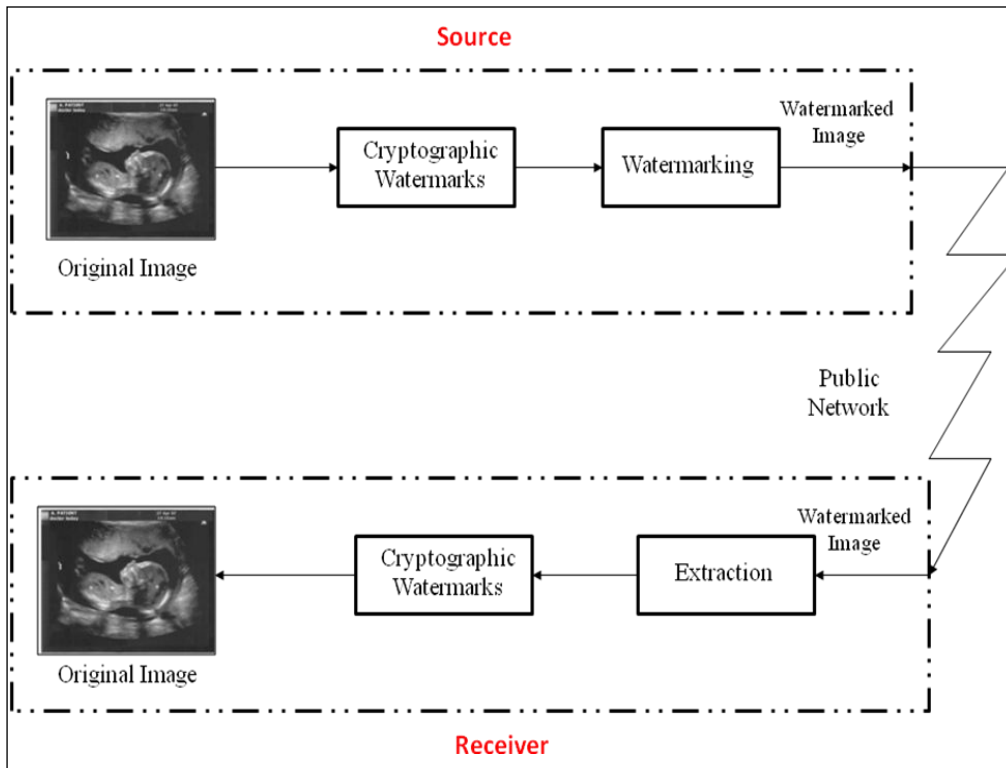


Figure 3. System block diagram for the hybrid approach

1.4 Proposed Approaches

A review by (Coatrieux, et al. 2000) has been selected as the classical motivational ground for the proposed techniques presented in this project. It discusses some security issues in medical information systems and current security tools in addition to different scenarios of the necessary requirements for such a system to be accepted by medical crew. It is worthwhile to mention that, mandates for ensuring health data security have been issued by the federal government such as Health Insurance Portability and Accountability Act (HIPAA), where healthcare infrastructures are obliged to take appropriate measures to guarantee that patient information is only provided to authorized people.

A comparison study is presented between many tested experiments which used different watermarking and encryption algorithms. Those studied algorithms are reviewed and compared with the proposed approaches in this research in terms of satisfying the three requirements.

In the proposed research, the three types of techniques that were mentioned in the previous section are applied and the three requirements are generally satisfied as follows:

- 1) The confidentiality property can be assured by applying the encryption algorithm to cipher the header and the image in order to keep the information secret from unauthorized entities.
- 2) The integrity can be assured through detects the alteration of data by means of one way hashing functions and embedding the hash code computed over the whole image. Then detect the difference between the recomputed hash and the embedded one to proof the property. Also, a fragile watermarks are used to detect any modifications alter the image.
- 3) The authentication guarantees the proof of origin by using public, private and secret keys in the encryption, decryption and watermarking processes. The keys are agreed, known and related to the sender and the receiver.

1.5 Thesis Organization

The reminder part of this thesis is organized as follows;

Chapter 2 gives a brief introduction to cryptographic fundamentals where the most common types are investigated. Next, the main role of cryptography in telemedicine is outlined. In the end of this chapter, the current literature review related to the encryption fields is presented.

Chapter 3 focuses on the watermarking fundamentals for a secured telemedicine. Then the requirements that are needed in this study, the watermarking domains and the algorithms in the literature are presented.

Chapter 4 presents the proposed crypto-based secured telemedicine design and implementation of the algorithms that are used. At the end of this chapter a performance evaluation of the algorithms is presented.

Chapter 5 highlights the proposed watermarking-based for secured telemedicine design and implementation of the algorithm that is used including the embedding and extraction procedures. The performance measurements to be used and its results are proposed.

Chapter 6 deals with the proposed crypto and watermarking-based for secured telemedicine system. The algorithm design and implementation is presented in addition to the discussion and evaluation; there are many evaluation metrics that are used to evaluate the proposed system, in terms of satisfying the three requirements.

Chapter 7 presents the concluding remarks, limitations, and results analysis along with suggestion for future work to develop the research in the future.

Chapter 2

Cryptography: Fundamentals and Application in Telemedicine

Nowadays, digital exchanges of medical images are available throughout the world via the internet. The necessity of fast and secure transmission is vital in the medical world. Various communications and non controlled channels are not secure for sending and receiving information that can be read or modified during their transmission (Popek and Kline, 1979). Accordingly, it is very important to protect this private personal information simply against unauthorized third parties for safe transmission by using cryptography.

In this chapter, a detailed investigation of cryptography fundamentals is viewed. Firstly, an overview of the encryption and cryptography is presented. After that, the main types of crypto schemes are explained. Next, the role that cryptography plays in telemedicine is outlined. Finally, literature review that is related to this area is highlighted with emphasis on the methodology that is carried out by a novel approach in (Kobayashi et al. 2009).

2.1 Introduction to Cryptography and Encryption

Cryptography is the science and study of secret writing in which data can be encoded using codes, ciphers or any algorithms to prevent disclosure of their contents through eavesdropping or message interception, so that only the authorized parties can read it (Denning, 1982). Cryptography is an ancient art; the first documented use of cryptography dates back to circa 1900 B.C when an Egyptian scribe used hieroglyphs in an inscription. David Kahn traces the history of cryptography from Ancient Egypt into the computer age. According to Kahn's, research began from Julius Caesar to Mary, Queen of Scots to Abraham Lincoln's Civil War (Kahn, 1972). Through World War I, the Germans developed the Enigma machine to have

secure communications. Enigma codes were decrypted under the secret ultra project during World War II by the British (Perera and Tom, 2004). Over the centuries new forms of cryptography came after the widespread development of computer communications where it is necessary to encode data when communicating over any non trusted medium.

There are four types of cryptographic schemes typically used to achieve goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, data hashing functions, and digital signatures which are explained in the next subsections. In all cases, the initial unencrypted data is called a plaintext. It is encrypted into ciphertext, which will usually in turn be decrypted into applicable plaintext as seen in Figure 4.

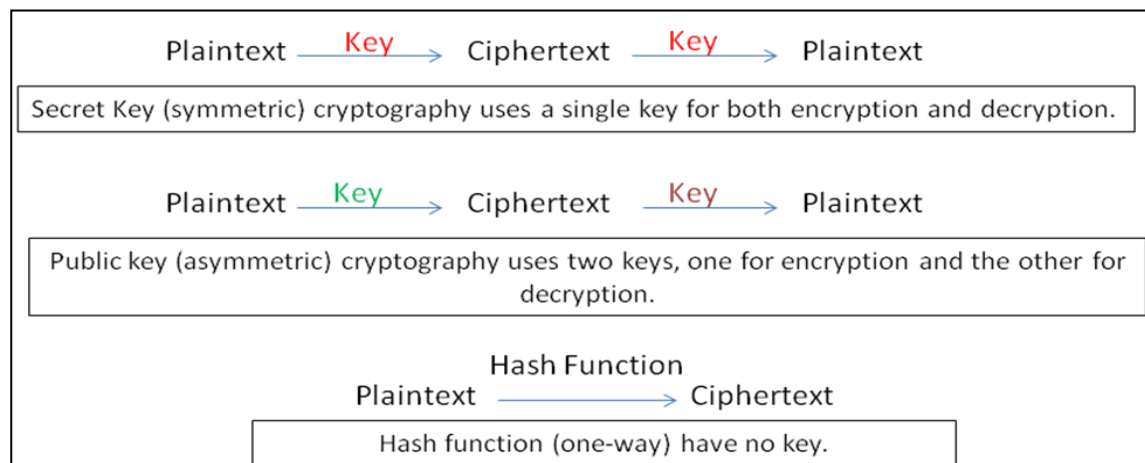


Figure 4. Types of cryptography

Until recent time, cryptography was synonymous with encryption, that is a process of transforming information (the plaintext) into unreadable form (the ciphertext) using a mathematical algorithm and secret information (the encryption key). The process of decryption using a mathematical algorithm related with secret value (the decryption key) that reverses the

process of the encryption algorithm. An encryption algorithm and all its possible keys, plaintexts and ciphertexts are known as a cryptosystem or cryptographic system as shown in Figure 5.

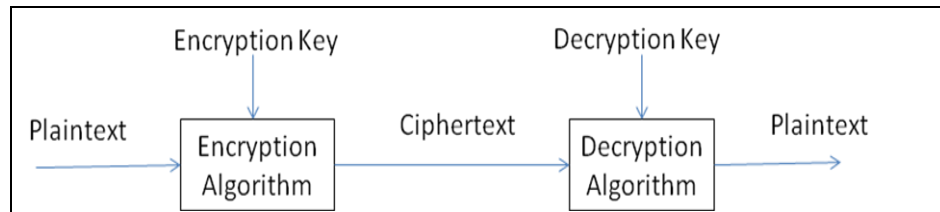


Figure 5. Encryption and decryption process.

2.2 Symmetric Encryption

In symmetric cryptosystems, the same secret key is used for the encryption or decryption process and this key needs to be secure and shared between the sender and the receiver. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message. These systems are very fast, simple, use less computer resources when compared to public key encryption, and have the advantage of not consuming too much computing power, thus providing privacy and confidentiality (Elbirt, 2009).

Symmetric key systems are also known as shared-key, single-key, secret-key, and private-key or one-key encryption. They rely on using some secure method whereby the two communication entities can first agree on a secret key that is known only to them. When any of those entities wants to send a private message to some other entity, another secret key must first be shared. As seen in Figure 6, for a group of three separate entities to send each other private messages, three separate shared keys are required.

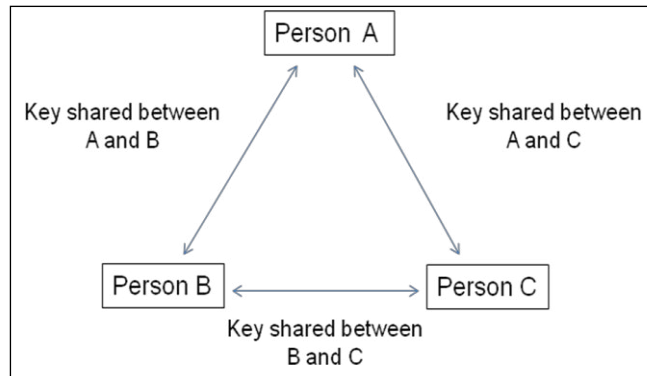


Figure 6. Keys needed for privately communicating with each other.

The symmetric key systems can use either a stream cipher or a block cipher. A stream cipher operates on one bit of plaintext at a time, where a generator called keystream generates a sequence of bits is used with the plaintext bits to produce the ciphertext (Paar and Pelzl, 2009). The block cipher operates on groups of bits, usually groups of 64 bits, and encrypts each block independently. If the final block of the plaintext is less than 64 bits, it is padded with regular pattern of 1s and 0s to make 64 bits block. Block ciphers can operate in one of several modes; the following five are the most important (Chakraborty and Rodriguez-Henriquez, 2008):

- Electronic codebook (ECB) mode is the simplest and most obvious mode where the secret key is used to encrypt the plaintext block to a ciphertext block. In this mode, two identical plaintext blocks will generate the same ciphertext block. Though this is the most common mode of block ciphers, it may be affected by brute-force attacks.
- Cipher block chaining (CBC) mode adds a feedback technique to the encryption process. The plaintext is exclusively-ORed (XOR) with the previous ciphertext block before the encryption. For this mode, two identical blocks of plaintext is never encrypted to the same ciphertext.

- Cipher feedback (CFB) mode is a block cipher as well as a self-synchronizing stream cipher. It allows data to be encrypted in units smaller than the block size. If we were using 1-byte CFB mode, for instance, each incoming character is placed into a shift register the same size as the block, then encrypted, and transmitted. At the receiving side, the ciphertext block is decrypted and the extra bits are discarded.
- Output feedback (OFB) mode is a block cipher similar to a synchronous stream cipher. The OFB prevents the same plaintext block from generating the same ciphertext block by using an independent internal feedback technique.
- Galois/Counter mode (GCM) that has been widely agreed due to its efficiency and performance. It is an authenticated encryption algorithm that gives the key feature of Galois field multiplication to be implemented by parallel processing pipeline instruction. It combines the counter mode of encryption with the new Galois mode of authentication and defines for block ciphers with sizes of 128, 192, and 256 bits (Gueron and Shay, 2013).

A selection of some symmetric key modes used is given in Table 1.

Table 1. Symmetric key systems (Stallings, 1999)

Algorithm	Description
Advanced Encryption Standard (AES)	A block cipher with key size of 128, 192 or 256 bits. Adopted by the U.S. government in 2001. AES uses a secret key cryptography scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen,

	where the block size is restricted to 128 bits.
Data Encryption Standard (DES)	A block cipher with a 56-bit key. Accepted in 1977 by the US National Security Agency (NSA) as the US Federal standard for commercial and unclassified government applications. It has been one of the most widely used encryption algorithms but, as computers have become more powerful, it is now considered to have become too weak.
Triple-DES (3DES)	A variant of DES developed to increase its security. It has many forms; each operates on a block three times using the DES algorithm, therefore effectively increasing the key length. Some variants can use three different keys, the same key three times, or use an encryption–decryption–encryption mode.
International Data Encryption Algorithm (IDEA)	A block cipher with a 128-bit key adopted in 1990 and rated by Schneier. It encrypts data faster than DES, so it is considered to be a more secure algorithm.
Blowfish	A 64-bit simple block cipher invented by Schneier to be fast, compact, easy to implement with a variable-length key of up to 448 bits. It is available freely and intended as a substitute for DES or IDEA, is in use in a large number of products.

Rivest cipher no. 2 (RC2)	A block cipher with a variable-length key of up to 2048 bits. Designed by Ron Rivest in 1987 to replace DES.
Rivest cipher no. 4 (RC4)	A stream cipher with a variable-length key of up to 2048 bits. Developed in 1987 by Rivest. It is widely used in commercial cryptography products.

2.3 Asymmetric Encryption

Also known as asymmetric key encryption, was first published in 1976 by Diffie and Hellmann, it uses pairs of keys: a public key and a private key. The public key is made publicly available used to encrypt messages by anyone who wants to send a message to the person that the key belongs to. The private key is kept secret and used to decrypt received messages and can't be reconstructed from the public key. Both keys are mathematically related and the public key of a key pair is often distributed by means of a digital certificate. If A encrypts a message with his private key then B, the recipient of the message, can decrypt it with A's public key. If anyone knows A's public key then he can send him a message by encrypting it with his public key. So A will decrypt it with his private key. Figure 7 shows the key-based asymmetric algorithm. Well-known asymmetric algorithms are Rivest, Shamir and Adleman standard (RSA), Digital Signature Algorithm (DSA), and ELGAMAL. This method solves the problem of distributing the key for encryption since anyone publishes their public and private keys are kept secret so it seems to be ideally suited for real world use. In addition it achieves a message authentication by allowing the use of digital signatures to verify the message's sender (Hellman, 2002).

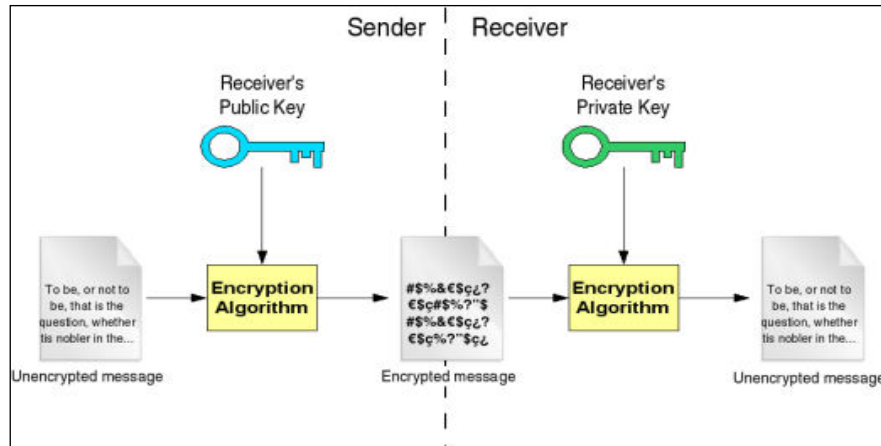


Figure 7. Key-based asymmetric algorithm (Paar and Pelzl, 2009)

On the other hand, public key encryption is slow compared to symmetric encryption and requires more computer resources (Choudhury et al. 1994). There are two factors that are of importance: Firstly, symmetric key operations are usually based on low-level bit manipulation primitives and the standard computer hardware is optimized already for these operations, so they can be performed quickly. But Public key operations are often based on exponentiation of large integers and the modern hardware is not optimized for these operations, it needs special hardware to compute them more quickly. Secondly, public keys must have more bits than secret keys to achieve the same level of security. This is often because shared keys are kept secret between each pair of users, so an attacker has little choice to find the right one. A public key, on the other side, uniquely determines the corresponding private key, so it can be exploited by an attacker trying to find the private key. Therefore, it is impractical to use public key algorithms to encrypt large amounts of data. In practice, they are used to encrypt session keys. Symmetric algorithms are used for encryption and decryption of most data (Roeder et al. 2012). Public key cryptography algorithms that are in use today for key exchange or digital signatures are listed in Table 2.

Table 2. Commercial public key systems (Stallings, 1999)

Algorithm	Description
Rivest, Shamir and Adleman (RSA)	A block cipher RSA uses a variable size encryption block and a variable size key. Published in 1978 and used for both encryption and authentication. Its security is based on the problem of factoring large integers.
Digital Signature Algorithm (DSA)	Algorithm published by the US National Security Agency (NSA) for digital signature standard (DSS), provides digital signature capability for the authentication of messages and not for encryption or key distribution.
ELGamal	Designed by Taher Elgamal, a public key cryptography system similar to Diffie-Hellman algorithm and used for key exchange.
Elliptic Curve Cryptography (ECC)	Algorithm based upon elliptic curves and it can offer levels of security with small keys comparable to RSA and other methods. It was designed for devices with limited compute power and/or memory.

However, in many applications, a public key encryption can be used with secret key encryption to get the best of both worlds. The asymmetric key is used for authentication and when this has been successfully done; one or more symmetric keys are generated and exchanged using the asymmetric encryption (Katz and Lindell, 2007).

2.4 Data Hashing

Hash functions, also called message digests or one-way encryption functions, are algorithms that take a block of data called message and return a fixed-size bit string called the hash value meaning that the output is shorter than the input, such that any change to the data will change the hash value. Although it is easy to compute the hash value for any given message, it is impractical to generate a message that has a given hash (Silva, 2003).

The cryptographic hash functions have several information security applications such as using it in digital signatures, message authentication codes (MAC), fingerprinting (to detect duplicate data), and checksums (to detect data corruption). An important application of hashes that are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver side by calculating a different hash value than the one placed by the sender (Schnorr, 1991). It must take into consideration that two different messages can not have the same hash value, so data integrity is ensured to a high degree of confidence. Hash functions can also be used in the generation of pseudorandom bits and commonly employed by many operating systems to encrypt passwords. Therefore, the functions can provide uniformly distributed hashes even when the keys are chosen by a malicious agent. It is worth to mention that one application of hash function lies in the area of image authentication and watermarking.

As a disadvantage, the cryptographic hash functions tend to be much more expensive computationally compared with standard hash functions.

There are many different types of hash algorithms, with different security properties that are used today. They include:

- Message Digest (MD5) algorithm developed by Rivest in 1991 that produce 128-bit hash value from an arbitrary-length message. It is basically the most widely used version that is more secure than the previous algorithm MD4 but is slower because more manipulation is applied to the data. It has several weaknesses described by German cryptographer Hans Dobbertin in 1996. It has been used in a wide variety of security applications, and is also commonly used to check data integrity (Rivest, 1992).
- Secure Hash Algorithm (SHA): is a family of cryptographic hash functions for national institute of standards technology (NIST) as a secure hash standard (SHS) that describes five algorithms: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively (Jones, 2007):
 - SHA-1: published in 1995 when federal information processing standard came out from the NIST that specified this simple algorithm. It produces a 160-bit hash value. This was designed to be part of the Digital Signature Algorithm.
 - SHA-2: A series of two hash functions, with different block sizes, known as SHA-256 and SHA-512 designed by NSA. They differ in the word size; SHA-256

uses 32-bit words whereas SHA-512 uses 64-bit words. There are truncated versions of each standardized, known as SHA-224 and SHA-384.

- SHA-3: A hash function called Keccak, published in 2012 after a public competition among non-NSA designers. It has the same hash lengths as SHA-2, but its structure differs from the rest of the SHA family.
- Whirlpool: a new hash function, designed by V. Rijmen and P.S.L.M. Barreto. It operates on messages less than 2^{256} bits in length, to produce a message digest of 512 bits. The design of this hash function making it immune to the same attacks faced MD5 and SHA-1 algorithms (Barreto and Rijmen, 2000).

2.5 Digital Signatures

In 1976, Whitfield Diffie and Martin Hellman characterized the concept of a digital signature scheme. A digital signature is a mathematical scheme for proving the authenticity of a digital message, so if the signature is valid, it will give a recipient an indication that the message was created by a known sender (Hellman, 2002). The digital signature for a message is generated as a message digest which is smaller than the message itself and generated using a set of hashing algorithms. Then the message digest is encrypted using the sender's private key to output the digital signature that is attached to the message and sent to the receiver. On the other end, the receiver uses the sender's public key to decrypt the digital signature and obtain the message digest generated by the sender. He uses the same message digest algorithm used by the sender to generate a message digest for the received message, after that he compares both message digest: if they are not the same, this indicates that the message has been tampered with (Buchmann,

2001). Digital signatures provide support for public key cryptography because digital signatures contain the public key of the entity identified in the certificate. Because the certificate matches a public key to a particular individual, the digital certificate provides a solution to the problem of how to find a user's public key and know that it is valid.

So, it can be summarized that the digital signature scheme consists of three algorithms as shown in Figure 8:

- A key generation algorithm: that has two phases. The first phase is a selection of algorithm parameters, and the second phase computes the private key and a corresponding public key.
- A signing algorithm: that produces a signature from the message and a private key.
- A signature verifying algorithm: that the public key and a signature accepts or rejects the message's claim to authenticity.

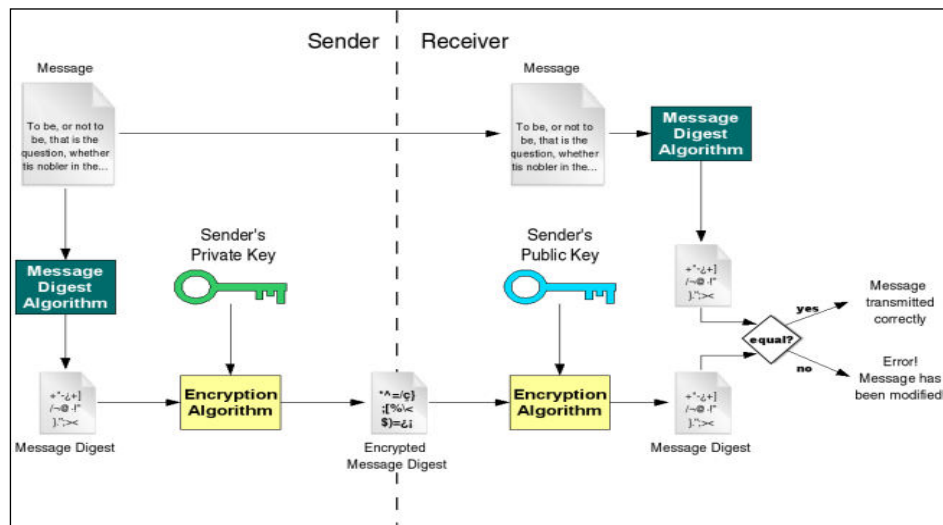


Figure 8. Digital signature signing and verifying algorithm (Paar and Pelzl, 2009)

As applications, digital signatures can be used to authenticate the source of messages (authentication). In many scenarios, the sender and receiver of a message may need to know that the message has not been altered during transmission (integrity). An important aspect is the entity that has signed some information cannot at a later time deny having signed it (non-repudiation).

The digital signature standard (DSS) is the format for digital signatures based on a type of public key encryption method. This standard is also available to the private sector and commercial organizations. There are three algorithms that are suitable for digital signature generation under the DSS standard: the DSA, the RSA algorithm, and the elliptic curve digital signature algorithm (ECDSA). The DSA developed by the United States Federal Government standard for digital signatures. It is a pair of large numbers that are computed according to the specified algorithm (Caelli et al. 1999).

2.6 Cryptography in Telemedicine

Telemedicine completely depends on public network for the transmission of any medical information so there is a need to provide security for the patient data so that unauthorized users can not access or modify the data. As mentioned before, there are some requirements needed for any communication channel, including the following:

- ***Confidentiality***: ensuring that no one can read the image except the authorized receiver.
- ***Integrity***: ensuring that the received image has not been altered in any way from the original. By use hashing.

- **Authentication:** is to ensure of the person's identity and the originator of data. By use digital signature.

Therefore, to achieve the privacy or security requirements of information, several cryptography mechanisms incorporated into healthcare applications insure the secure access to the data channel. The related works in the next section introduces some methodologies regarding the encryption-based secured telemedicine works. For example, one method of authentication is for the sender and recipient to share a secret key. The sender uses the key, to encrypt the message, which is included with the data transfer and the receiver uses the key to decrypt the encrypted data. If the result matches the plaintext message, this provides an assurance that it was sent by the other key owner, and thus a proof of its authenticity.

2.7 The DICOM Standard

The best known approach is Part 15 of the DICOM standard, in which the digital signature information is stored in its header. Some applications of this approach have already been examined. The contents of the DICOM standard concentrate on a definition of an exchange format for medical image data. Today, virtually all modalities that are used in radiology, such as CT, MRI, and Ultrasound supports the DICOM standard for the exchange of images and related information. Also, it defines the network oriented services, image transmission, query of an image archive (PACS), print (hardcopy), data interchange protocol, digital image format and requirements for conforming devices and programs (Bidgood et al. 1997).

A DICOM image consists of data elements named attributes which contain the image related information: patient information that is called DICOM directory (such as name, sex,

identification number), modality and imaging procedure information (such as device parameters, calibration, contrast media), and image information (such as resolution, windowing). For each modality, DICOM actually defines the required and optional attributes. However, this flexibility is viewed as a weakness point of the DICOM standard because in such objects, required fields are missing or contain incorrect values (Cao et al. 2003). These problems affect on the data exchanging process.

The DICOM network services were written in terms of service-class-users (clients) and service-class-providers (servers); such that when two DICOM applications want to exchange information, they have to establish a connection and agree on the following issues (Mildenberger et al. 2002):

- Determine the client and the server.
- The DICOM services to be used.
- The format of transmitted data (compressed or uncompressed).

If both sides agree on the previous mentioned parameters, in this case the connection will be established.

- **Part PS3.15 and Use of Encryption**

This part of the DICOM standard defines security and system management profiles to which implementations specify conformance. They are used by several standard protocols, in addition to their use in a system that uses DICOM standard protocols for information interchange (PS 3.15-2001). Although achieving any level of security needs appropriate security policies, the DICOM standard does not address issues of security

policies. It only provides mechanisms to implement security policies related to the interchange of DICOM objects between application entities which agree to some level of trust that their communication partners will ensure the confidentiality and integrity of data under their control (Hamilton, 1992). This standard provides mechanisms for application entities to securely authenticate each other and detect any tampering with the messages exchanged. As a result, application entities can choose any of these mechanisms, relying on the level of trust they place in the communications channel (Wong et al. 1995).

The basic DICOM media security profile allows encapsulation of a DICOM file into a secure DICOM file so that, the three aspects of security: the confidentiality, integrity, and authentication are defined (Cao et al. 2003). Moreover, the PS 3.15 addendum which called attribute level confidentiality security profiles makes use of the previous aspects.

Part PS3.15 of the DICOM standard adopted the current data encryption techniques to be used with the DICOM data. These techniques serve three purposes: data encryption, data origin verification, and data integrity verification. In this profile, using encryption algorithms such as RSA, AES, and Triple-DES are accepted by the standard for converting original data into a protected format. Also, data integrity algorithms such as SHA have been adopted in DICOM to solve the problem related to the changes of the data or replacing the original attribute in the DICOM file with another during the transmission. Therefore, validating data origin is done using digital signatures. The key point of any digital signature is verifying the identity of the data and its authenticity (Zhou et al. 2000).

- **De-Identification:** The DICOM realizes de-identification concept as protecting the confidential attributes by either removing or encrypting them, while defines the inverse concept re-identification by removing the data protection (Zhou and Haung, 2001).

The standard aims to divide the de-identification process into several attribute confidentiality profiles. Each profile addresses certain parts of security and attributes. DICOM PS3.15 defines the basic application level confidentiality profile to hide confidential data. Application level confidentiality profile acts as a de-identifier if it protects all instances of the attributes that listed in Table 3 and may be used by unauthorized entities to identify the patient. An application conforming to this profile may take all instances of the encrypted attributes data set, encrypt their original values with a standard encryption algorithm and store the encrypted result in the tag (0400,0550) modified attributes sequence, however the values in the original locations are replaced with dummy ones. PS3.15 does not demonstrate what and how to remove, but it is the de-identifier responsibility to ensure that all identifying information is removed (Pianykh, 2012).

The DICOM supplement 142, entitled with “Clinical Trial De-identification Profiles,” provides more explanation on DICOM de-identification that is used for clinical research, and teaching files.

- **Re-Identification:** On the other hand, a re-identification process is done to find the confidential attributes. This operation is efficient to remove the protection from a protected instance, assuming that the recipient keys that are required for the decryption of the encrypted attributes are available (Pianykh, 2012). Table 3 lists all the attributes’

names along with their tags (DICOM Supplement 55, accessed March 2013). The tag is a kind of metadata helps describe the confidential attribute and found its location.

Table 3. Basic application level confidentiality profile attributes

Attribute Name	Tag
Instance Creator UID	(0008,0014)
SOP Instance UID	(0008,0018)
Accession Number	(0008,0050)
Institution Name	(0008,0080)
Institution Address	(0008,0081)
Referring Physician's Name	(0008,0090)
Referring Physician's Address	(0008,0092)
Referring Physician's Telephone Numbers	(0008,0094)
Station Name	(0008,1010)
Study Description	(0008,1030)
Series Description	(0008,103E)
Institutional Department Name	(0008,1040)
Physician(s) of Record	(0008,1048)
Performing Physicians' Name	(0008,1050)
Name of Physician(s) Reading Study	(0008,1060)
Operators' Name	(0008,1070)
Admitting Diagnoses Description	(0008,1080)
Referenced SOP Instance UID	(0008,1155)

Derivation Description	(0008,2111)
Patient's Name	(0010,0010)
Patient ID	(0010,0020)
Patient's Birth Date	(0010,0030)
Patient's Birth Time	(0010,0032)
Patient's Sex	(0010,0040)
Other Patient Ids	(0010,1000)
Other Patient Names	(0010,1001)
Patient's Age	(0010,1010)
Patient's Size	(0010,1020)
Patient's Weight	(0010,1030)
Medical Record Locator	(0010,1090)
Ethnic Group	(0010,2160)
Occupation	(0010,2180)
Additional Patient's History	(0010,21B0)
Patient Comments	(0010,4000)
Device Serial Number	(0018,1000)
Protocol Name	(0018,1030)
Study Instance UID	(0020,000D)
Series Instance UID	(0020,000E)
Study I	(0020,0010)
Frame of Reference UID	(0020,0052)
Synchronization Frame of Reference UID	(0020,0200)

Image Comments	(0020,400)
Request Attributes Sequence	(0040,0275)
UID	(0040,A124)
Content Sequence	(0040,A730)
Storage Media File-set UID	(0088,0140)
Referenced Frame of Reference UID	(3006,0024)
Related Frame of Reference UID	(3006,00C2)

2.8 Literature Review

Regardless of the importance of integrity and authenticity for medical images, only recently this area of research has been classified. There are a number of works done in this field. One of the earlier works was released in 1995, but it was only after 1999, the medical image integrity and authenticity got a great concern (Cao et al. 2003). Throughout this section, an overview of the related works is highlighted.

2.8.1 Encryption-based Only Schemes

Some related works that are based on applying encryption techniques in order to achieve a secure telemedicine are outlined in this section as shown in Table 4 below.

Table 4. Comparison study related encryption techniques

Projects	Encryption Techniques					
	Public-Key Cryptography		Private-Key Cryptography		Hashing	Stream Cipher
	RSA	DSA	DES	AES		
(Norcen, et al. 2003)				✓		
(Alvarez, et al. 2007)				✓		
(Brahimi, et al. 2008)				✓		
(Puech, 2008)			✓	✓		✓
(Kobayashi, et al. 2009)		✓		✓	✓	
Proposed Algorithm I		✓		✓	✓	
Proposed Algorithm II		✓		✓	✓	

Norcen (Norcen, et al. 2003) introduces an efficient techniques for achieving a confidential storage and transmission of medical image data. Two methods of partial encryption techniques based on advanced encryption standard (AES) are discussed. The first scheme encrypts a subset of bitplanes of plain image data that encrypts all packets corresponding to two consecutive layers and reconstruct the resulting bitstream to measure the peak signal to noise ratio (PSNR) quality of the resulting images. Whereas the second scheme encrypts parts of the joint photographic expert group (JPEG2000) bitstream in order to investigate whether resolution progressive order or layer progressive order is more appropriate for selective JPEG2000 bitstream encryption. They decided to use angiograms as a sample test images since they represent an important class of medical image data. Simple cipher text-only attacks are applied against both encryption schemes and the results for both techniques indicate that encrypting only a fraction of the

original data between 20% and 50% is sufficient to provide high confidentiality. This large difference of fractions is due to the fact that important visual features are found at the beginning of the embedded JPEG2000 bitstream and may be protected effectively while the visual features are spread across bitplanes.

According to (Alvarez, et al. 2007), analyzing the security of Rajendra Acharya et al. storage system (Rajendra, et al. 2003), that was proposed in 2003. The authors discuss how to improve the secure transmission and efficient storage of medical images embedded with patient information and encrypted with an algorithm developed by Rajendra. They point out that the Rajendra's method is very weak encryption algorithm for two reasons. First, there is no secret key. Therefore, it is not a correct encryption approach, but an encoding approach. Second, the algorithm is a simple substitution cipher, meaning that the same plain character will always be encrypted into the same cipher character under the same key. They suggested a simple method of encrypting medical images resorting to publicly available standard algorithms such as AES and triple data encryption standard (DES), so the results give a truly secure system used in practice. Their view that all of these algorithms use a secret key of variable length which makes unfeasible for a brute force attack to try all possible combinations of the secret key. They are very fast and easy to implement.

Brahimi, et al. (2008) captures a modified novel selective image schemes based on JPEG2000. The method consists of two partial encryption techniques where partial encryption is combined to a permutation of selected codeblocks in the first approach. In the second approach, encryption is combined to a permutation of the packets headers of corresponding where all packets headers are separated from the bodies' packets. Then process a cyclic permutation of all the header

packets, when encryption process is done on the only bodies of selected packets. They employ AES in cipher feed-back (CFB) mode for data encryption. For the performance tests they evaluate the selective encryption combined to the packets headers permutation and obtain best PSNR for neurological and hematological images. For the security evaluation, they exploit a built-in resilience functionality to simulate a bitstream based replacement attack. The results of decoding operation show no visual information appear on the images. For an advantage: The scheme works with any standard ciphers and introduces negligible computational cost. Besides it keeps the compression ratio unchanged and doesn't degrade the original error robustness.

Another approach is (Puech, 2008) who took into consideration how standard encryption algorithms provide security to medical imagery. The images encrypted in their source codes in order to apply this functionality at the application level and the functionalities of encryption are inserted at the software level. As the test applied on the original images by a stream cipher algorithm with a 128-bit key, the results show that the homogeneous zones are no longer visible either in the images or the histogram and the calculations which make it up are small in number. The images is also encrypted by DES and AES as another test to prove that the stream cipher algorithm is better than AES, and assuring that DES is very poor algorithm. The main advantage is the ability of the approach to link several types of coding in one algorithm.

2.8.2 Encryption-based Approach (Kobayashi, et al. 2009)

An important novel approach proposes by (Kobayashi, et al. 2009), provides integrity and authenticity of medical images issue. This paper has been selected as the classical motivational ground for the proposed techniques related to the encryption field presented in this project. It is distinct from the other approaches, and provided a strong point in the trustworthiness of the

medical images without compromising their quality. The method has the feature of using many specifications from the DICOM standard, making it easier to be applied.

The encryption process takes here three inputs: header data to authenticate patient data, pixel data to validate the image itself, and authentication entity data for determining the authorship of the image. On the other hand, the outputs are: the encrypted pixel data and the security data that was used for encrypting the image (digital signature). Besides, the algorithm was applied on multiframe images and performed a different encryption for each frame. For this approach, a Java application was developed in Eclipse platform and a basic algorithm has been proposed and implemented, using the DICOM header data to calculate the key and initialization vector (IV) needed for the encryption process related to the original pixel data. The IV is a fixed size input to the cryptographic primitive that is typically required to be random to achieve semantic security. For block ciphers, the use of an IV is described by so called modes of operation and it is called the nonce which used to avoid replay attack. The encryption process tracking is shown in Figure 9 represents the block diagram and the main parts and the relations between the different blocks.

Encryption Flow at the Sender Side

Firstly, a part of the header is hashed by a Whirlpool method, only the SOP instance unique identification (UID) and patient name were chosen to be hashed, generating an output of fixed size of bits is used as the key and IV of the encryption algorithm. After a complete data encryption process, the results are the ciphertext and the authentication tag of the pixel data. It is worth to mention that the encryption algorithm of choice was AES in Galois counter mode (GCM) with a key size of 256 bits and an IV of 96 bits. The tag is then signed with the private key of the image owner by the elliptic curve digital signature algorithm (ECDSA) with a 256-bit

key, and generating a signature that is stored in the image header itself together with the owner public key.

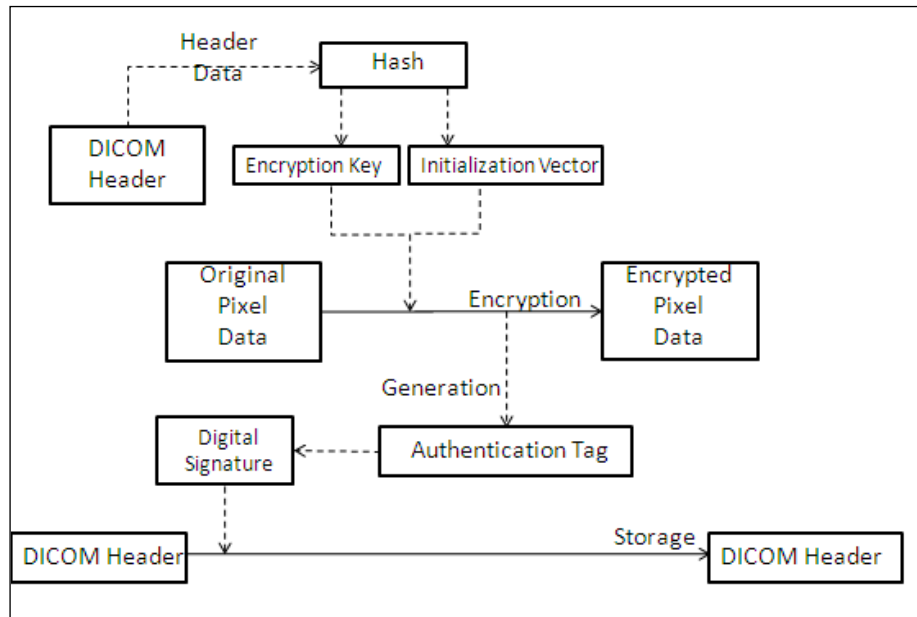


Figure 9. Signing and encryption process

Decryption Flow at the Receiver Side

The decryption and security verification of the proposed algorithm are proposed in Figure 10, where the same header parts used in the encryption are retrieved and hashed to generate the key and the IV. Then, the original pixel data is recovered from the encrypted data, in addition to its authentication tag that is matched against the signature stored in the header to verify the integrity and authenticity of the image. Note that for multislice images, each slice is encrypted independently, and they are stored in separated files. For multiframe images, the encryption for each frame and the result is stored in one single file.

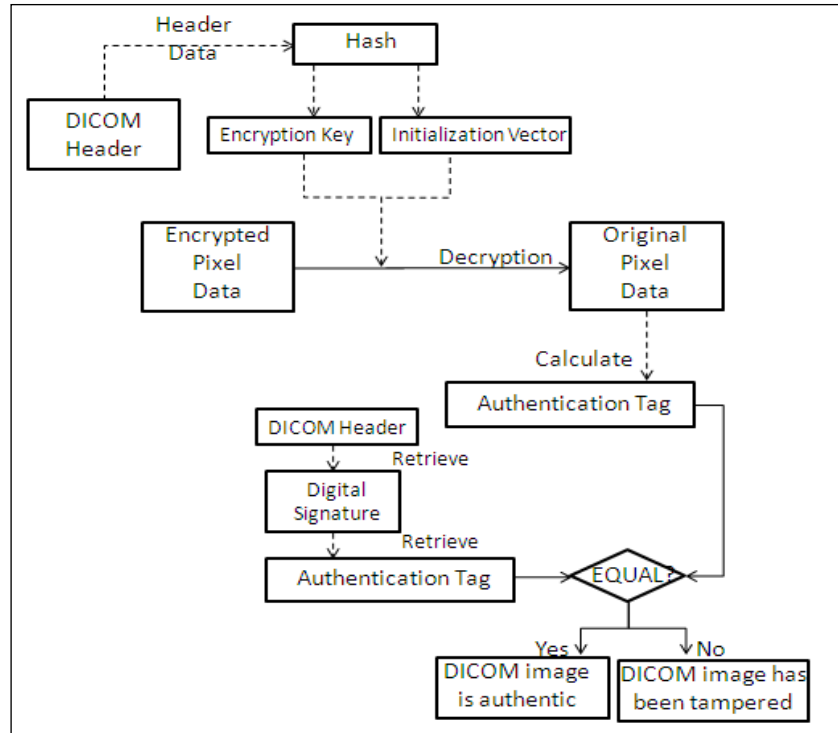


Figure 10. Decryption and verification process

Performance Evaluation of the Algorithm

The evaluation was done using two metrics: correlation and performance. Correlation displayed that each frame holds little similarity with its encrypted pair and with its consecutive frames. However, performance evaluation showed good results although it must be improved in order to minimize the times needed to encrypt and decrypt multislice images.

For drawbacks of this algorithm, it must be asserted that this approach does not achieve confidentiality, as the key for the decryption is stored in the image header. And, if the key and/or the image are tampered, it would be very hard to retrieve the original patient data, maintaining the privacy. Also, it needs an optimization due to implementation issues in order to improve the performance for both cipher and decipher operations. Moreover, it has a strict integrity that when the encryption key is tampered, the decryption process will not be applied anymore.

Chapter 3

Watermarking: Fundamentals and Application in Telemedicine

Due to the rapid growth of the Internet in the past several years which increased the digital multimedia evolution to the public, the problem of protecting digital information becomes more serious. Many copyright owners are concerned about any illegal duplication of their data or unauthorized use to be protected from detecting their work. Of the many schemes used to protect the media, digital watermarking is possibly the modern one that has received most interest. Digital watermarking is the process that embeds data called watermark, into a multimedia object such that the watermark can be detected and extracted from that multimedia object to make sure that this object belongs to a specific party. Watermarking has the power to embed records into an image, such that the host media is not noticeably degraded to the human eye. There are other digital watermarking applications, but here we are talking about hidden annotations application for secured telemedicine. In the medical applications, watermarks might be used for embedding patient records.

3.1 Watermarking Systems

In general, digital watermarking involves three major operations: watermark selection, watermark embedding, and watermark extraction as shown in Figure 11. For both operations, embedding and extraction, a secret key is needed to secure the watermark as in Figure 12.

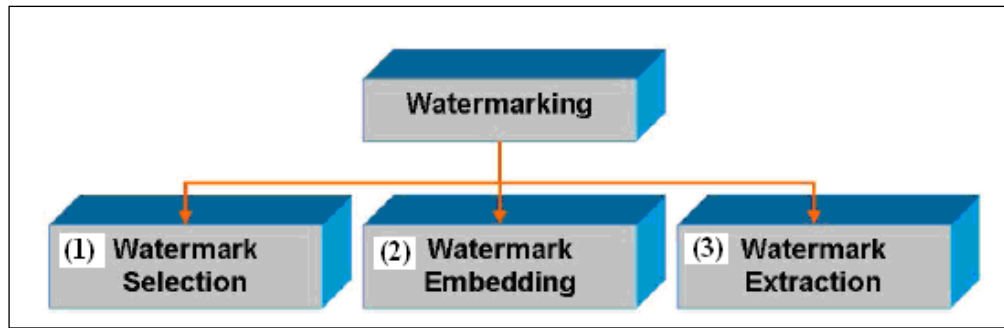


Figure 11. Watermarking Processes

Watermark Selection: in this step, choosing the appropriate image to be embedded into an image. There are two types of watermarks that can be embedded into an image and they are (Kumar et al. 2013):

- **Pseudo-Random Gaussian Sequence:** A Gaussian sequence watermark is a sequence of numbers comprising 1 and -1 and which has equal number of 1's and -1's is termed as a watermark. It is termed as a watermark with zero mean and one variance. Such watermarks are used for objective detection using a correlation measure.
- **Binary Image or Grey Scale Image Watermarks:** Some watermarking algorithms embed meaningful data in form of a logo image instead of a pseudo-random Gaussian sequence. Such watermarks are termed as binary image watermarks or grey scale watermarks. Such watermarks are used for subjective detection.

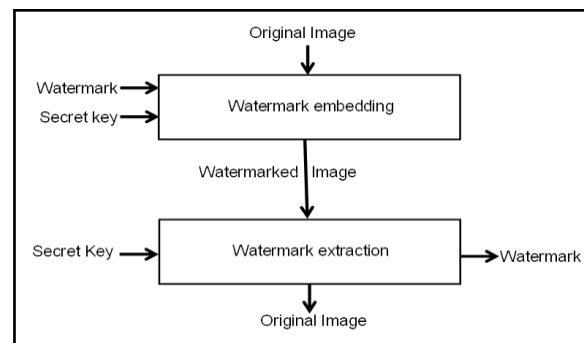


Figure 12. Generic watermarking scheme

Watermark Embedding: after selecting the watermark, it can be embedded using different techniques such as the spatial domain and the frequency domain techniques. Detailed description of these techniques is given in sections 3.3 and 3.4.

Watermark Extraction: the watermark can be extracted from the watermarked image by using the same technique used in the embedding. Extraction can be done with the presence of the original image, or the absence of the original image depending on the watermarking system. A private (non-blind) watermarking system requires that the original signal be present at the decoder in order to extract watermark information. In contrast, a public (blind) watermarking system does not require access to the original signal in order to decode the watermark (Cox et al. 2001).

3.2 Watermarking Requirements

Watermarking has the following requirements that represented by (Trichili et al. 2002):

- ***Imperceptibility (Visibility):*** The watermark should not be visible in the image under typical viewing conditions and not affect the quality of the original image. As it is discussed more clearly in section 3.2.1.
- ***Robustness:*** The watermark can still be detected after the image has undergone linear or nonlinear image processing operations intentionally or unintentionally like compression, cropping, dithering, rotation and noise. So the watermarks should be robust against variety of such attacks that are explained more in section 3.2.2.
- ***Capacity:*** The watermarking technique must be capable of allowing multiple watermarks to be inserted in an image, with each watermark still being independently

verifiable and can be successfully detected during extraction. However, the capacity is the maximum amount of information can reliably be hidden in the signal and can be measured by bit per pixel (bpp).

- **Security:** Watermarking technique is truly secure if knowing that exact algorithm for embedding and extracting, the watermark does not help an unauthorized party to detect the presence of the watermark or remove it without knowing the secret key.

All of these specifications must be taken into consideration when applying any digital watermarking technique. The relationship between robustness, capacity, and invisibility is shown in Figure 13 as a triangle. When one axis is fixed, then the other two axes are oppositely proportional.

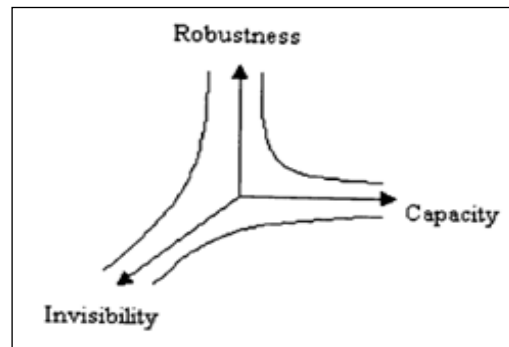


Figure 13. Watermarking

properties

3.2.1 Imperceptibility

Performance of the watermarking scheme is measured mainly with respect to: imperceptibility and robustness against attacks. Where, imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked image, the PSNR is usually used. It can be measured using equation 1 as:

$$\text{PSNR} = 10 \cdot \log_{10} (\text{MAX}_i^2 / \text{MSE}) \quad (1)$$

Where max I is the peak value of the original image (usually 255 for 8 bit grey-scale image).

About the mean square error (MSE) can be measured by equation 2:

$$MSE = \frac{1}{m \ n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (2)$$

Where I and K are matrices that represent the images being compared. And the two summations are performed for the dimensions "i" and "j" where I(i,j) represents the value of pixel (i,j) of image I.

3.2.2 Robustness

In most watermarking applications, the watermarked image is likely to be processed in some way before it reaches receiver. An embedded watermark may unintentionally or intentionally be affected by such processing. An attack is a signal processing operation that may remove or degrade the quality of the embedded watermarks .It can be in general classified as: intentional attacks and non-intentional attacks (Shukla and Sharma, 2012). So far, an important side of any watermarking scheme is its robustness against attacks. As a measure of robustness, the correlation is used by equation 3 and equation 4, where C.C is the correlation coefficient:

$$C.C = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}} \quad (3)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (4)$$

The parameter x and y are the gray scale pixel values of the original and encrypted images.

There are two classes of attacks: removal attacks and geometric attacks.

- The removal attacks aim on the removal of the watermark information from the watermarked image without affecting the security of the watermarking scheme. This category includes: JPEG compression, noise (Gaussian, white, salt & pepper), low pass filter, and dithering. These types may damage the watermark information only without causing a complete watermark removal.
- In contrast to the previous type of attacks, the geometric attacks do not indeed remove the embedded watermark itself, but intend to corrupt the watermark detector synchronization with the embedded information. Also, this category includes: cropping, rotation, and resizing.

The required properties of the watermark strongly depend on the application; this means that the appropriate evaluation criteria is application dependent. Benchmarking is a reasonable means of comparing watermarking system. It is worth to mention a universe benchmark called stirmark that is able to give a single and scalar score to a proposed watermarking system, knowing that no benchmark can ever be relevant to all watermarking systems and applications (Mitrea et al. 2005).

3.3 Classification of Watermarking Techniques

Watermarking techniques can be classified as in Figure 14 according to the type of document (text, image, audio or video), or according to the working (spatial or frequency) domain. Also they can be classified according to the human perception (imperceptible, perceptible, and dual). The invisible watermark can be robust that doesn't break easily besides intended to authenticate original authorship while fragile watermark that breaks easily and intended to authenticate integrity of image. The invisible robust watermark could be public, private, or semi-private. Thus

the private watermarking needs the original host or the cover image to extract the embedded watermark from the watermarking image, but the public extracts without the need of the cover image Cox et al. 2001).

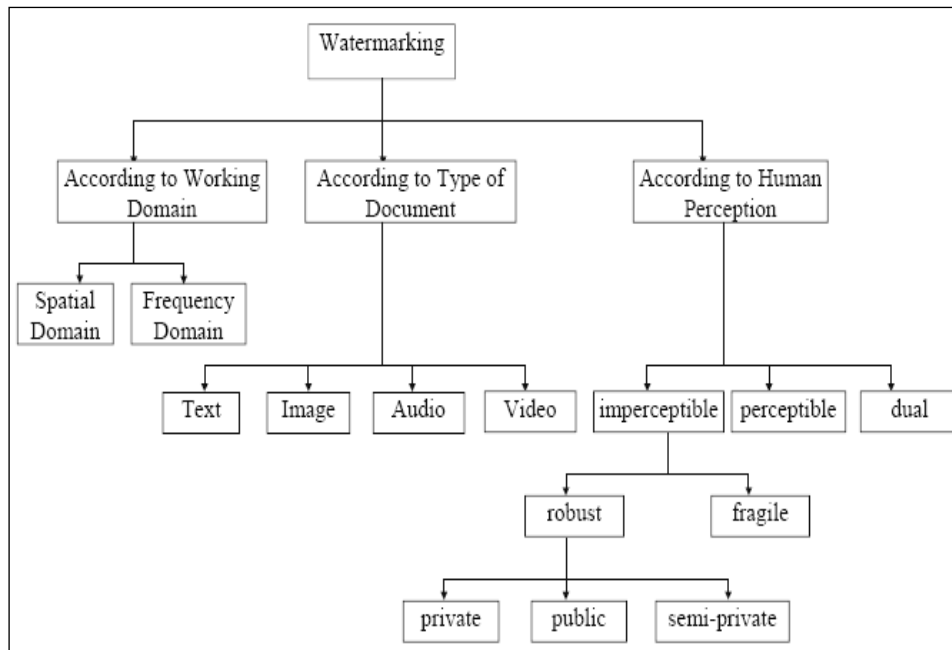


Figure 14. Watermarking classification

3.3.1 Spatial Domain Watermarking

Images (cover objects) can be represented in spatial domain and frequency domain. In the spatial domain images, images are represented by pixels. Simple watermarks can be embedded in the spatial domain of images by modifying the pixel values or the LSB values. This is easy to implement, but it is not robust enough to protect watermark information against different kinds of attacks such as the lossy compression (Swanson et al. 1996). The spatial domain methods are applicable for fragile watermark scheme.

Some authors focus on the spatial domain which is the most straightforward simple scheme for the digital watermarking and the common simplest technique in this domain is the least significant bit (LSB) in which the watermark to be embedded is placed in the LSB of the host image. Other techniques in this domain are: correlation based techniques. One advantage, for spatial domain is lower complexity as no transform is used. However, the human visual system is not realizing every small variance in color, so the processing of small difference in the LSB for example will not be noticeable (Lin and Chang, 2001). As a disadvantages, this technique is simple, lacks the robustness against the attacks. It can survive any addition of noise. Moreover, lossy compression is used to overcome the watermark; the attack is to set all the LSB bits to '1' fully overcoming the watermark at the cost of negligible visible effect on the cover image (Cruz et al. 2008). In addition to, when the algorithm is discovered, it would be very easy for an intermediate party to change the watermark.

- **Least Significant Bit Substitution Technique**

The common, simplest, and straight-forward technique in the spatial domain is LSB, in which that the watermark to be embedded is placed in the LSB of the host image as shown in Figure 15 below.

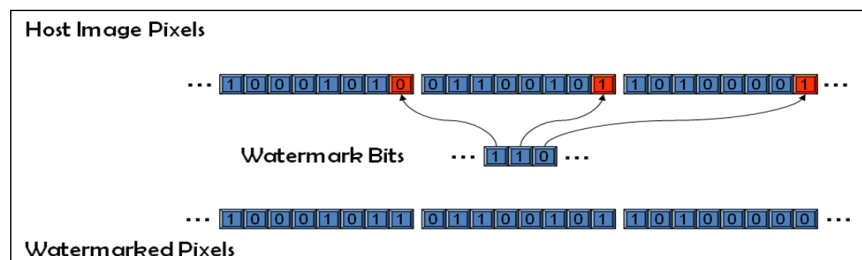


Figure 15. Least significant bit substitution technique

Another scheme is a LSB with secret key, since inserting the watermark bit at random pixels, dependent upon a key will enhance the watermark secrecy. The user selects a secret key and a sequence of pseudo-random numbers is generated using the key as the seed (Skicioglu, 2003).

As a disadvantage, LSB substitution is not robust against attacks to remove the watermark. Such an example a simple modification of the image by setting all LSBs of all pixels to '1' or resetting with '0' can defeat the watermark. Also transcoding (such as converting the image into lossy JPEG file) can also remove the watermark effectively.

- **Correlation Based Techniques**

Another technique is the correlation-based technique, to utilize the correlation characteristics of additive pseudo-random noise patterns applied to an image (Langelaar et al. 2000). Related to equation 5 below, a pseudo-random noise (PN) pattern $W(x, y)$ is added to the host image $I(x, y)$:

$$I_w(x, y) = I(x, y) + k * W(x, y) \quad (5)$$

Where, K the gain factor, and I_w the output watermarked image. It is worth to notice that, when k is increasing, the robustness of the watermark is increasing too.

When recovering the watermark, the same pseudo-random noise generator algorithm is defined its correlation with the noise pattern and the watermarked image are seeded with the same key. If the correlation exceeds some threshold T , then the watermark is recovered and a single bit is set. And so it could be expanded to multiple bit messages by

embedding multiple watermarks into the image by dividing the image into blocks and applying the same process on each block.

According to the spatial domain, an improvement is done on the basic algorithm where the step that threshold being used for determining a logical “1” or “0” can be removed by applying two independent PN sequence and an independent seed for each patterns. Which is added to the detail coefficients as mentioned in equation 5. One pattern is designated a logical “1” and the other a “0”. Throughout detection, the pattern with the higher resulting correlation is used. The recovery procedure is repeated through the entire PN sequence till recovering all the bits of the watermark (Dey et al. 2012).

3.3.2 Frequency Domain Watermarking

According to the frequency domain, images are represented in terms of their frequencies. It transfers an image to its frequency representation and the image is segmented into multiple frequency bands. The watermark spread throughout the image not just holding on an individual pixel. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients. Then inverse transforming the marked coefficients forms the watermarked image. The embedded watermark in the frequency domain of a signal can provide more robustness than spatial domain. It is strong against attacks like compression, cropping where spatial domain is not. Many transform techniques are available; such as discrete wavelet transform (DWT). The use of frequency based transforms allows the direct understanding of the content of the image and the hue saturation value (HVS) characteristics can be considered when it is time to decide the intensity and position of the watermarks to be applied to a required image (Mistry, 2010).

- **Discrete Wavelet Transform Technique**

After taking an overview of what is meant of watermarking and explaining the two main domains, now talking about what are the wave characteristics and what is meant by DWT. A wave is an oscillating function of time or space and is periodic as in Figure 16 (a), a wavelet is localized wave. They have their energy concentrated in time or space and are suited to analysis of transient signals as in Figure 16 (b). The wavelet characterized by its scale due to compress or extend the mother wavelet where the small scale (compress) captures high frequency and the large scale (extend) captures low frequency. Also, shifting the wave along signal so the wavelet coefficient measures similarity between signal and scaled, shifted wavelet (Misiti et al. 2006).

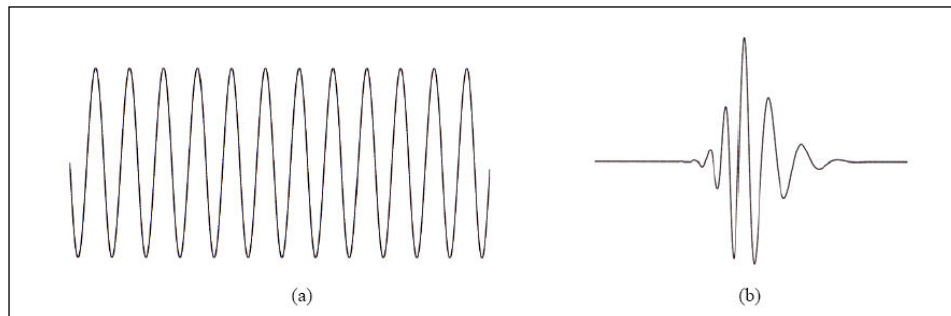


Figure 16. Wavelet analysis

In Figure 17 many types of wavelet transform are presented. (Pickholtz et al. 1980) defined spread spectrum as: "Spread spectrum is a means of transmission in which the signal occupies a band width in excess of minimum necessary to send the information, the band spread is accompanied by a code which is independent of the data, and a synchronized reception with the code at the receiver is used for despreading and subsequent data recovery".

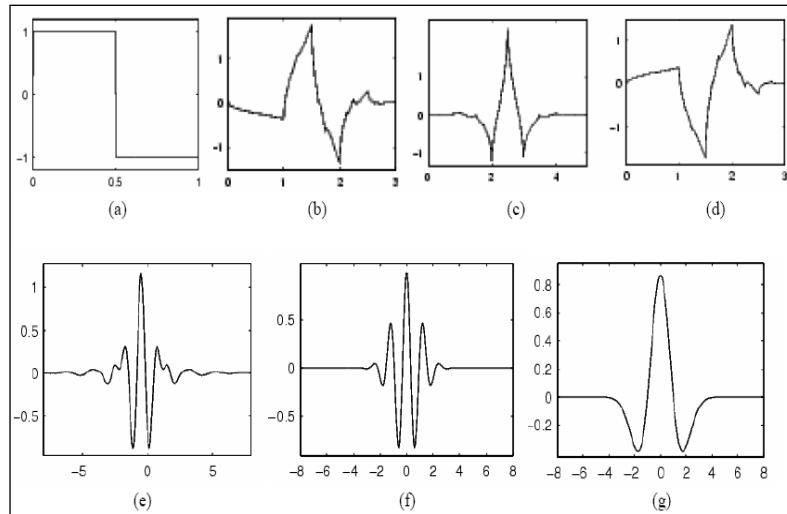


Figure 17. Wavelets transform types a). Haar (b). Daubechies-4 (c). Coiflet-1 (d). Symlet (e). Meyer (f). Morlet (g). Mexican Hat

Discrete wavelet transform, is a mathematical formula which transforms an image from spatial domain to its frequency domain. The DWT of an image can be obtained by passing the image through a series of filters as shown in the block diagram Figure 18. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales. It is based on sub-band coding to yield a fast computation of wavelet transform, easy to implement and reduces the computation time and resources required.

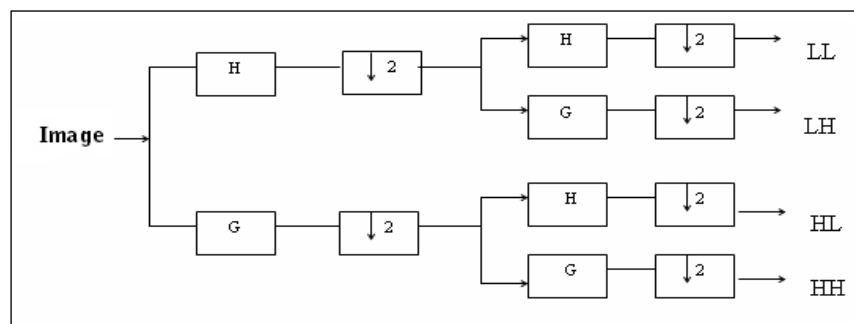
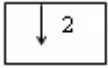


Figure 18. 1-level DWT decomposition process

In the above block diagram, you will notice a box , the \downarrow is the downsampling operator. The reason we included the downsampling operator is: when the image passes through the filters, we would wind up with twice as much data as we started with and this problem is solved by downsampling the resulted data from filters by 2 (Frerking, 1994). LL, LH, HL and HH are the outputs of the filters and we shall explain what is meant by each one. According to Figure 18 the DWT decomposes the host image into four bands of different resolutions: low-low (LL), high-low (HL), low-high (LH), and high-high (HH). The LL sub-band is the approximation coefficients/sub-bands, which are the low frequency components whose contents are considered to be the most important. LH, HL and HH are detailed coefficients/sub-bands, which are the high frequency components. Therefore, the HH sub-band contains the high frequency components of the image and the HVS is a low pass visual system, thus it does not recognize this band. Embedding the watermark in this band does not violate the imperceptibility requirement of watermarking; however compression might remove the HH band that contains the watermark. While, HL and LH sub-bands regions contain frequencies that lie between the LL and HH bands. These bands are not sensitive to HVS as the LL band and they are not the best candidate for removal in compression application as the HH band. So, these bands are the best candidates to embed the watermark in. Till now we have been talking about 1-level DWT decomposition, let's see what 1-level DWT does to the image block as seen in Figure19.

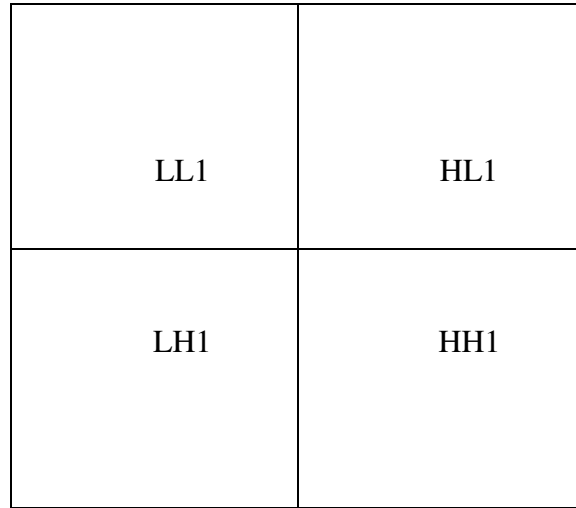


Figure 19. One-Level DWT decomposition

For the sake of understanding what 1-level DWT composition does to an image, we did 1-level DWT composition for a medical image that represents an MRI human brain image as seen in Figure20 (using the wavelet toolbox in matlab).

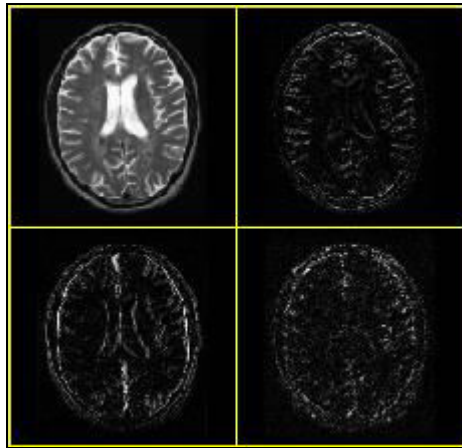


Figure 20. One-Level DWT decomposition of MRI image

So as to obtain other levels of DWT decomposition, the LL sub-band is further processed until some final scale N is reached. Figure 21, shows the 3-level DWT decomposition (N=3).

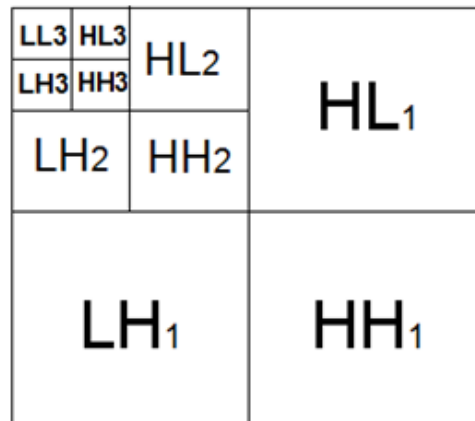


Figure 21. Three-Level DWT decomposition

Figure22 shows the implementation of 3-level dwt on the same MRI medical image.

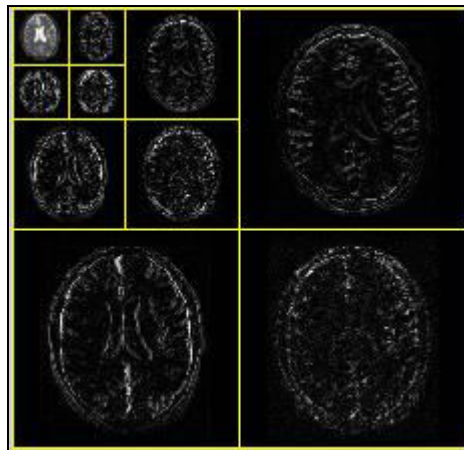


Figure 22. Three-Level DWT decomposition of MRI image

The image can be reconstructed using the four sub-bands' coefficients including the modified ones by using the inverse DWT (IDWT). Wavelet reconstruction includes upsampling and filtering.

A digital watermarking method is pointed to as spread spectrum if the marked signal is got by an additive modification. One of the known techniques is the embedding of a CDMA sequence in the detail bands related to the following equation 6:

$$I_{W_{u,v}} = \begin{cases} W_i + \alpha |W_i| x_i, & u, v \in HL, LH \\ W_i & u, v \in LL, HH \end{cases} \quad (6)$$

Where W_i is the coefficient of the transformed image, X_i the embedded watermark bit, and α is a scaling factor. For detecting the watermark, the same PN sequence used in CDMA is generated with determining its correlation with the two transformed detail bands. If the correlation exceeds certain T , the watermark is detected. As before it could be extended to embed multiple watermarks into the image, thus a separate seed is used for each PN sequence that added to the detail coefficients as the equation above. While the detection procedure, if the correlation exceeds T for a specific sequence a “1” is recovered; else a “0”. Until all of the watermark bits have been detected. Spread-spectrum is robust, but also has a low information capacity due to host interference (Hartung and Kutter, 1999).

3.4 Relevance of Watermarking with Telemedicine

Due to the importance of the security issues related to the management of medical information with such modern forms, hospital information system (HIS) and picture archiving and communication system (PACS), one solution is to use watermarking techniques for protecting medical images. A review by (Coatrieux, et al. 2000) has been selected as the basis for the proposed techniques presented in this thesis. It discusses some security issues in medical

information systems and current security tools in addition to different scenarios of the necessary requirements for such a system to be accepted by medical crew.

Electronic patient record (EPR) contains the digital format of patient annotations, clinical examinations, and images in various modalities to be used for different purposes. So, in general, security of medical information is controlled by a strict ethics and legislative rules; with substantial requirements: confidentiality and reliability. Where confidentiality denotes that only the authorized users, in the normally scheduled conditions, have access to the information; reliability which deals with two portions; i) Integrity: means the information has not been modified by non authorized persons, and, ii) Authentication: a proof that the information belongs to the correct person and from the correct source (Len and Delp, 1999).

Achieving confidentiality means fighting against confidentiality violation, by access control, and secure transmission protocols. In case of integrity threats; destruction and modification of the files contents, the same solutions may also be used, because the violations are similar in most cases. During the transmission, data integrity can be ensured by using digital signatures that generate secure hash which sent with the data.

Lately, there is an increasing number of methods for image watermarking and a number of studies in the literature dedicated to watermarking of medical images. In case of medical field, three requirements are controlled the scheme of watermarking: data hiding (inserting meta data and annotations), integrity control (verification that the image is intact), and authenticity (verification that the image is what the user supposes it is).

However, in case of transmissions, they are done mostly in a secure manner without loss and specific workstations with sufficient protocols, it may be ready for handling local security issues and problems may appear from malicious attempts or human mistakes. As mentioned before, the main constraints of watermarking are invisibility of the mark, capacity, security, robustness against attacks. These demands also require in the medical domain and further constraints are added.

For imperceptibility concept; 1) medical tradition is often not allowed to alter the medical image, in other words, it is very strict with the quality of biomedical images. Therefore, the watermarking method must be reversible meaning that the original pixel values must be exactly recovered. It also constrains to introduce the watermark to prevent transmission of unprotected data.

2) Another alternative to insert the watermark is to define regions of interest so the watermark protects these regions to left intact while being inserted in the rest of the image plane. In fact, the alterations caused in the regions of non-interest will not affect the diagnosis. For example an alteration occurring in image compression; will not interfere with the diagnosis ability.

3) As a third alternative, watermark insertion methods applying in all multimedia signals and medical files too, that use the whole image and result imperceptible alterations in the image pixels (Miaou et al. 2000).

For the integrity control aspect, the "secure camera" concept applies also to the medical images. There is a need to prove that the images on which the diagnoses are based have protected their integrity. The integrity control based on the proper preservation of all the image bits may be unnecessarily strict.

For the authentication aspect, a crucial demand in patient documents is to authenticate the different parts of the EPR in the images. An image is identified by an attached header that holds all the meta data such as the DICOM solution to the radiology images. A possible alternative is to embed all information into the image data itself. Another scheme is to hold both the DICOM header in a separate file and embed the digest of the same information inside the image (Coatrieux et al. 2001).

It could be concluded that, watermarking can raise up the security level of the system and complete the actual security tools by detecting/manipulation errors and malicious actions. It is an ultimate guarantee of authentication more than any other tool protection. Medical images have many annotations and may go through several services that recorded in a historical resume attached to the image as a patient references. If a watermark that is inserted in the image as an identifier is also presented in the header, it guarantees that no error could occur in the image and the header. The handling of both the watermark and the header acts as an additional security for the records. In case of using non-reversible watermarking, addition of watermarks may hold track of the different services that handled the record.

But In case if the EPR is kept by the patient or transmitted to the different services, some techniques must exist to assure the integrity of the record. And watermarking is performed as a tool for integrity control used when important security problems happen (Fridrich, 1999).

3.5 Literature Review

The concept of digital watermarking dates back to the 1992 by Andrew Tirkel and Charles Osborne (Laskar et al. 2013). Many researches of digital image watermarking that present a

complete view of different domain issues in the watermarking field. Following are some current existing literature review regarding pure watermarking techniques related to the secure transmission of medical images although the evolution of digital watermarking in medical applications is still in its infancy. Then some current existing related work according to the hybrid techniques that combined both encryption and watermarking techniques are highlighted.

3.5.1 Pure Watermarking-based Schemes

The studies, that are propriety directed to watermarking method of medical field, are presented in some approaches working in this domain, as shown in Table 5 below.

Table 5. Comparison study related watermarking schemes

Projects	Watermarking Techniques				
	Spatial Domain			Frequency Domain	
	LSB	SVD	Correlation based	DCT	DWT
(Chao et al. 2002)	✓				
(Nambakhash, et al. 2006)					✓
(Umaamaheshvari and Thanushkodi, 2012)				✓	✓
(Soliman, et al. 2012)		✓		✓	✓
(Giakoumaki, et al. 2006)					✓
Proposed Technique	✓		✓		✓

Some authors using LSB technique in specific such as (Chao et al. 2002) that introduces a watermarking system based on LSB replacement to provide origin authentication and protection

of the patient's health document. Their algorithm based on a bipolar multiple-number base that embedded a watermark containing an ECG signal, a diagnostic report, and the physician's stamp. It is noted that the extraction of the watermark requires the original image that weaken the value of the system in practice.

In (Nambakhsh, et al. 2006) a novel blind image watermark approach is developed by embedding electrocardiography (ECG) signals in medical images. There are two processes for embedding the mark signal during the zero-tree wavelet (EZW) coder: the insertion process and the extraction process. The embedding is done when using EZW algorithm after the decomposition step. The algorithm has been tested on several CT and MRI images by measuring PSNR between the original and watermarked image. Cross correlation (CC %) have been calculated between the original and extracted signals for evaluation of percentage of the unchanged signal. The results show that the scheme has proved its imperceptibility and make an optimum balance between the resolution of host image and the size of the mark by controlling the maximum scale to be scanned in EZW algorithm. One advantage, the approach is able to decode the host image and the mark signal progressively.

Also, (Umaamaheshvari and Thanushkodi, 2012) present a hybrid frequency domain watermarking scheme for verifying the integrity and authenticity of medical images. They combine discrete cosine transform (DCT) and DWT. The original image is decomposed using hybrid transform and the watermark embedding and extraction are performed in frequency domain using the presented scheme. For DWT, the Daubechies 4 wavelet transform is chosen. The proposed method is tested for different types of Attacks and is compared with existing methods. The results achieved by using Matlab and tested with different sizes of CT medical

images. As advantages of the hybrid DWT-DCT transform algorithm results, it is enhanced PSNR and structural similarity index measure (SSIM) when comparing the extracted watermark with the original image.

A secure patient medical images and authentication system proposes in (Soliman, et al. 2012) in order to improve the security, confidentiality and integrity of medical image transferring through the internet. The system based on a watermarking technique using particle swarm optimization (PSO) mechanism in adaptive quantization index modulation and singular value decomposition in combination with DWT and DCT. The concept of swarm intelligence acts at collective behavior of intelligent agents in decentralized schemes. Therefore, PSO approach is used to get basic quantization steps which are varied to achieve the most suitable locations for many images with different frequency properties. Authors assume a group of five medical professionals, which are x-ray images as a test samples. The results show that the algorithm can improve the quality of watermarked image and increase the robustness against JPEG compression, noise addition attacks, noise filtration, and geometric attack.

By studying the overwhelming amount of algorithms proposed in the literature, (Giakoumaki, et al. 2006) present a multiple watermarking scheme based on Haar wavelet decomposition and embedding four types of watermarks into a single band of the wavelet coefficients of medical images. The multiple watermarks are embedded in the image by applying 4-level DWT and a proper quantization of coefficients as shown in Figure 23. It can fit the independent block coding strategy of the wavelet-based JPEG2000 standard so it could be coupled with JPEG2000 compression. The watermarks contains: patients personal and examination data, keywords for

information retrieval, the physician's digital signature for authentication, and a reference message for data integrity control.

The authors propose the embedding procedure by decomposing the image through these levels of wavelet transform in a coarse scale image approximation at the highest decomposition level and a sequence of detail images (horizontal, vertical, and diagonal) at each of the four levels. Then a quantization function is applied to each coefficient to be watermarked. If the resulting value is equal to the value of the watermark bit to be embedded, the coefficient is not changed; else, it is modified in order to cast the watermark bit value. So the 4-level inverse wavelet transform is implemented to obtain the watermarked image.

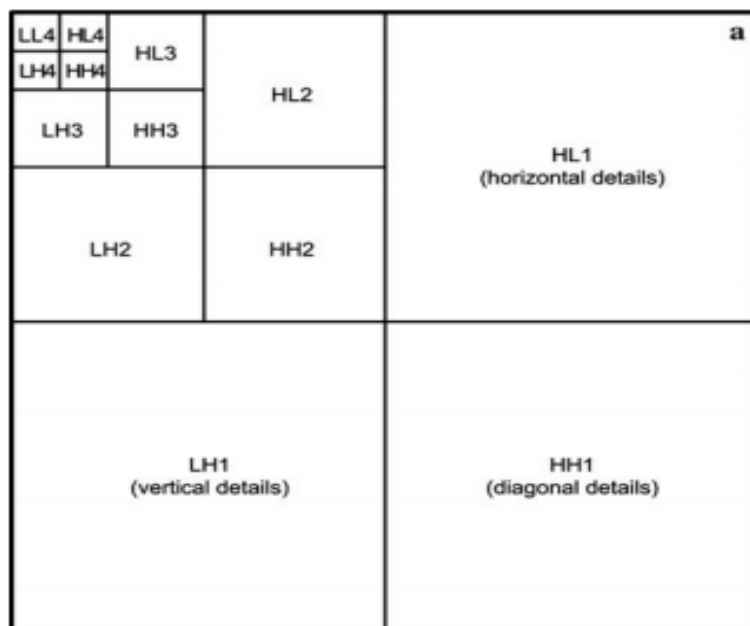


Figure 23. Wavelet decomposition (4-level DWT) of an image

On the other hand, the extraction of the multiple watermarks is implemented through decomposition of the watermarked image using 4-level Haar wavelet transform and key based

detection of the watermarked coefficients. The multiple watermark bits are thus extracted by applying the quantization function to each of these coefficients.

The algorithm was tested on different medical imaging modalities like (CT, MRI). The experimental results highlight the efficiency of the scheme in terms of robustness, transparency, and integrity control capability by measuring the PSNR and the average weighted PSNR (wPSNR). It is noticed that, no distortion can compromise the quality and diagnostic value of the image. The performance of the scheme in terms of robustness was evaluated through JPEG compression of the watermarked images.

As an advantage, the scheme captures a secure and efficient health data management through the use of multiple purpose watermarks where different types of data are carried in each watermark. Each watermark has different features in terms of robustness and capacity, based on the purpose that it addresses. For example, the signature watermark allows the identification of the source of the medical data and the index watermark carries keywords, based on which efficient image retrieval from image databases can take place. The caption watermark contains patient's personal data as well as additional data that are useful for the diagnosis. Moreover, the fragile reference watermark is embedded in all levels aiming to guarantee the data integrity control and detect tampering. Take into consideration, that the scheme allows the definition of a region of interest (ROI) that provides using of reference watermark embedding due to its tampering property. The region of non interest (RONI) can be marked with all the watermarks.

3.5.2 Encryption and Watermarking-based Schemes

The studies that are directed to crypto-watermarking methodologies for medical image safe transfer are presented in schemes as shown in Table 6 below.

Table 6. Comparison study related encryption and watermarking schemes

Projects	Encryption Techniques				Hashing	Watermarking Techniques					
	Public-Key Cryptography		Private-Key Cryptography			Spatial Domain			Frequency Domain		
	RSA	DSA	DES	AES		LSB	SVD	Corr. based	DCT	DWT	IWT
(Puech, et al. 2008)				✓				✓			
(Umamageswari, et al. 2011)	✓	✓			✓	✓					
(Bouslimi and Coatrieux, 2011)				✓				✓			
(Viswanathan and Krishna, 2011)				✓						✓	
(Piao et al. 2008)					✓	✓					✓
Proposed Technique					✓			✓		✓	

Some authors have presented a number of techniques such as (Puech, et al. 2008) they defined a method of applying reversible data hiding algorithms on the encrypted medical images by trying to remove the embedded data before the decryption process. The encoding algorithm done by the electronic code book (ECB) mode of AES algorithm then hiding the data by a bit- substitution based method. Then the extraction of the message and the decryption-removing have done within the analysis of the local standard deviation of the marked encrypted images. The results are achieved by applying the method on various gray level images and measuring the PSNR and the

variation of the local standard deviation for each pixel while taking its neighbors into account. The image information content with the entropy was measured too. They mentioned that the encrypted images are protected against statistical attacks without showing the results.

The authors in the (Umamageswari, et al. 2011) propose the need for reversible watermarking techniques and security related problems in various medical image modalities. It is based on ROI supporting lossless watermarking systems to verify authentication, and public key cryptography RSA algorithm to verify confidentiality. The discussion includes the capacity rate and PSNR values, shows that the normal reversible watermarking without using any additional security techniques having least capacity rate and PSNR values. But applying reversible watermarking with DSA approach has better capacity rate and PSNR value. When compared to reversible watermarking with secure hash algorithm (SHA-256), the PSNR value is low beside the good capacity rate. Comparing the lossless watermarking techniques is done for various medical image modalities like MRI, ultrasonic, positron emission tomography (PET), Endoscopic and angiographic images. As a result the best findings achieved by reversible watermarking were with RSA approach and LSB modification proves to be a simple and fairly powerful tool although it is not robust method.

It is worth to mention that the authors in (Bouslimi and Coatrieux, 2011) discuss a new joint watermarking/encryption algorithm by merging the quantization index modulation (QIM) and a block cipher algorithm the AES in cipher block chaining (CBC) mode. The system relies on two main procedures: image protection and verification. This makes it support by the DICOM standard and gives access to the messages in the spatial domain and in the encrypted domain. The encrypted domain is used for verifying the reliability. Experimental results are evaluated and

proved that the image distortion is very low. But for the limitations: the insertion of the messages does not affect general performances of the encryption procedure. Also, the algorithm is not suitable for real time transmission of image since it needs twice the time necessary for encryption with AES only. They defend that the messages will be lost after any image modification, by the fact that the authors focus on verifying data reliability.

Also (Viswanathan and Krishna, 2011) is a system known as randomized cryptographic fusion watermarking system. The mechanism based on the encryption of the patient document and the cipher is randomly embedded in the medical image by the bit wise operation. Within authentication, the embedded data is extracted and decrypted then compared with the patient original information. By choosing a sample of image data, the mathematical evaluation is tested by PSNR measures. The results assure that the algorithm provides high payload capacity, less computational complexity and enhancement of the security due to the fact that the quality of the image is maintained without any distortion. For an advantage, they apply the confidentiality requirement by encryption and hiding the data randomly in different locations in the image. The drawbacks of the system is, it only uphold the image of size (256×256). This system may be extended with the combination of cryptography based on Biometric data for personal authentication to be more confidential.

While, (Piao et al. 2008) algorithm introduces a fragile watermarking system in order to secure the medical images. It depend on the hash function. Integer wavelet transform (IWT) and LSB method. In this case, and in contrast to DWT method, an IWT is used to utilize hash function. Before the embedding process, the watermark related to the hash values is inserted into the LSB of IWT coefficients then the host image is transformed into wavelet domain by IWT and

decomposes the image up to one level. Where LL1 is divided into equal size of blocks and the bit planes of LL1 are randomly selected for embedding process. After that, the most significant bit (MSB) values and image size information is passed to hash function to obtain the hash value. And the output of hash function is then embedded in selected bit plane and combined with MSBs to get the watermarked coefficients besides the inverse IWT process is applied to get the watermarked image. About the extraction mechanism, first level IWT decomposed the image into four sub-bands. Approximation coefficients are divided into blocks and the bit plane of each block is selected so the bitstream is extracted. At the final stage, the MSB values and image size information are passed to hash function to calculate the hash value. Then an integrity check is done between the extracted hash value and embedded hash value; if they are the same, then the image is identified authentic.

Chapter 4

Proposed Crypto-based Secured Telemedicine Algorithm

In this chapter, the focus is on applying two different techniques for secured telemedicine applications that satisfies the needed requirements. A brief description for both proposed algorithms is presented. Then a block diagram for the sending side and the receiving side are drawn explaining how the confidentiality, integrity, and authentication are achieved for the header level and the image level. After that the algorithms implementation are discussed and finally they are evaluated by determining the main metrics. A comparison between both proposed algorithms and other crypto-based algorithms is highlighted.

4.1 Proposed Algorithm I

In this section, the details of the proposed encryption algorithm I are outlined. The proposed approach uses encryption to provide secure transfer for medical images. Since the DICOM standard was the choice to apply the algorithm, so the three security requirements are achieved on the header level and on the image (pixel data) level too. In general the encryption process takes three inputs as shown in Figure 24; header data to authenticate patient data, pixel data to validate the image, and authentication entity data to determine the authorship of the image. The outputs are: the encrypted pixel data and the security data (digital signatures) that will be used for decryption.

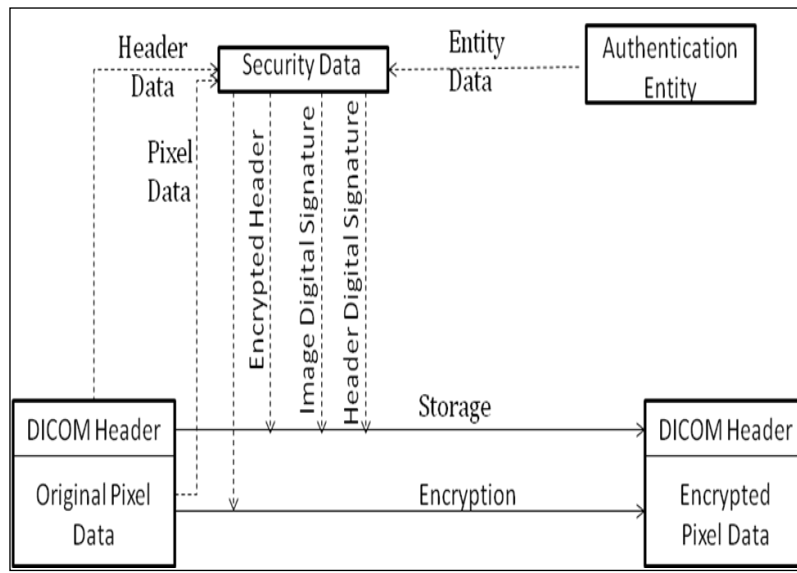


Figure 24. Proposed approach for data encryption

The security verification process related to pixel data decryption is shown in Figure 25. It recovers the original pixels and checks if the data are reliable or not. It was important to choose what metadata will be used. The DICOM standard depends on PS3.15 that defines the basic application level confidentiality profile attributes. This was our choice to be used. All the attributes in the research's dataset are listed along with their tags in Table 3 page 27.

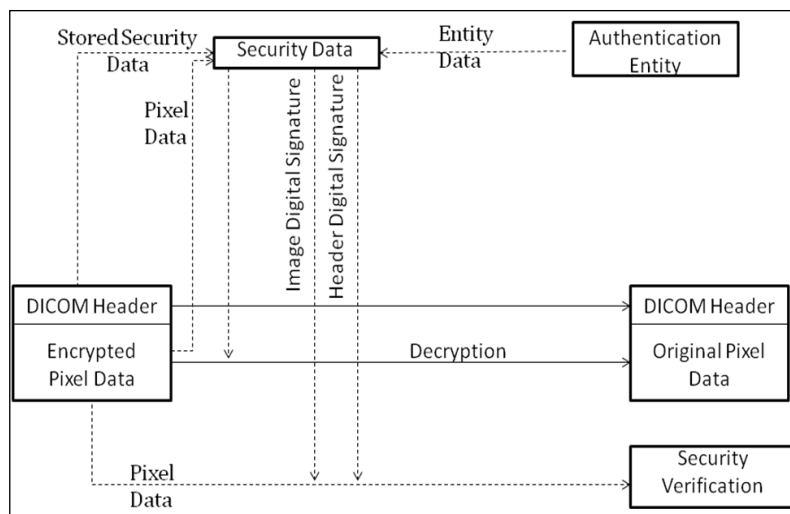


Figure 25. Proposed approach for data retrieval and verification

4.1.1 Encryption Flow at the Sending Side

For this approach, a basic algorithm is proposed and implemented. The encryption flow of the proposed algorithm is shown as in Figure 26. The Figure presents the block diagram that illustrates the main parts of the proposed algorithm at sending side where (a) is for the header and (b) for the data, besides the relations between the different blocks.

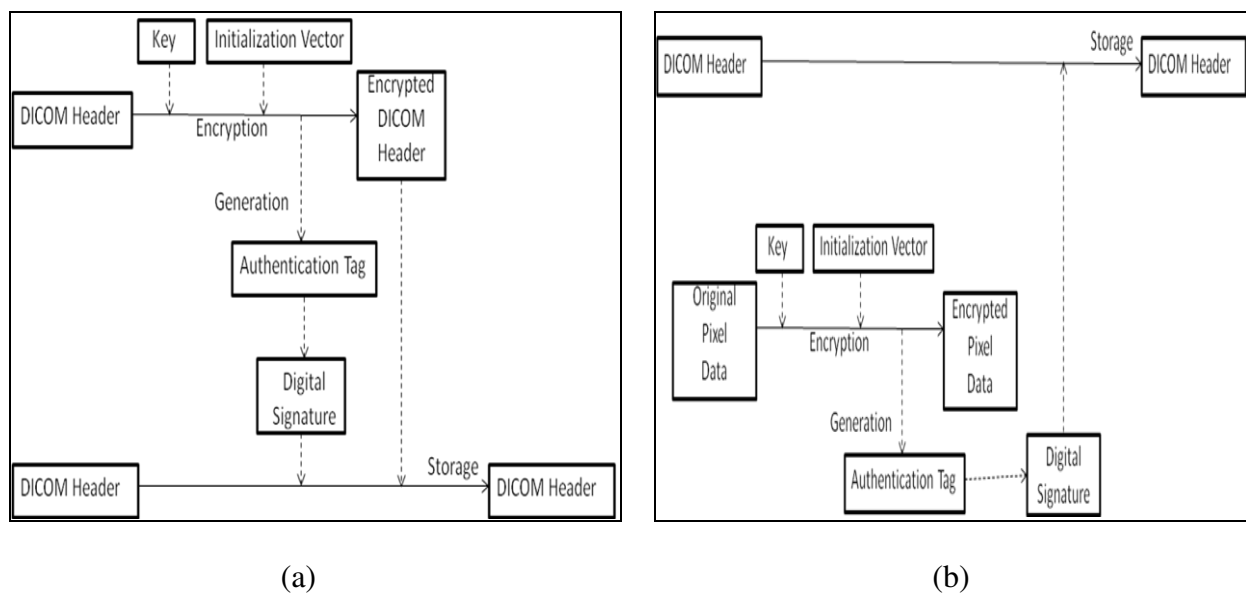


Figure 26. Signing and encryption process: (a) for the header, (b) for the image

The header encryption process falls as in the following steps:

Step 1: use an externally supplement (personal token) as source to provide the key and the initialization vector (IV) of the symmetric encryption algorithm. For example the IV is given as 4 vectors of 256 bits: the first and third vectors consist of 64 bits of zeros, the second and fourth vectors consist of 64 bits of ones.

Step 2: encrypt the DICOM header by means of encrypting only the confidential attributes values with the symmetric encryption algorithm that is used here, and store the encryption result of encrypted header in the (0400, 0550) modified attributes sequence location, while replacing the values in the original locations with dummy ones (it is one application of de-identification of DICOM standard), confirming the confidentiality requirement.

Step 3: the process also generates an authentication tag, contains information about the integrity of the header data. This tag acts as an original hash, and signed to generate a digital signature of the header along with a 256 bits private key using asymmetric digital signature algorithm.

Step 4: the digital signature is stored in the original header to be sent with it along with the public key of the owner. This step is achieved the header authentication.

About the image pixel data encryption is applied as in the following steps:

Step 1: supply the image with the same key and IV that used with the header encryption process.

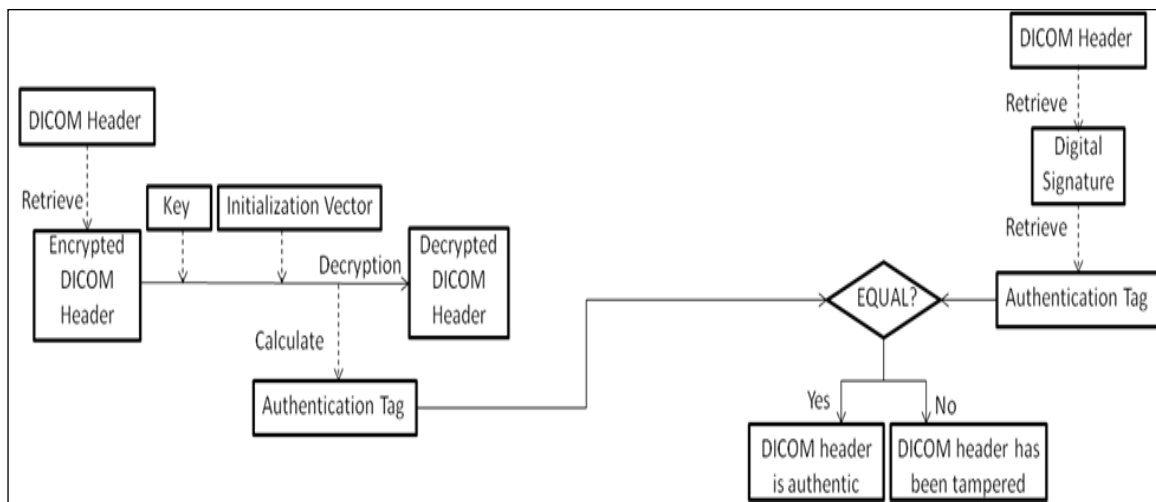
Step 2: the data encrypted using the same symmetric encryption algorithm that is used in encrypting header to generate a stream of encrypted pixel data (the encryption result is such that the processed pixel data hold no visual relation to the original image). An authentication tag is produced here, containing the information about the integrity of the pixel data. By this step the image confidentiality is achieved due to the used encryption algorithm and the image integrity is achieved due to the authentication tag generation.

Step 3: the tag is used with a private key of the signing entity and generates a digital signature (256 bits) of the image using asymmetric digital signature algorithm.

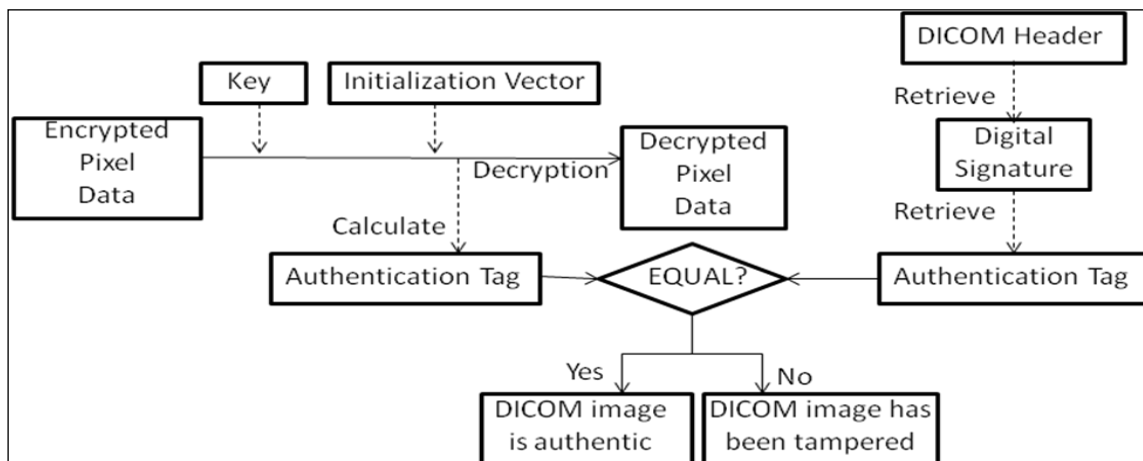
Step 4: the image digital signature is stored in the original header itself along achieving the authentication requirement related to the image.

4.1.2 Decryption Flow at the Receiving Side

On the other side, the decryption process and security verification of the proposed algorithm are viewed in Figure 27. Where (a) illustrates the header decryption and verification, and (b) illustrates the image decryption and verification.



(a)



(b)

Figure 27. Decryption and verification process: (a) for the header, (b) for the image

Based on the Figure above, the header operations fall as in the following steps:

Step 1: beginning with the same header attributes used in the encryption are retrieved in order to decrypt them using symmetric encryption algorithm. The same key and IV used in the encryption process will be used in the decryption process too. So the confidentiality is achieved.

Step 2: according to the previous step an authentication tag will be generated.

Step 3: the encrypted header digital signature that is stored in the received header before, is retrieved and decrypted using the same asymmetric digital signature algorithm to retrieve the received authentication tag.

Step 4: both tags, the received retrieved one and the calculated one, are matched against the signature stored in the header, verifying the integrity and authenticity confirming the header is tampered or not.

For the image decryption and security verification, the steps are:

Step 1: the original pixel data are recovered from the encrypted data using the same encryption key and IV that used by the sender. The same symmetric encryption algorithm is applied. The confidentiality is achieved by this step.

Step 2: the authentication tag is generated too from the previous decryption process.

Step 3: the encrypted image digital signature that is stored in the received header before, is retrieved and decrypted using the same asymmetric digital signature algorithm to retrieve the received authentication tag.

Step 4: for this implementation, both tags (the retrieved received one and the calculated one) are matched against the signatures stored in the header retrieved by asymmetric digital signature algorithm for the image. This step verifying the integrity and authenticity confirming the image is tampered or not.

4.2 Proposed Algorithm II

In this section, the details of the proposed encryption algorithm II are outlined. In general the encryption process takes three inputs and the same outputs that were explained before in the proposed algorithm I shown in Figure 24. The differences with the first proposed algorithm are shown in the sending and receiving sides below.

4.2.1 Encryption Flow at the Sending Side

The encryption flow of the proposed algorithm is shown as in Figure 28. The Figure presents the block diagram of the algorithm at the sending side where (a) for the header and (b) for the data.

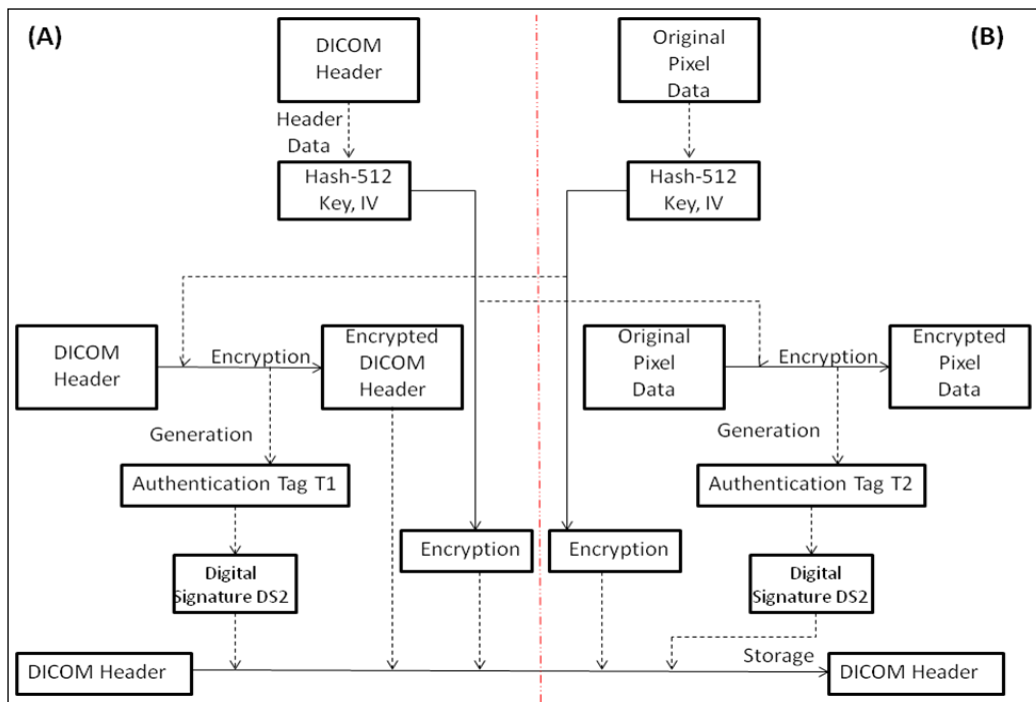


Figure 28. Signing and encryption process: (a) for the header, (b) for the image

The header encryption process falls as in the following steps:

Step 1: the header confidential attributes is hashed using a hashing function algorithm, producing an output of fixed size of bits clarifying its integrity.

Step 2: then, a fixed portion of 256 bits of the output is used as the encryption key and another portion as the IV (of 96 bits and it will be padded with dummy ones to be 256 bits) of the encryption algorithm. These will be the security data for image encryption.

Step 3: the header hashing value result is encrypted using asymmetric encryption algorithm and stored in the DICOM header to be sent.

Step 4: encrypt only the confidential attributes values of the DICOM header with symmetric encryption algorithm, and store the encryption result in (0400,0550) modified attributes sequence, while replacing the values in the original locations with dummy ones, confirming the confidentiality requirement.

Step 5: the process also generates an authentication tag, containing the information about the integrity of the header data. This tag acts as an original hash and that achieved the integrity of the header, and signed to generate a digital signature of the header along with a 256 bits private key of the signing using asymmetric digital signature algorithm.

Step 6: the digital signature is stored in the original header to be sent with it. This step is achieved the header authentication.

The image pixel data encryption is applied as in the following steps:

Step 1: the image pixel data is hashed using a hashing function, generating an output of fixed portion for the key and another portion for the IV. And these will be the security data for the header encryption. This step achieved the integrity requirement.

Step 2: the image hashing value result is encrypted using asymmetric encryption algorithm and stored in the DICOM header to be sent.

Step 3: the image pixel data encryption supplied with the header output hashing as mentioned before; it will be encrypted using the same encryption algorithm to generate a stream of encrypted pixel data and an authentication tag, containing the information about the integrity of the pixel data. By this step the image confidentiality is achieved due to the encryption algorithm usage and the image integrity is achieved due to the authentication tag generation.

Step 4: the tag is used with a private key of the signing entity and generates a digital signature (256 bits) of the image using asymmetric digital signature algorithm.

Step 5: the image digital signature is stored in the original header itself achieving the authentication requirement related to the image.

4.2.2 Decryption Flow at the Receiving Side

On the other side, the decryption process and security verification of the proposed algorithm are viewed in Figure 29. Where (a) illustrates the header decryption and verification, and (b) illustrates the image decryption and verification.

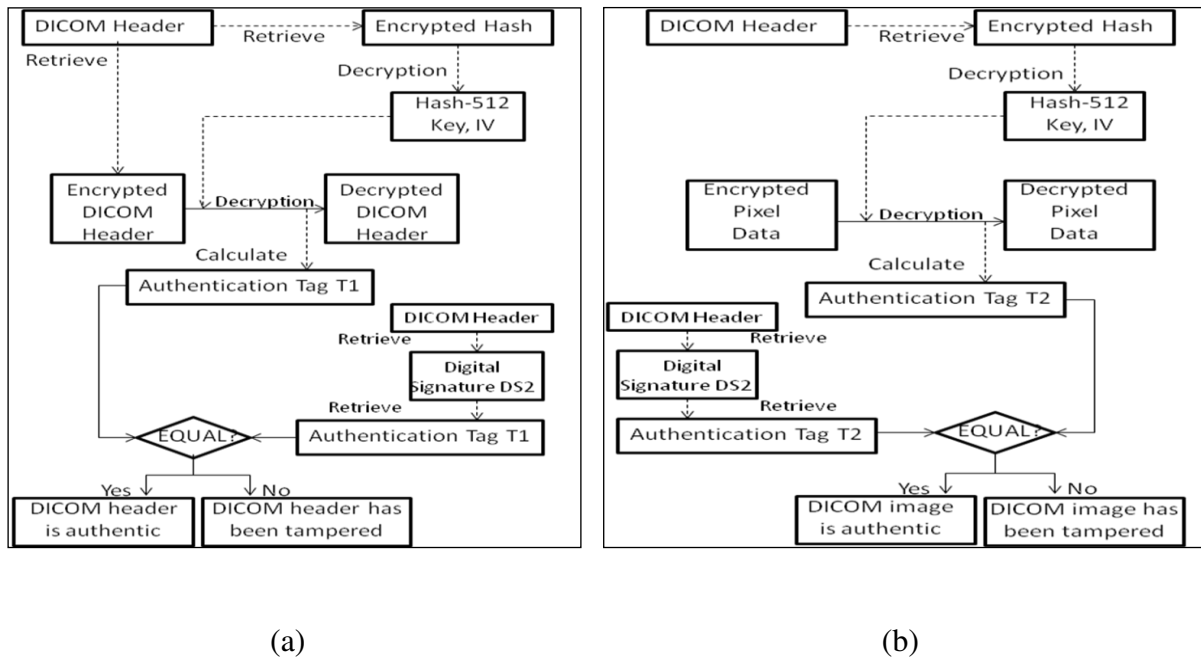


Figure 29. Decryption and verification process: (a) for the header, (b) for the image

Based on the Figure above, the header operations fall as in the following steps:

Step 1: extract the image encrypted hash from the received header and decrypt it by asymmetric encryption algorithm in order to retrieve the hash output (512 bits) which consists of the key and IV needed to decrypt the encrypted header attributes.

Step 2: the same header attributes used in the encryption are extracted in order to decrypt them using symmetric encryption algorithm. The confidentiality is achieved here.

Step 3: after the decryption process an authentication tag will be generated.

Step 4: the encrypted header digital signature that stored in the received header before, is retrieved and decrypted using the same asymmetric digital signature algorithm to retrieve the received authentication tag.

Step 5: both tags, the received retrieved one and the calculated one, are matched against the signature stored in the header, verifying the integrity and authenticity confirming the header is tampered or not.

For the image decryption and security verification, the steps are:

Step 1: extract the header encrypted hash from the received header and decrypt it by the same asymmetric algorithm in order to retrieve the hash output (512 bits) which consists of the key and IV needed to decrypt the encrypted image data.

Step 2: the original pixel data are recovered from the encrypted data, as well as its authentication tag by using the same symmetric algorithm achieving the confidentiality.

Step 3: the encrypted image digital signature that is stored in the received header before, is retrieved and decrypted using the same asymmetric digital signature algorithm to retrieve the received authentication tag.

Step 4: for this implementation, both tags (the retrieved received one and the calculated one) are matched against the signatures stored in the header retrieved by asymmetric digital signature algorithm for the image. This step verifying the integrity and authenticity confirming the image is tampered or not.

4.3 Implementations of the Algorithms

In both proposed techniques, many types of encryption/decryption algorithms are used. So it must be important to highlight the used algorithms and the purpose of choosing them. It is worthwhile to mention that the same types of techniques are used for the first and second proposed algorithms.

4.3.1 The AES-GCM Symmetric Encryption Primitive

The encryption algorithm of choice is the advanced encryption standard-Galois counter mode (AES-GCM) with a key size of 256 bits and an IV of 96 bits. It has been standardized by National Institutes of Standards and Technology (NIST). This algorithm is based on a universal hashing over a binary Galois field to provide authenticated encryption, producing both the ciphertext and the authentication tag for integrity verification. It combines the counter mode of encryption with the new Galois mode of authentication. Table 7 presents a summary of GCM properties (McGrew and Viega, 2005). The feature: authenticated encryption indicates that the GCM provides not just confidentiality but integrity/authenticity too. In other words, if the encrypted block has been tampered with (intentionally or unintentionally), the algorithm provides a means for its detection and will not decrypt the block.

In both proposed algorithms, AES-GCM takes three inputs: data to be encrypted or decrypted, encryption key of size 256 bits, and IV of size 96 bits which is padded here with 1's to be of size 256 bits. The outputs are: the encrypted or decrypted data and the authentication tag. The sender generates hash subkey for the hash function and a pre-counter from the IV. Then the ciphertext is generated by applying the 32-bit incrementing function to the pre-counter block. After that, concatenate of the additional authenticated data and the ciphertext, and apply the hash function to produce a block that is encrypted to generate the authentication tag. At the receiver side, the same procedure is applied so the result is compared with the authentication tag that was received. However, in the implementation, the choices of algorithms were based on finding the effective ones and not have been broken yet such as AES with a key of 256 bits that used in US government. Besides, GCM can take full advantage of parallel processing and using of pipeline instruction in contrast to the CBC mode in which the pipeline baulk its efficiency. The choice of

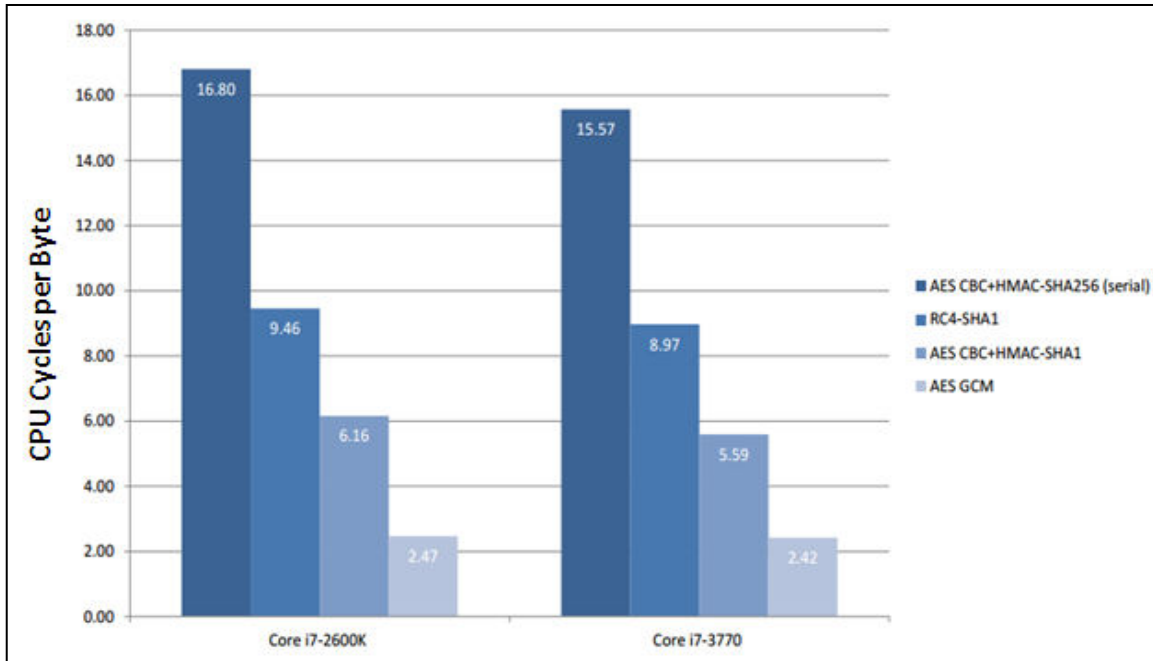
nonce in GCM to be not fixed and unique with every encryption operation is a secure option. It has a minimum latency and minimum operations overhead. So it is worthwhile to note that this mode of operation gives some valuable insights into how polynomial hash based authentication acts (McGrew and Viega, 2004).

Table 7. A summary of the properties of AES-GCM

Security Function	Authenticated encryption
Error Propagation	None
Synchronization	Same IV used by sender and recipient
Parallelizability	Encryption - block-level Authentication - bit-level
IV Requirements	Each IV must be distinct, for each fixed key IV can have arbitrary length from 1 to 2^{64} bits
Memory Requirements	Same as block cipher
Pre-processing capability	Effective methods available for accelerating authentication
Message Length Requirements	Arbitrary message up to $2^{39} - 256$ bits Arbitrary additional authenticated data up to 2^{64} bits.
Ciphertext Expansion	Ciphertext length is identical to plaintext length 0 to 128 bits required for the authentication tag

Among the NIST standard options, AES-GCM is the best performing authenticated encryption combination compared to the other authenticated encryption algorithms such as AES CBC+ (hash message authentication code) HMAC- SHA-1, AES CBC+HMAC-SHA256, and RC4-

SHA1. And it keeps improving performance across central processing unit (CPU) generation. In Figure 30 some authenticated encryption performance. It measures cycles per bytes versus (vs.) cores (Intel® Core™ i7-2600K and Intel® Core™ i7-3770 Processors) on 32KB buffer in CPU



cycles per byte where lower is better. (Gueron and Kounavis, 2012).

Figure 30. AES-GCM vs. other (NIST standard) Authenticated Encryption

4.3.2 The Whirlpool Hashing Function Primitive

The Whirlpool hashing function is a quite recent algorithm, proposed in the New European Schemes for Signatures, Integrity and Encryption (NESSIE) Project as a strong hash function. At the present, it has been standardized by International Standards Organization (ISO) (Barreto and Rijmen, 2003). It has one input: original or encrypted data less than 2^{256} bits and an output: of 512 bits that is divided into 256 bits representing the encryption key and 256 bits representing the IV. The encryption process consists of updating an 8 by 8 state matrix (block cipher) with

four round functions (sub bytes, shift columns, mix rows, and add round key) over 10 rounds. During each round the new state is computed.

The choice of Whirlpool to be the main hashing function here is that according to the (Andrew, 2007) for a hashing algorithm to be considered secure one it should have double the number of calculations required to solve it in a suitable time since computers are getting faster. Up to date of article 2007, the current strongest encryption algorithms are SHA-512 and Whirlpool. Any one of these algorithms are worthy of protecting information. So due to the fact that no attacks have been reported on earlier versions of Whirlpool and the new versions are produced to perform better, likely to be more secure, so we choose Whirlpool to be the used hash function.

4.3.3 The Elliptic Curve Digital Signature Primitive

Asymmetric DSA is applied in both proposed techniques by choosing the elliptic curve digital signature algorithm (ECDSA) to generate a digital signature along with a 256 bits private key. The ECDSA is now widely accepted and used in several applications, producing shorter signatures than the original DSA, with the same security properties. The generated signature is stored in the digital signature sequence location as defined in DICOM security part15 (Lopez and Dahab, 2000). It takes an input (authentication tag) of 256 bits and output the digital signature of 256 bits too using a private key. The algorithm has three phases: key generation, signature generation, and signature verification. Such the formula of the elliptic curve is $y^2 = x^3 + x + 1$. Determine the domain coefficients and the base point $G=(X_g, Y_g)$ such $X_g=13$ and $Y_g=7$. Take $n=7$, the order of the base point. Select the random private key d in range $1 \leq d \leq n-1$, take $d=4$. Then compute the public key $Q=(X_q, Y_q)$ which is $Q=(17, 20)$. Select $k=3$ in range $1 \leq k \leq n-1$. Compute $k \times G=(X_1, Y_1)$, $R=X_1 \pmod{n}$, and $S=k^{-1} \times [(e + d \times R) \pmod{n}]$. The generated

signature gives as (R, S) . Then the receiver verifies if the public key curve point is valid and calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q$. The signature is valid if $R = X_1 \pmod{n}$.

The reason for choosing ECDSA over other algorithms, that the size of the public key needed for ECDSA is about twice the size of the security level. And it is a newer operation compared to RSA and according to (Bendel and Mike, 2011) in December 2010, a group calling itself fail0verflow notified recovery of the ECDSA private key used by Sony to sign software for the PlayStation 3 game console. Although, this attack could be assumed invalid against ECDSA because it's Sony failed to implement valid signature(s).

4.4 Performance Evaluation of the Algorithms

A MATLAB (7.6.0) program is used to implement both proposed algorithms and the test is done on 20 brain DICOM image with a size of 256×256 pixels each, with a depth of 16 bits. The graphical user interface is used so it can be represented in form of rules which can be easily understood by humans. MATLAB is installed on Dell N5010 machine Model Laptop, Intel Core TM, 4.00 GB RAM, and M 350@ 2.27 GHz with Microsoft Windows XP operating system.

4.4.1 Performance Evaluation Metrics

In order to evaluate both systems, a numbers of metrics are used depends on:

- Histogram analysis.
- Key sensitivity analysis.
- Entropy.
- Correlation.
- PSNR.

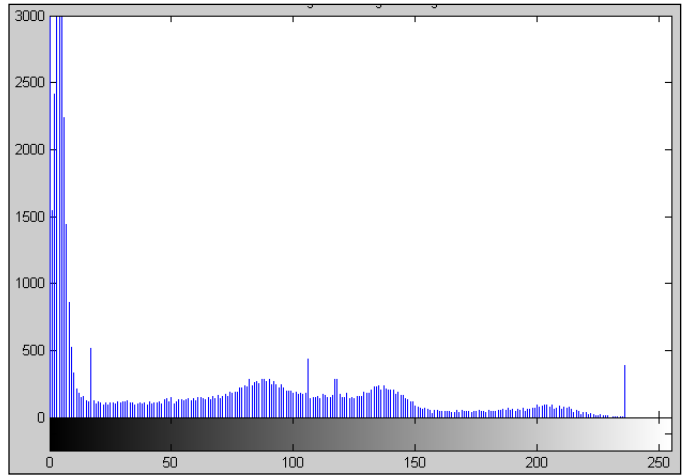
- Encryption/Decryption time.
- Robustness against noise or attacks.

4.4.2 Histogram Analysis

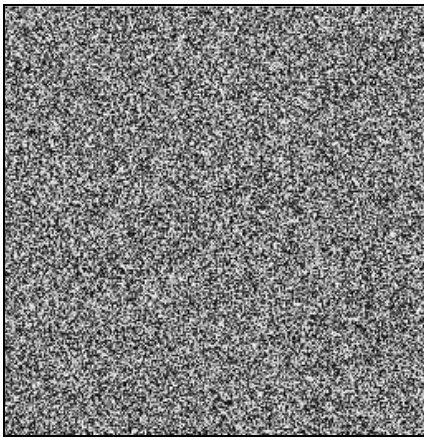
Image histograms aid in understanding the similarity among the pixels. If there is no or negligible similarity among the pixels then encrypted image is secure against attacks. Figure 31 shows the histogram of brain image for proposed algorithm I. Figure 31(b) represents the histogram plot of original plain image shown in Figure 31(a). It can be observed that the statistical relation among the pixels has resulted in variation in the histogram plot. Figure 31(d) represents the histogram plot of encrypted image shown in Figure 31(c). Figure 31(f) represents the histogram plot of the decrypted image shown in Figure 31(e). It is clear from the histogram plot shown in Figure 31(d) that attacker may conclude the least information from the ciphered image because neighboring images are not related to one another. The same is shown in Figure 32 for the proposed algorithm II. Figure 32(b) represents the histogram plot of original image shown in Figure 32(a). Figure 32(d) represents the histogram plot of encrypted image shown in Figure 32(c). Figure 32(f) represents the histogram of the decrypted image in Figure 32(e). Thus, both proposed encryption strategies can detect any statistical attacks that can be performed on encrypted image.



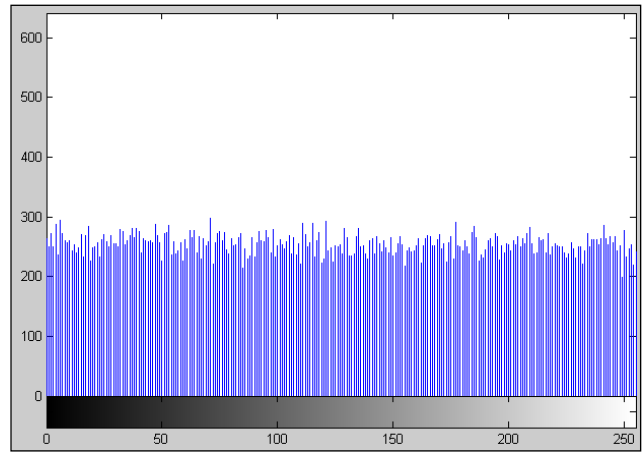
(a) Original image



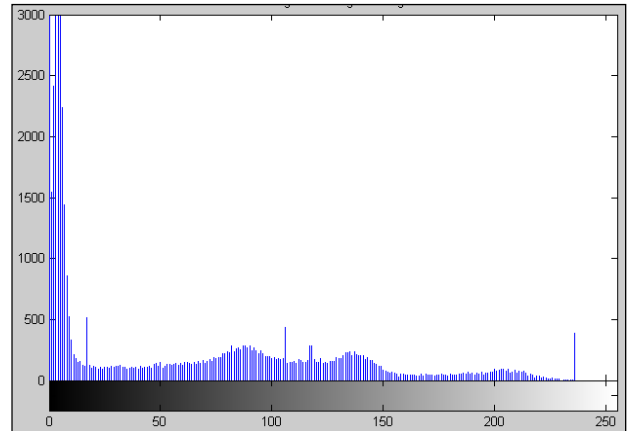
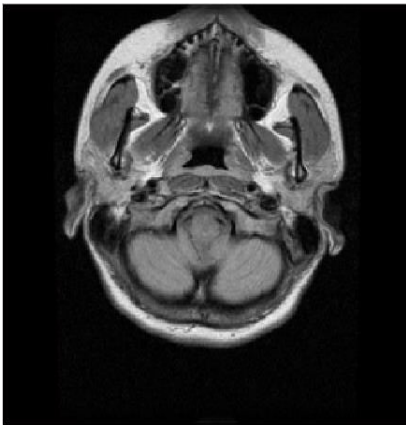
(b) Histogram of original image



(c) Cipher image



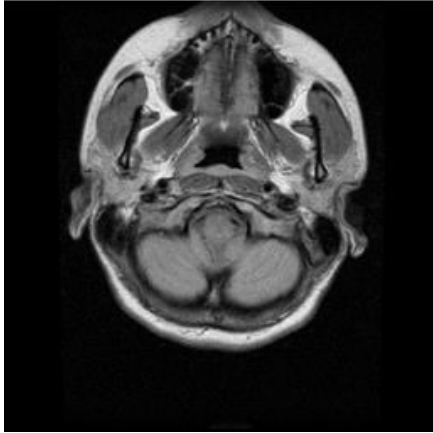
(d) Histogram of cipher image



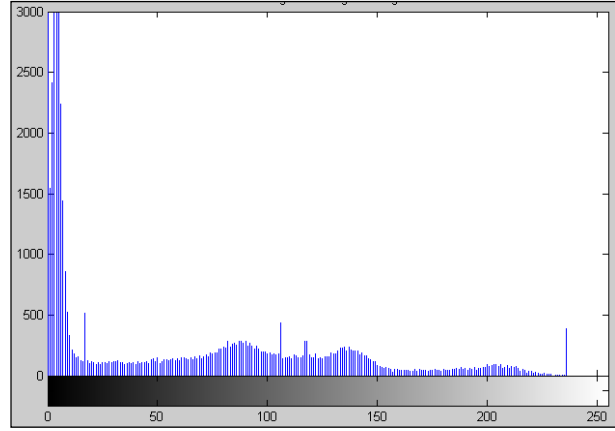
(e) Decipher image

(f) Histogram of decipher image

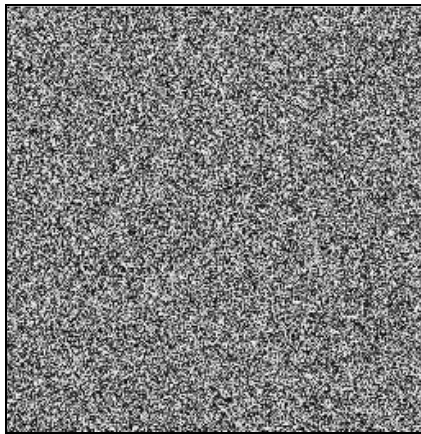
Figure 31. Histogram of plain and cipher image related to the proposed algorithm I



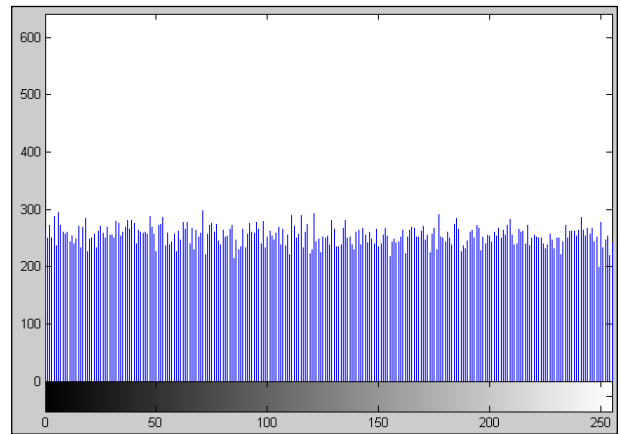
(a) Original image



(b) Histogram of original image



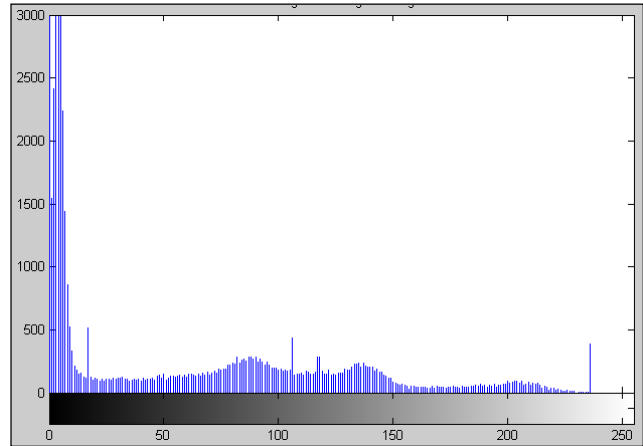
(c) Cipher image



(d) Histogram of cipher image



(e) Decipher image



(f) Histogram of decipher image

Figure 32. Histogram of plain and cipher image related to the proposed algorithm II

4.4.3 Key Sensitivity Analysis

Encryption technique should be secure enough even if there is little alteration in key. If the attackers guess the partial correct key, then the decryption process fails. So this analysis is performed by changing the two byte information of the correct key. Figure 33 shows the decryption of encrypted image with a valid key. Figure 34 shows decryption of ciphered image with the incorrect key. Here changing first two hexadecimal digits of the key. Under such instance the proposed encryption algorithm I is secure. For the proposed algorithm II, Figure 35 shows the decryption of encrypted image with a valid key. Figure 36 shows decryption of ciphered image with the incorrect key. Proposed algorithms are completely secured since a change of one byte of the valid key will not lead to the original image again.

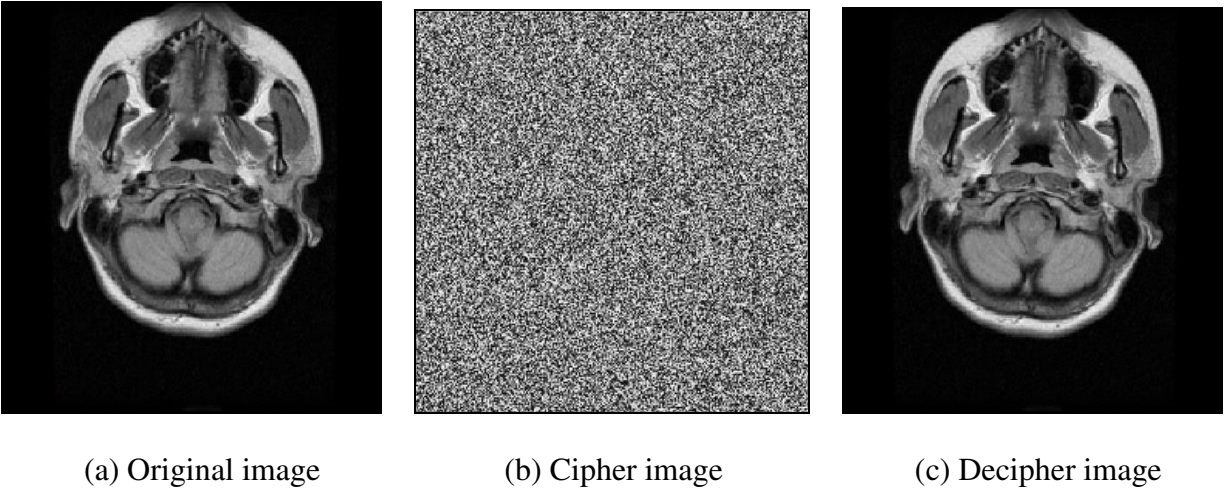


Figure 33. Decryption using correct key related to the proposed algorithm I

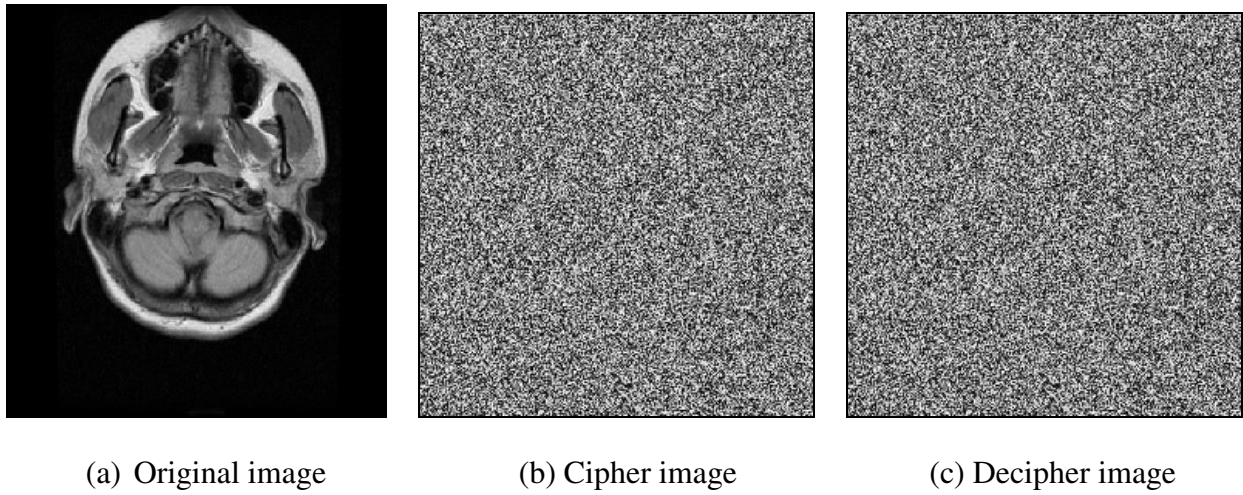


Figure 34. Decryption using incorrect key related to the proposed algorithm I

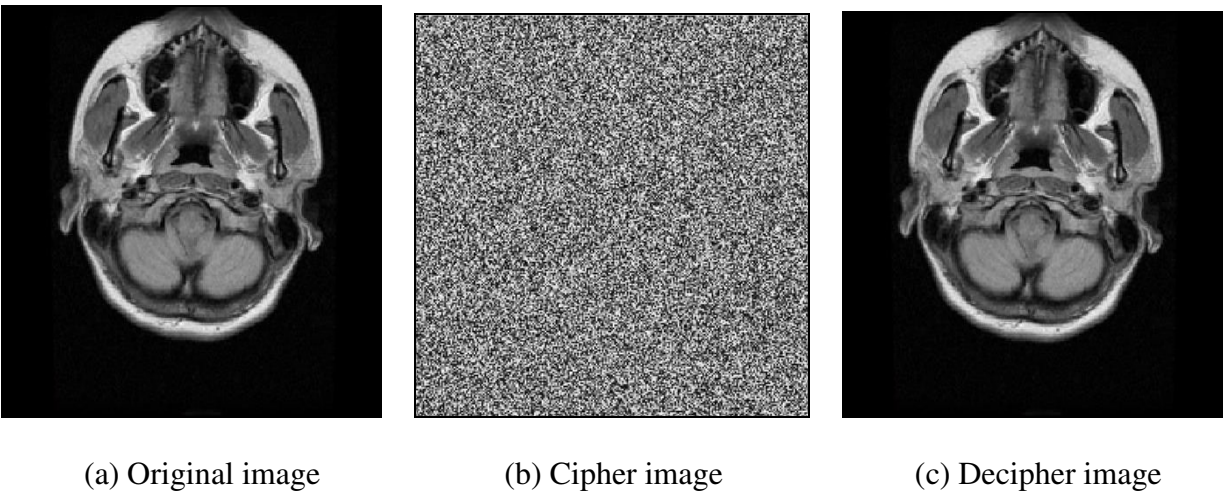
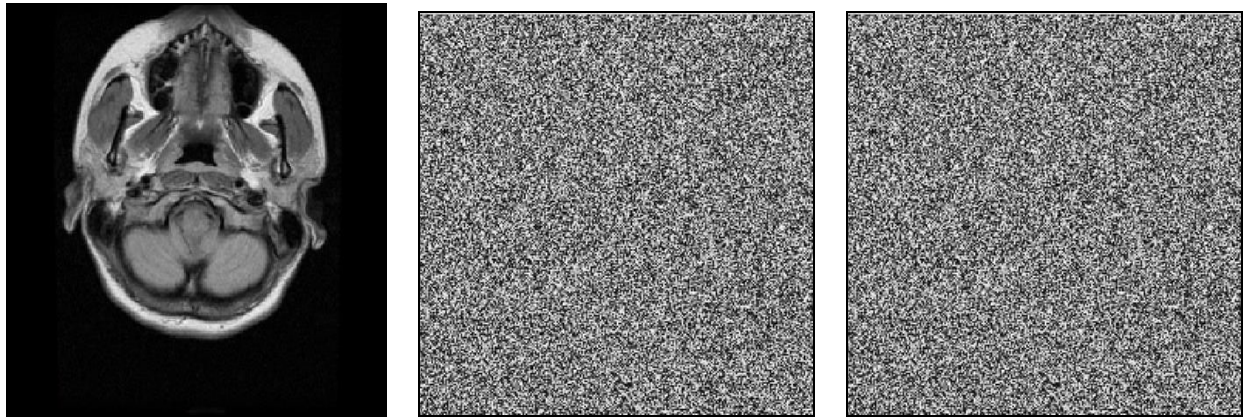


Figure 35. Decryption using correct key related to the proposed algorithm II



(a) Original image

(b) Cipher image

(c) Decipher image

Figure 36. Decryption using incorrect key related to the proposed algorithm II

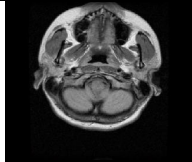
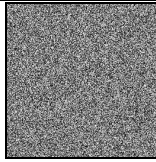
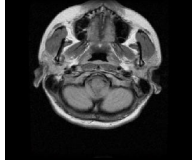
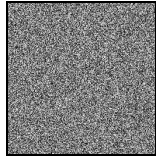
4.4.4 Entropy

Entropy is a measure of uncertainty. It is an important measure to analyze the encrypted image. The higher the value of entropy of encrypted image, the better of the security. The Entropy E_n of the input original image and the encrypted image is calculated using equation 5:

$$E_n = \sum_{i=0}^{255} (p(i) * \log_2(1/p(i))). \quad (5)$$

The term $p(i)$ is the number of occurrence of a pixel/total number of pixel in the image. Information entropy is calculated by using the above equation and the results are shown in Table 8 for both proposed algorithms. It is worthwhile to note that ideally the entropy should be 8 bits for gray scale images. If an encryption scheme generates an output cipher image whose entropy is less than 8 bits, then there might be a possibility of predictability, which may threaten its security. The results of our algorithms are very close to the theoretical value of 8, implying that information leakage is negligible and (AES-GCM) encryption algorithm is secure

Table 8. Entropy values for original image and ciphered ones

Proposed Algorithms	Original Image	Cipher Image	Entropy of Original Image (bits)	Entropy of Cipher Image (bits)
Proposed Algorithm I			5.8739	7.9969
Proposed Algorithm II			5.8739	7.8909

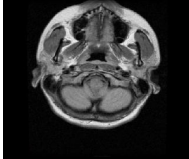
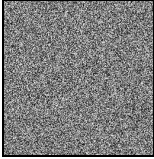
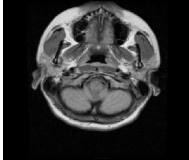
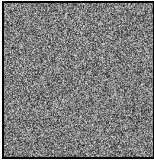
4.4.5 Correlation

Correlation is a measure that computes the degree of similarity between two images. It is a useful measure to judge encryption quality of any cryptosystem. Any encryption system is assumed to be good, if the encryption algorithm hides all attributes of a plain image, and the encrypted image is totally random and highly uncorrelated. If encrypted image and plain image are completely different then their correlation coefficient will be very low, or very close to zero. If correlation is equal to one, then the two images are identical and the encryption method will completely fail. The results of both proposed algorithms shown in Table 9 based on equation 3, indicate that the system is working well.

4.4.6 Peak Signal to Noise Ratio

The PSNR measures the similarity between the original image and the encrypted one. The PSNR value related to the same test images in Table 9 is calculated based on equation 1.

Table 9. Correlation and PSNR between original plain and encrypted images

Proposed Algorithms	Original Image	Cipher Image	Correlation Value	PSNR Value (db)
Proposed Algorithm I			0.0081	11.3778
Proposed Algorithm II			0.0081	11.1309

4.4.7 Encryption/Decryption Time Performance

Measuring the average time required for the encryption and decryption operations are presented in Table 10 for the same image of size (256×256). The table shows the time needed for the header and image operations in seconds.

Table 10. Time in seconds required for encryption and decryption

Proposed Algorithms	Encryption Time for Header Operations (s)	Encryption Time for Image Operations (s)	Decryption Time for Header Operations (s)	Decryption Time for Image Operations (s)	Total Encryption Time (s)	Total Decryption Time (s)
Proposed Algorithm I	100.3	384.5	50.1	502.6	484.8	552.7

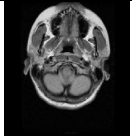
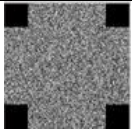

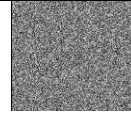
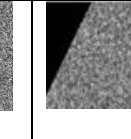
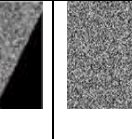

Proposed Algorithm II	147.4	664.3	411.7	449.4	811.7	861.1
--------------------------	-------	-------	-------	-------	-------	-------

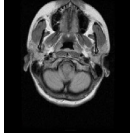
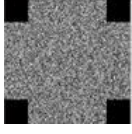


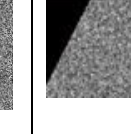
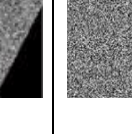
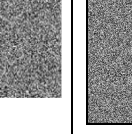
4.4.8 Robustness against Noise and Attacks

An algorithm for encrypting an image should be robust against statistical attacks. This means the system should have high key sensitivity or plain image sensitivity. In section 4.4.3 a test against the key sensitivity is done. Therefore, a small modification, even a single pixel being changed by one bit in the original image, causes a great difference in the cipher-image or it will not decrypt the cipher image. These properties make it difficult for attackers to break the system.

Based on these aspects it is shown in Table 11 below that the proposed algorithms are immune against statistical attack. The Table shows the decryption operation for the cropped cipher image, Gaussian-noised cipher image, compressed cipher image, rotated cipher image, and dithered cipher image. All the attacks are applied in order to test the algorithms confirming that a robust encryption details are used in both algorithms, so the cipher images will not be decrypted after being attacked.

Table 11. Robustness against statistical attacks

Proposed Algorithm	Original Image	Cropped Cipher Image	Gaussian- noised Cipher Image	Compressed Cipher Image	Rotated Cipher Image	Dithered Cipher Image	Deciphered Attacked Image after each attack
Proposed Algorithm I							

Proposed Algorithm II							

4.4.9 Comparison Results

It must be emphasized that the proposed algorithms provide the three security requirements on the header level and on the image level. Also, it should be considered that there must be a standardized way to exchange images in telemedicine so that in a DICOM context, the recovery issues (such as recovery from the database) could be solved by defining a security profile for this approach. Another advantage; the implementation is robust because of using strong cryptographic algorithms (none of them have been broken yet) and the mechanisms are being executed in a secure mode. As a result, it is noticed that the processed images have no relation to its original parts, reducing the probability of an unauthorized people to break the approach.

The proposed algorithm II has a main attractive point that have a strict integrity, referring to the fact that if the encryption key was tampered, then the encrypted image data will not be decrypted and the execution for the algorithm will be broken down. Then it will be known that an attack has happened during the transmission and cause a tamper. It is a secure related issue that just the physician knows the encryption key could be able to decrypt and read the medical image.

Comparing between both proposed approaches with (Kobayashi et al. 2009) that mentioned some limitations in their approach, founding that the confidentiality in (Kobayashi et al. 2009) does not achieve since the decryption key is stored in the header in order to decrypt the received image. Their approach applied on many frames, but our algorithms applied on one frame only.

In addition to that, it is worthwhile to mention that in our proposed algorithms, an optimization is done over the AES-GCM algorithm regarding a software implementation issues. Thus, the code of AES-GCM is written in MATLAB language by means of using (Dworkin, 2007) that contains a recommendation for block cipher modes of operations related GCM. The main point was the modification applied later on the implementation code by using nested IF statement each time instead of using nested FOR loop statement. By exchanging the WHILE statements with IF statements and separating the files, the code becomes needed a time less than before. By this enhancement features our proposed algorithms take an advantages over the compared approach.

Table 12, give comparison results in terms of entropy, PSNR, correlation, and execution time between the three schemes. In Figure 37 the total execution time are drawn. In details, the time required for encryption specified to the three operations: AES-GCM (before and after the enhancement), Whirlpool, and ECDSA are compared in Figure 38. In contrast, the time required for decryption specified to the three operations too is drawn in Figure 39.

Table 12. A comparison results in terms of entropy, PSNR, correlation, and time

Projects	Entropy of Cipher Image	PSNR Value	Correlation Value	Total Encryption	Total Decryption
----------	----------------------------	---------------	----------------------	---------------------	---------------------

	(bits)	(db)		Time (s)	Time (s)
Proposed Algorithm I	7.9969	11.3778	0.0081	484.8	552.7
Proposed Algorithm II	7.8909	11.1309	0.0081	811.7	861.1
(Kobayashi et al. 2009)	7.4764	11.4760	0.0242	876.2	904.2

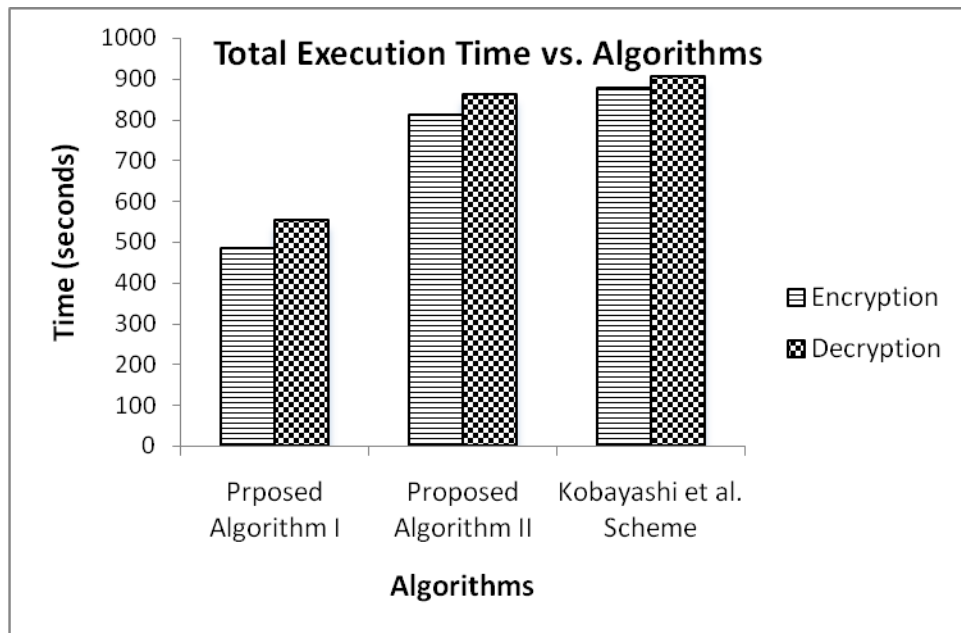


Figure 37. Total execution time needed for the schemes

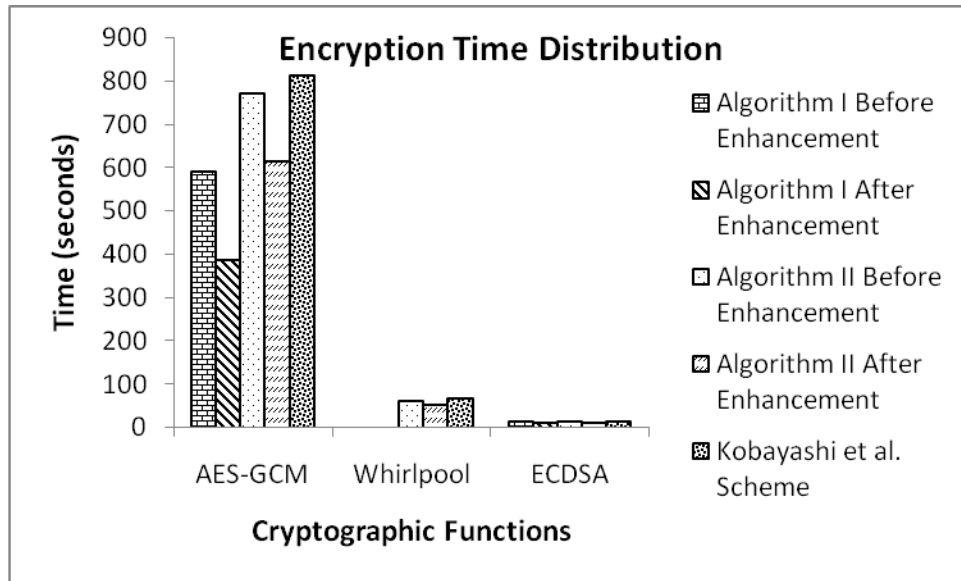


Figure 38. Encryption time needed for AES-GCM, Whirlpool, and ECDSA

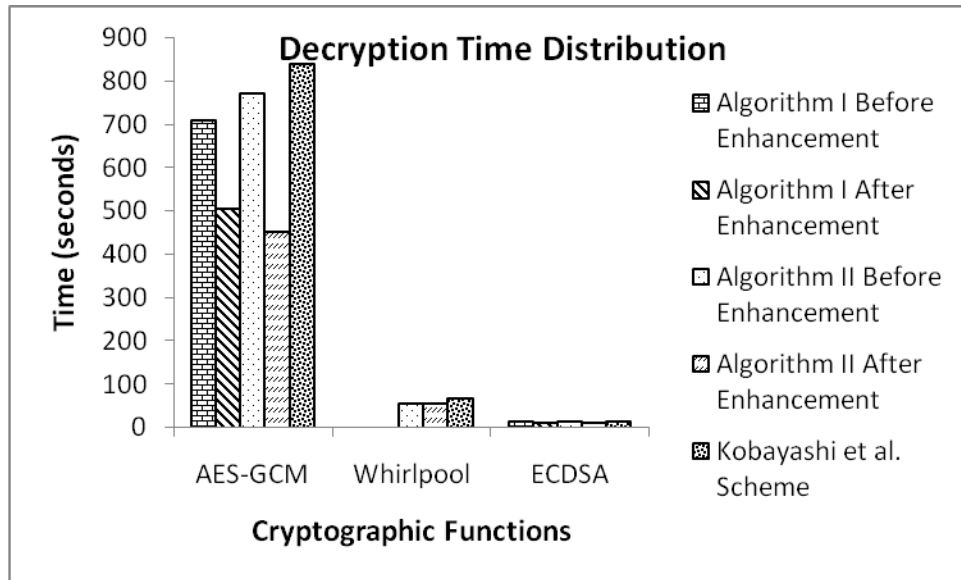


Figure 39. Decryption time needed for AES-GCM, Whirlpool, and ECDSA

It is worthwhile to be noted, that the proposed algorithm I in Figure 38 and 39, is not drawn for a Whirlpool comparison because it does not use the hashing technique. About the ECDSA, all the compared schemes are extremely similar and need a little time for encryption or decryption.

Chapter 5

Proposed Watermarking-based Secured Telemedicine Algorithm

In this chapter we shall see how we will develop a public medical image watermarking algorithm that is resistant to several attacks. The proposed scheme is based on the idea of combining multiple watermarks related to the patient data into the medical image, through digital watermarking algorithm for a telemedicine application. It aims to enhance medical confidentiality protection, origin data authentication, and data integrity control. In this method 3-level DWT is applied to the original image and the concept of region of interest is used. Then a correlation-based technique is used for embedding the watermarks besides using LSB for embedding the fragile watermark. The performance is evaluated by testing the imperceptibility by calculating the PSNR between the original image and the watermarked image. Also testing the robustness by applying different types of attacks and then the correlation between the original and extracted watermarks is calculated.

5.1 Watermark Generation Module

In the proposed algorithm, three watermarks are used so each one will be applied for a specific purpose. There is one authentication watermark and two integrity watermarks used in this project.

5.1.1 Authentication Watermark

The scheme simultaneously inserts different purpose watermarks, starting with the patient information watermark for the purpose of achieved authentication requirement since the

confidentiality is achieved by the embedding process itself. This watermark is generated from the DICOM header and presented in the project as a gray-scale image which consists of the basic application level confidentiality profile attributes that was defined in the header. It contains the patient's personal information, physician's information, image comments, health history, etc. So, the size of the watermark depends on the image size and is related to the existing patient records that are defined, not a fixed one. In the case of the testing image that we used in the algorithm, the size of the watermark is (50 ×60) pixels which equal to 3000 bits. This embedding is done in the DWT third layer of HL horizontal details decomposition of each block in the RONI. The Figure 40 shows a watermark image related to one of the test medical image that we used in the algorithm.

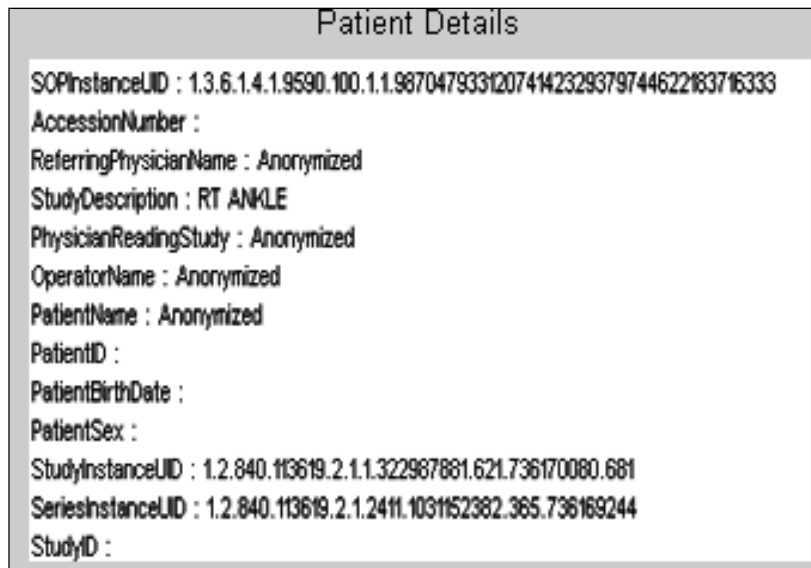


Figure 40. Image of the patient information watermark

5.1.2 Integrity Watermarks

For this type, two watermarks are defined for strict integrity requirement and tamper detection.

- 1) ROI watermark: this watermark is generated by taking the LSB's of all pixels/blocks in ROI region and formed as a binary array values of {0, 1}. It is defined for integrity

purpose and the embedding process is done in the DWT second layer of HH subband diagonal detail decomposition of the block in the RONI region. The size of the watermark depends on the size of the selected region of interest.

- 2) A fragile watermark is generated randomly by the user and known to the recipient. It is embedded in the LSBs in each ROI pixels instead of their bits that embedded in the RONI before. The procedure is done for the purpose of data integrity control by using LSB method. This fragile watermark consists of a randomly 64 bits PN sequence generation. Its extraction and comparison are done of the extracted watermark bits with the originally embedded ones. It provides information on whether and the image has been modified (tamper localization purpose). Figure 41 displays the fragile watermark as a binary image of size (64×1).



(1100101100110010000000010101100001001101100001110011100100001110)

Figure 41. Fragile watermark image

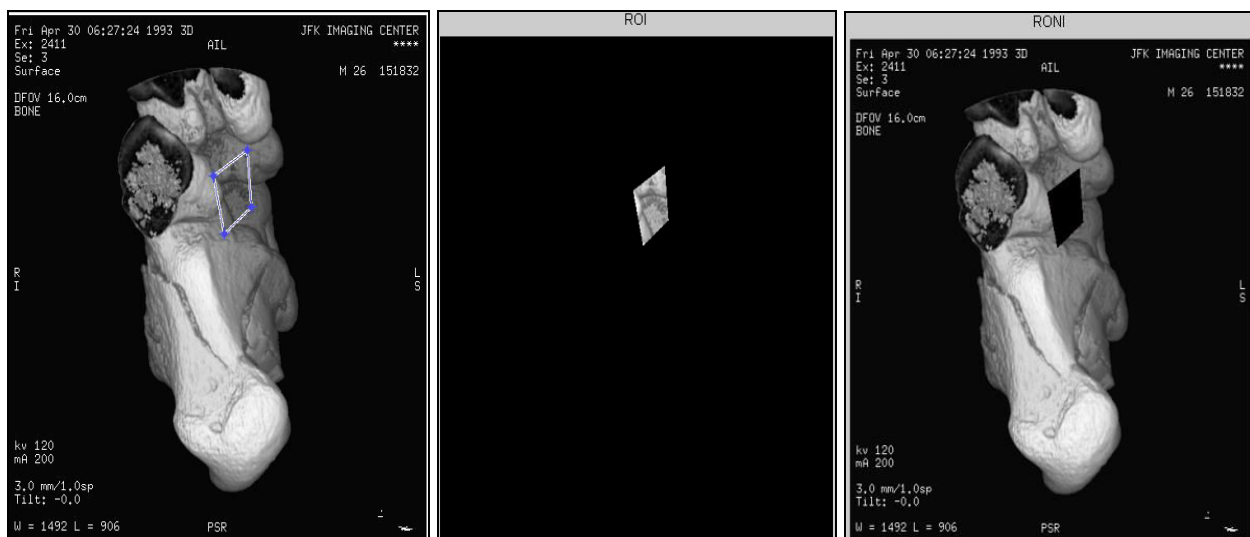
5.2 Image Preprocessing

As mentioned in the algorithm overview, the multiple generated watermarks are embedded and extracted according to the DWT and correlation-based technique, besides using the LSB method for the fragile watermark. Before the embedding, the original image is pre-processed and the following concepts in this subsection are applied to the image.

The ROI has somewhat different meanings and definitions for the different applications, so it can be defined simply as a polygon or as any combination of irregular shapes to represent a subset of data as shown in Figure 42. The Figure shows that the selection of the ROI is done by a

MATLAB roipoly tool to be formed as a polygon shape with a small size made by the user. By software implementation issue the ROI is separated from the RONI and while dividing the plain image into blocks of equal size (16×16) and the blocks that enter the borders of the ROI even with just one pixel, it will be considered as an ROI block. The remaining blocks will be considered as RONI blocks. The previous step is done by scanning the blocks and flagged the meant region with ones whereas the other region is flagged by zero. Figure 43 explains how the image plain divided into blocks and determining ROI/RONI blocks.

The ROI acts as the important parts of the data based on the targeted application, where selecting these sub-regions will enable some special processing to be done that is not applied to the whole image area. Any distortion in ROI may lead to undesirable result for patient. To secure medical images by watermarking, the ROI should be protected and the watermarks can be applied on the remaining part of the image, i.e. in the RONI region.



(a) Selected ROI

(b) Separated ROI

(c) Separated RONI

Figure 42. ROI selection and RONI separation from polygon shape of ROI

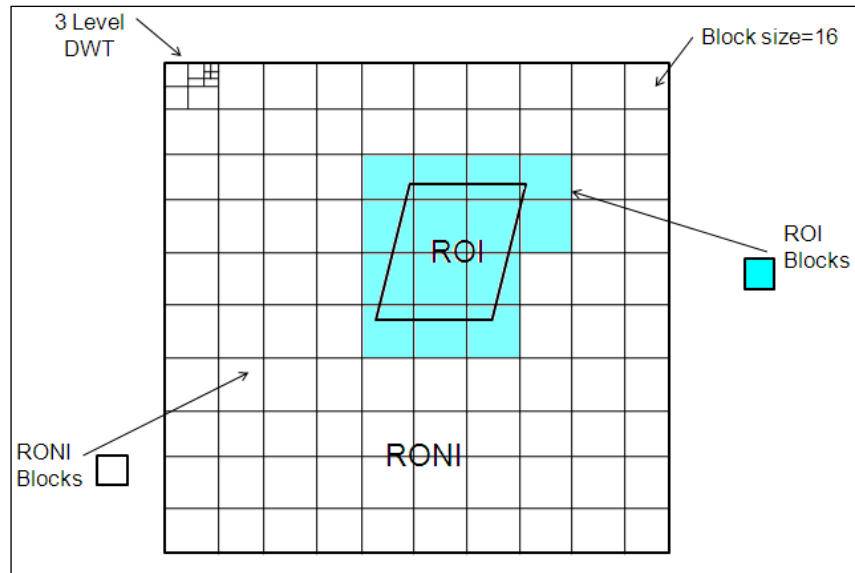


Figure 43. Dividing the image into blocks and determining ROI/RONI blocks

5.3 Watermarks Embedding/Extraction in RONI

The watermarking algorithm consists of two procedures; watermark embedding and watermark extraction that applied for the two regions: ROI and RONI separately. The two procedures are described in the following subsections.

5.3.1 Watermarks Embedding Procedure in RONI

In general, the embedding operation is done in the RONI and in the ROI separately, then they will be combined together to perform the watermarked image. Figure 44 shows the embedding procedures for both regions, before discussing the details about each region separately.

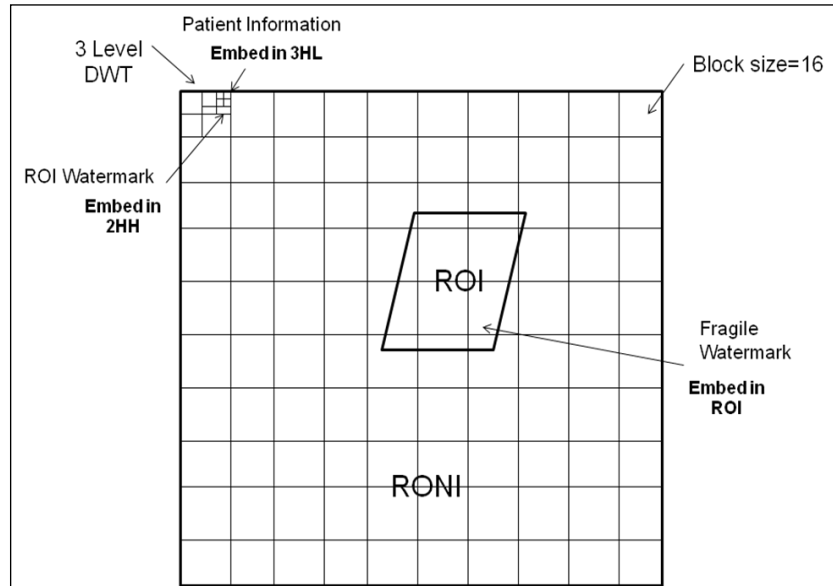


Figure 44.

Embedding

procedures for ROI and RONI

About RONI embedding procedure, after illustrated the image by ROI and RONI, and dividing it into blocks of size 16×16 pixels, we take the RONI region and the 3-levels DWT are applied to each block. So each block of size 16×16 has a corresponding block of size 8×8 in the first decomposition level, a block of 4×4 coefficients in the second level, and a block of 2×2 in the third level. Figure 45 illustrates the pyramid structure of a 3-level wavelet decomposition of each block, including a horizontal detail at the highest decomposition level (3HL), and 9 decomposition corresponding to the approximation (LL), vertical details (LH), and diagonal details (HH) at each of the three levels. The Haar wavelet is selected as the mother wavelet for the image blocks decomposition aiming to exploit the dyadic rationality of the coefficients in order to increase watermark robustness.

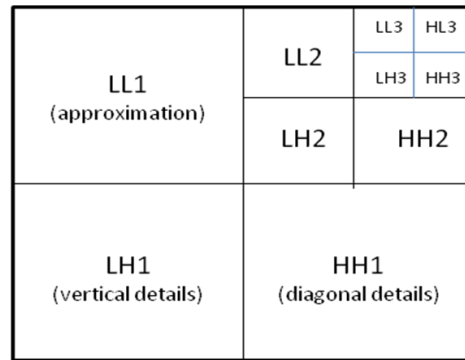


Figure 45. Three level DWT decomposition of each block

A block diagram displaying the steps of embedding the multiple watermarks in a cover image is shown below in Figure 46.

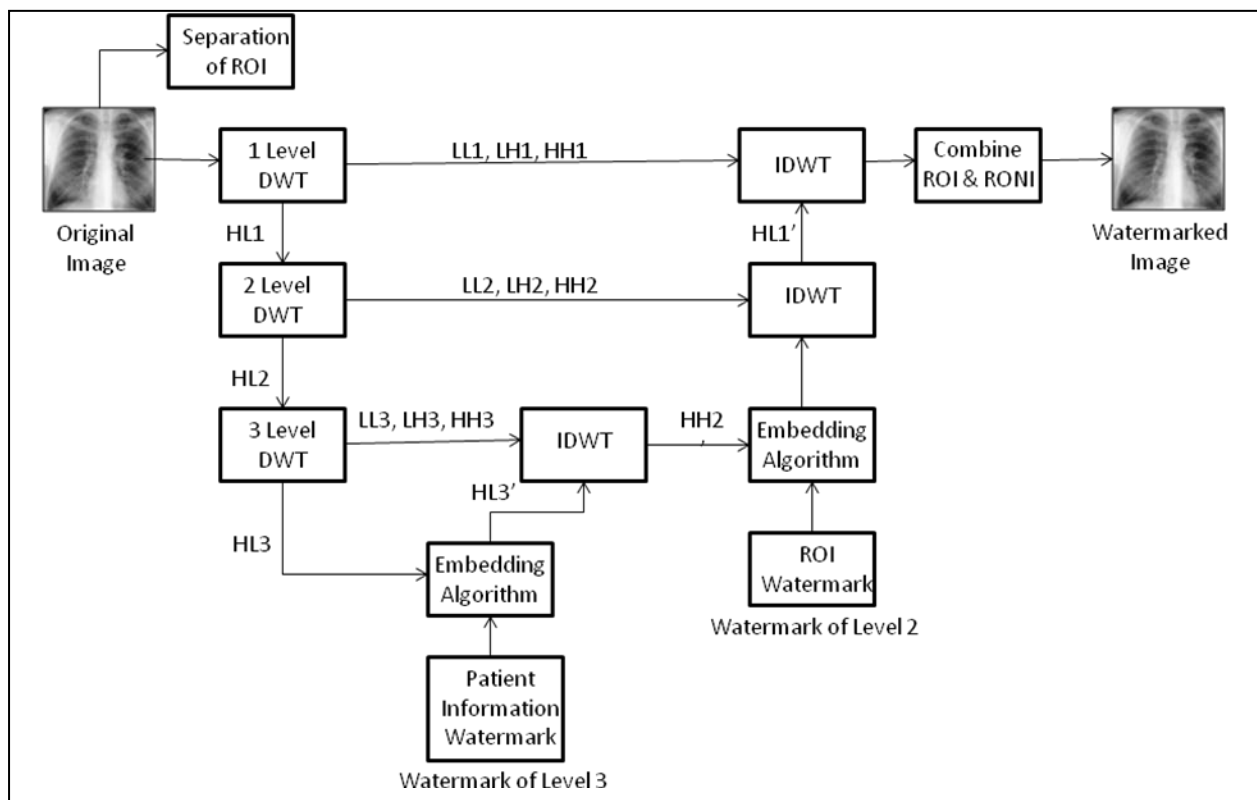


Figure 46. A block diagram of RONI embedding procedure

The RONI blocks are prepared for the following embedding steps after the image processing steps. Based on the block diagram above:

Step 1: for a 1-level DWT, decompose each RONI blocks into 4 sub-bands: LL_1 , HL_1 , LH_1 , and HH_1 .

Step 2: for a 2-level DWT, apply DWT to the HL_1 sub-band to get another 4 sub-bands (LL_2 , HL_2 , LH_2 , and HH_2) and choose the sub-band (HL_2) shown in Figure 47(a)

Step 3: for 3-level DWT, we applied DWT to the HL_2 sub-band to get 4 sub-bands (LL_3 , HL_3 , LH_3 , and HH_3) and chose the sub-band (HL_3) as shown in Figure 47(b)

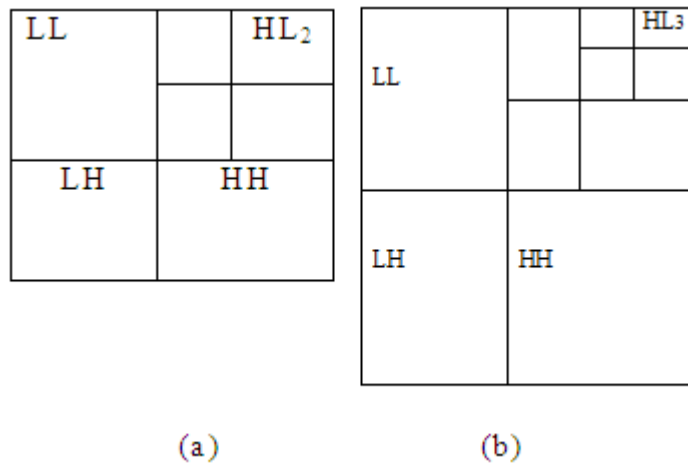


Figure 47. Choosing the sub-bands for each block (a) HL_2 and (b) HL_3

Step 4: the patient information watermark that will be embedded in HL_3 is reformulated into a sequence of ones and zeros in order to make it a binary matrix.

Step 5: the embedding algorithm is applied by; generating PN sequences to designate “1” and “0”. Then finding two highly uncorrelated PN sequence: $pn_sequence_1$ and $pn_sequence_0$. Where the size of both sequences will be the same as the size of the embedding block (in our case in the third level, will be equal to 2×2) in order to apply the matrix addition property.

When the watermark bit = 0; then the addition is done between $pn_sequence_0$ matrix of size 2×2 and the block of HL3 is of size 2×2 . The addition result will be a matrix of size 2×2 embedded in the block of HL3 with a gain factor K.

When the watermark bit = 1; then the addition is done between $pn_sequence_1$ matrix of size 2×2 and the block of HL3 of size 2×2 . The addition result will be matrix of size 2×2 embedded in the block of HL3 with a gain factor K.

This method will be applied until embedding all the patient information watermark bits.

Step 6: apply the inverse DWT (IDWT) using the 4 sets DWT coefficients. However, apply IDWT to the modified coefficients of level 3 (LL_3 , HL_3 , LH_3 , and HH_3) to reconstruct the chosen sub-band of level 2 (HH_2).

Step 7: the ROI watermark is embedded in the HH_2 by applying the same method for the patient information watermark that mentioned in step 5. But the size of both sequences in this case to be embedded in the second level, will be equal to 4×4 , and so the result of matrix addition will be a matrix of size 4×4 too, embedded in the block of HH_2 with a gain factor K. Repeat the embedding process with one bit each time of embedding, until the watermark bits are handled.

Step 8: apply IDWT to the modified coefficients of level 2 (LL_2 , HL_2 , LH_2 , and HH_2) to reconstruct the chosen sub-bands of level 1 (HL_1).

Step 9: apply IDWT to the modified coefficients of level 1 to reconstruct the watermarked medical image (cover object).

Step 10: combine the ROI and RONI regions, to reconstruct the watermarked medical image.

It must be noted that, two different watermarks with different sizes will be embedded into two different sub-bands (in our case HH_2 and HL_3), where the size of the block in the selected sub-bands must not exceed the size of the selected watermark that is to be embedded into the

specified sub-band. Notice that the embedding is done as 1 embedding bit of watermark each time.

In this research, the medical image was of size 512×512 . The size of each block is 16×16 , so the image has 1024 blocks. After applying 1-level DWT, the resulted four sub-bands were each of size 8×8 . When we applied DWT to one of these sub-bands; the resulted four sub-bands were each of size 4×4 . At last we applied DWT to level 3 to one of the sub-bands; and the resulted four sub-bands were each of size 2×2 . The chosen sub-band of level 1, resulted in 256×256 maximum message size that can be embedded, and the chosen sub-band of level 2 resulted in 128×128 maximum message (ROI watermark) size that can be embedded to HH2 and finally a 64×64 maximum message (patient information) size that can be embedded to HL₃.

5.3.2 Watermarks Extraction Procedure in RONI

In general, the extraction procedure is done in the ROI and RONI regions as shown in Figure 48.

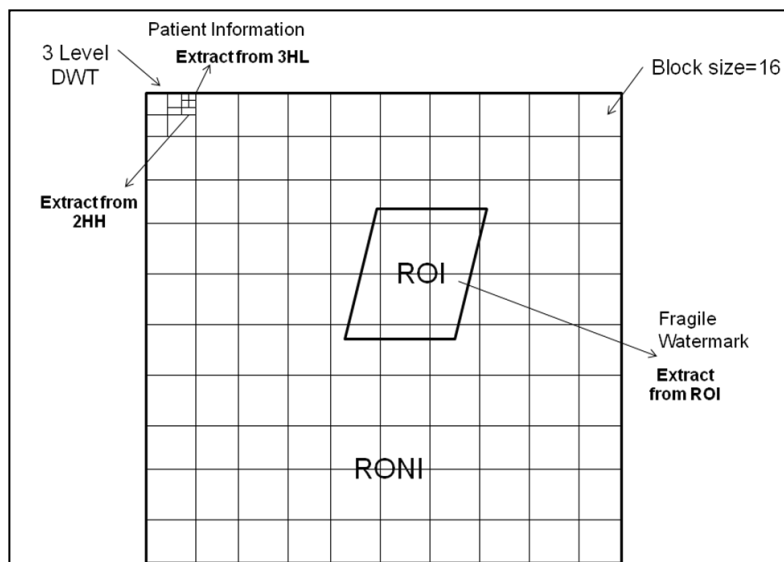


Figure 48. The extraction procedures for ROI and RONI

A block diagram below is showing the steps of extracting watermarks from watermarked image in RONI as Figure 49.

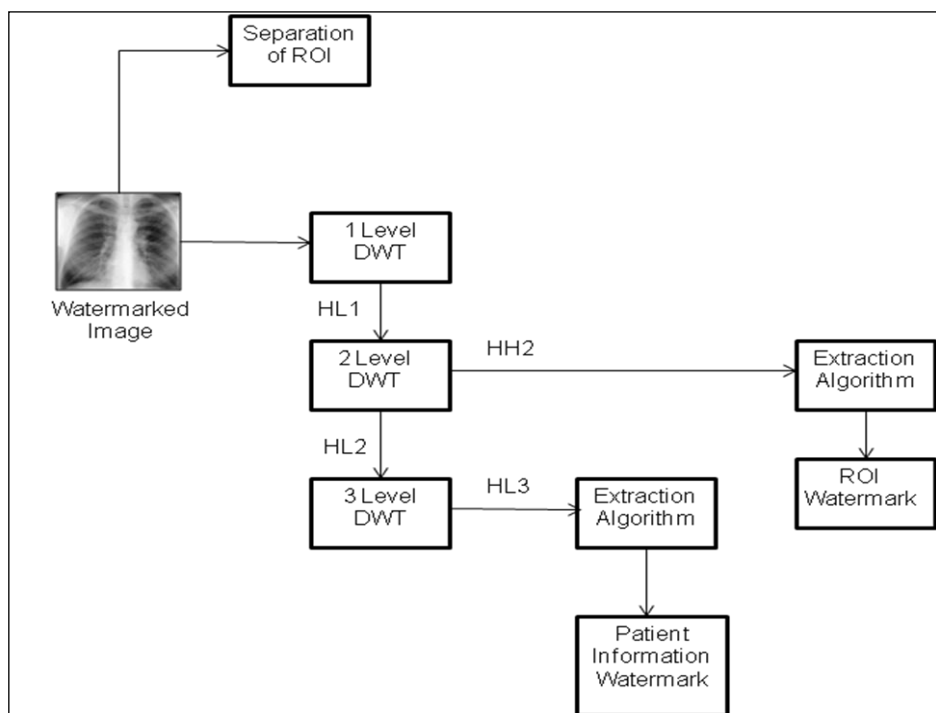


Figure 49. A block diagram of RONI extraction procedure

The extraction steps based on the block diagram above are:

Step 1: Separate ROI region from the watermarked image, in order to apply the procedure on the RONI only.

Step 2: divide the watermarked image into blocks of size 16×16 .

Step 3: apply DWT to the watermarked image 3 times and determine the 4 sub-bands: LL, HL, LH, and HH for level 1, 2 and level 3 respectively, where HL_3 sub-band contains the patient information watermark that has to be extracted, HH_2 sub-band contains the ROI watermark.

Step 4: when recovering the watermarks, the same pseudo-random noise generator algorithm is defined its correlation with the noise pattern and seeded with the same key. Throughout

detection, the pattern with the higher resulting correlation is used. The recovery procedure is repeated through the entire PN sequence till recovering all the bits of the watermark.

5.4 Watermarks Embedding/Extraction in ROI

The two procedures are described in the following subsections.

5.4.1 Watermarks Embedding Procedure in ROI

The region of interest has one watermark to be embedded and extracted. A block diagram in Figure 50 is showing the steps of embedding a fragile watermark in a cover image.

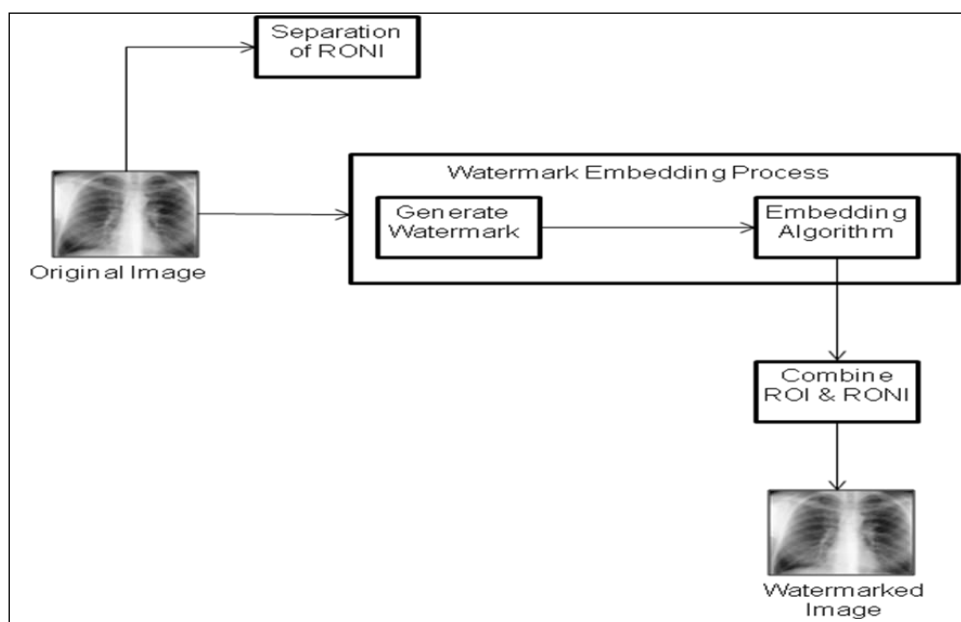


Figure 50. A block diagram of ROI embedding procedure

The embedding procedure includes the following steps:

Step 1: separate the RONI from the original image in order to apply the fragile watermark in the ROI. And divide the image into blocks of size 16×16 .

Step 2: Generate the fragile watermark PN sequence by the user randomly.

Step 3: The fragile watermark bits are embedded in the LSBs in each ROI pixels instead of their bits that embedded in the RONI before with one bit each time of embedding using LSB method until the watermark bits are carried out. The remaining blocks in the ROI without embedding, will be embedded by zero's using LSB method too.

Step 4: combine the ROI and RONI to reconstruct the watermarked image.

5.4.2 Watermarks Extraction Procedure in ROI

The extraction of the fragile watermark is done by the procedure shown in a block diagram below for Figure 51.

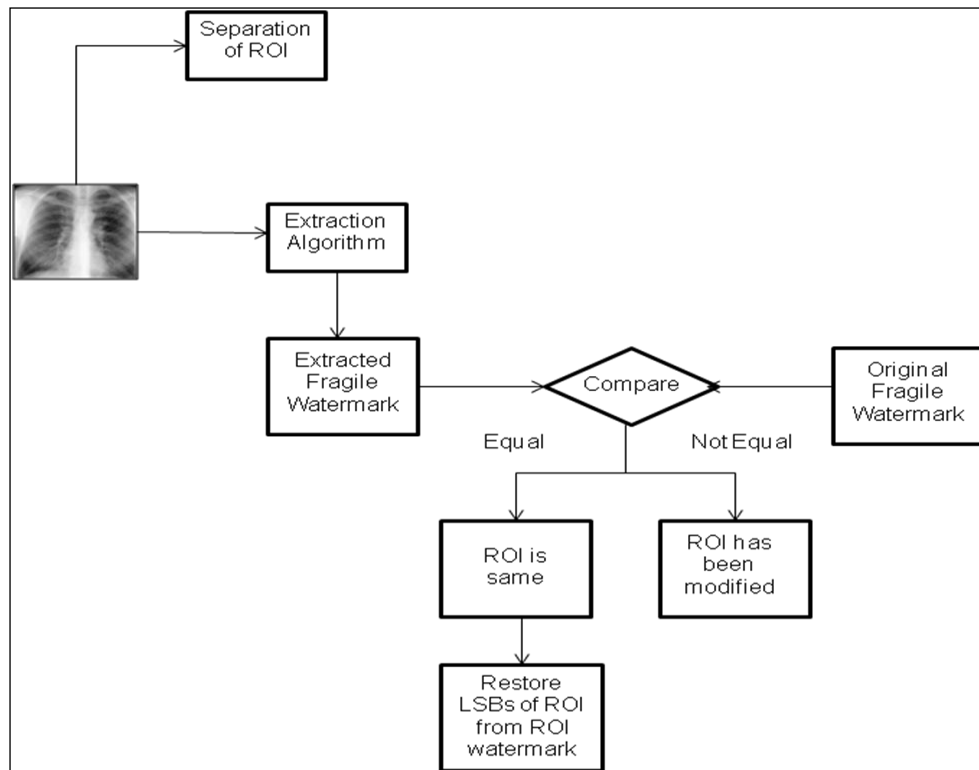


Figure 51. A block diagram of ROI extraction procedure

The extraction process steps are:

Step 1: separate RONI from the watermarked image in order to extract the watermark from the ROI. And divide the image into blocks of size 16×16 .

Step 2: apply the extraction algorithm using LSB method on each block of the ROI so the watermark bits are subsequently extracted.

Step 3: after retrieving all watermark bits, do a comparison between the extracted watermark bits with the originally embedded ones. If they are the equal, then ROI is the same. So restore LSBs of ROI from ROI watermark. If they are not equal, then ROI is modified.

5.5 Performance Evaluation of the Algorithm

The algorithm was tested on different medical images (MRI and X-ray) of different sizes using MATLAB 7.6. The performance of this algorithm was evaluated by studying the visibility of the watermarked image and the robustness of this algorithm to different kinds of attacks. In this section we will deal with many types of attacks.

5.5.1 Setup of MATLAB-based Simulation Experiments

Several simulation experiments are done in order to test and evaluate the effectiveness of the proposed algorithm. The main performance evaluation metrics are: imperceptibility, authentication, and integrity verification.

Imperceptibility is measured by the PSNR which provides an efficient measure of image distortion. It is observed later, that the high PSNR values obtained represent the transparency of the proposed technique. The larger the PSNR, the better is the image quality.

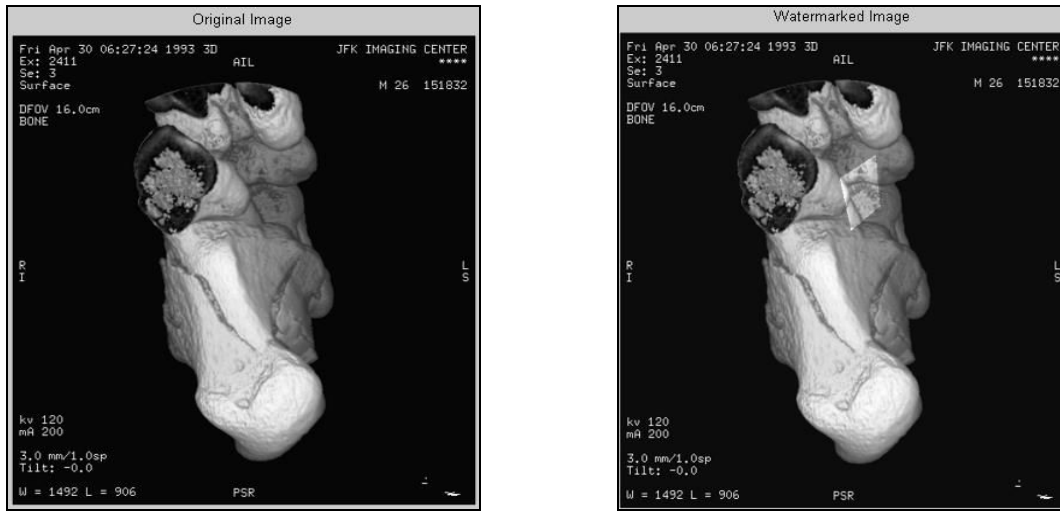
The performance of the scheme in terms of robustness of the watermark without applying attacks was evaluated through measuring the correlation between the extracted watermark and the original one to determine how closely the original resembles the extracted watermark. The range of the correlation is in between 1 and 0 where 1 indicates that the image is exactly the same while the value of 0, means that there is no correlation between the original image and the extracted watermark, such the image is unrecognizable at all. The patient information watermark were extracted and subsequently compared with the originally embedded one; showing the percentage of similarity in the extracted watermarks confirming on the authentication metric. Besides the integrity verification for the fragile watermark is checked to find the similarity between the extracted and the reference fragile watermark.

In addition, a test is done to show whether a watermark can survive against different modifications to the image it is embedded in, such as cropping, white Gaussian noise, JPEG compression, and dithering attacks of the watermarked images.

Also, the simulation test and evaluation is done using StirMark benchmark 4.0. It is a generic tool for simple robustness testing of image watermarking algorithms used by researchers to automatically try to remove watermarks created by attacks (Petitcolas et al. 1998).

5.5.2 Imperceptibility Results

The visibility of this algorithm was tested by calculating the PSNR between the original image and the watermarked image. By taking right (RT) ankle medical image as an original image shown in Figure 52(a), and embedding all the watermarks to get the watermarked image as shown in Figure 52(b), the PSNR value was calculated as shown below.



(a)

(b)

Figure 52. (a) The original image, (b) the watermarked image, PSNR value = 90.8481 db

As shown from the experimental result that we did above, embedding the watermarks in HH and HL sub-bands have shown high PSNR values and high imperceptibility as well. The two sub-bands didn't affect the visibility of the image.

5.5.3 Authentication Results

1) Without applying attacks

We studied the robustness of the extracted patient information watermark from the sub-band HL3 in RONI. Then the similarity between the extracted watermark and the original watermark was computed using the correlation factor. In the following Figure 53(a) the original patient information watermark image is shown, and Figure 53(b) the extracted watermark image is shown along with the correlation value.

Patient Details	Recovered Message (Patient Details)
SOPInstanceUID : 1.3.6.1.4.1.9590.100.1.1.98704793312074142329379744622183716333	SOPInstanceUID : 1.3.6.1.4.1.9590.100.1.1.98704793312074142329379744622183716333
AccessionNumber :	AccessionNumber :
ReferringPhysicianName : Anonymized	ReferringPhysicianName : Anonymized
StudyDescription : RT ANKLE	StudyDescription : RT ANKLE
PhysicianReadingStudy : Anonymized	PhysicianReadingStudy : Anonymized
OperatorName : Anonymized	OperatorName : Anonymized
PatientName : Anonymized	PatientName : Anonymized
PatientID :	PatientID :
PatientBirthDate :	PatientBirthDate :
PatientSex :	PatientSex :
StudyInstanceUID : 1.2.840.113619.2.1.1.322987881.621.736170080.681	StudyInstanceUID : 1.2.840.113619.2.1.1.322987881.621.736170080.681
SeriesInstanceUID : 1.2.840.113619.2.1.2411.1031152382.365.736169244	SeriesInstanceUID : 1.2.840.113619.2.1.2411.1031152382.365.736169244
StudyID :	StudyID :

Figure 53. (a) Original watermark, (b) extracted watermark, correlation = 0.9811

2) With attacks

- **Effect of cropping attack:** we cropped the watermarked image by different block sizes.

The block cropping is done on the four corners: up right, up left, down right, and down left.

The attacked watermarked image at different values of block size is shown in Figure 54.

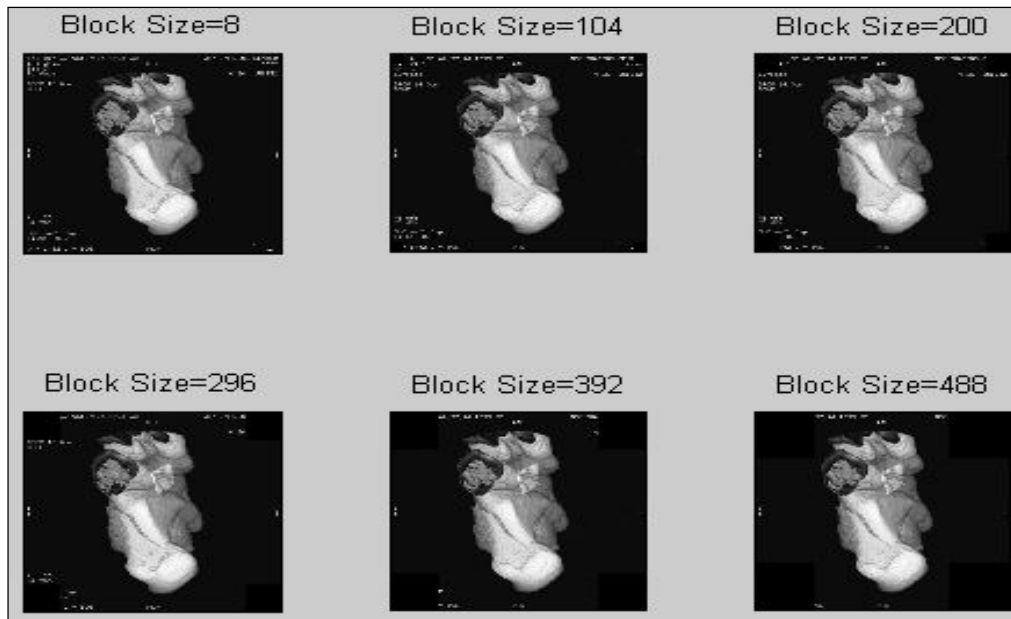


Figure 54. Watermarked image cropping with different values of block size

The extracted watermark (Patient information) for HL3 besides the correlation and PSNR results at different values of block size are shown in Figure 55, Figure 56 respectively.

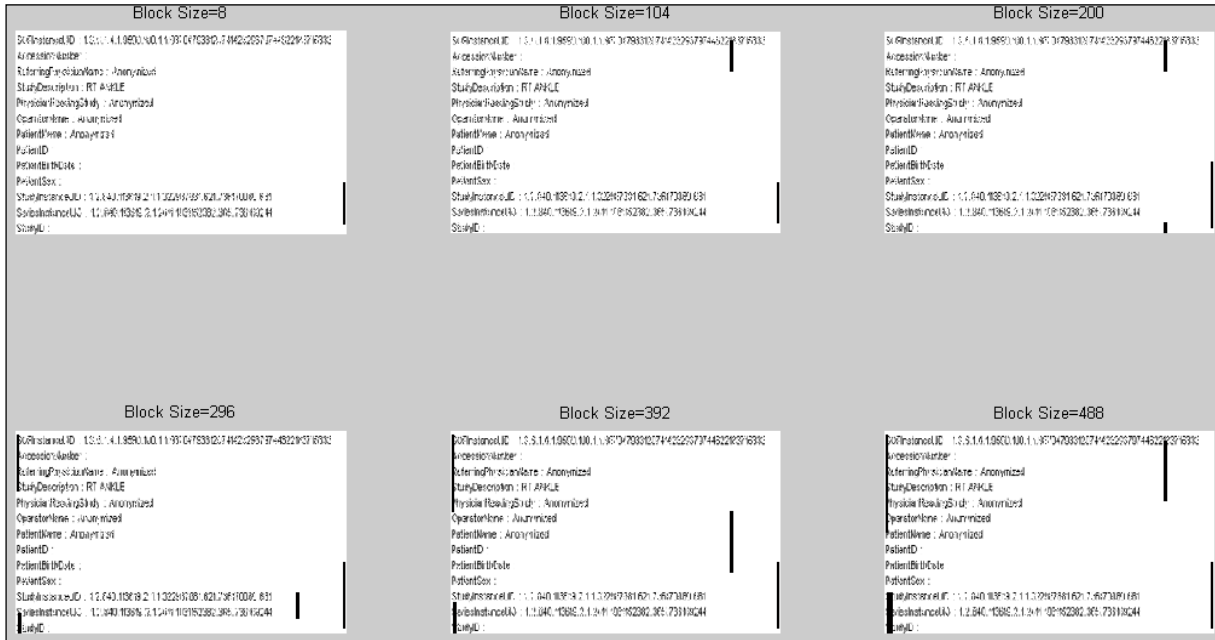
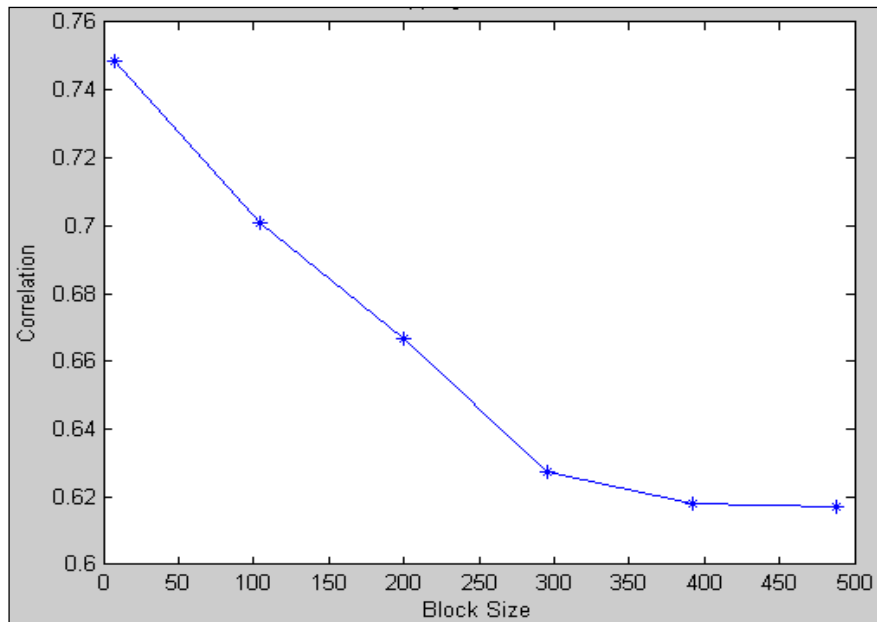
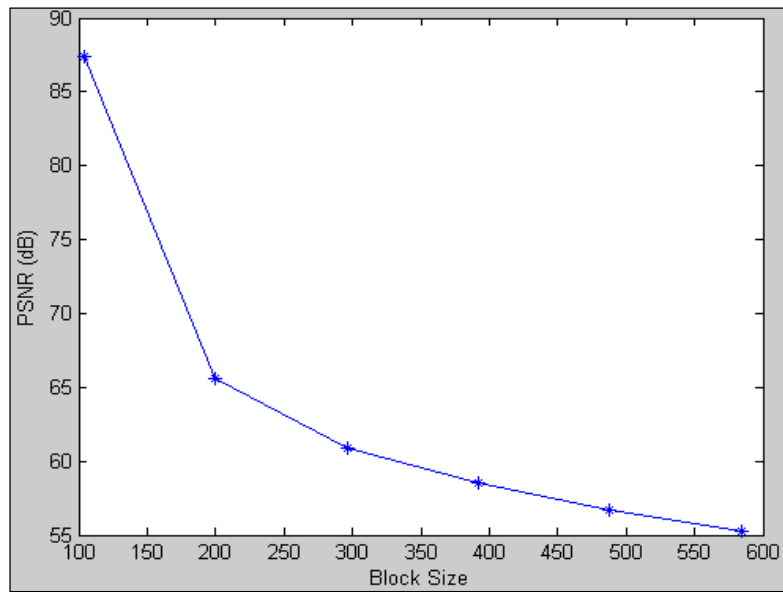


Figure 55. Extracted watermark (patient information) after cropping



(a)



(b)

Figure 56. (a) Correlation vs. block size and (b) PSNR vs. block size; after cropping

- Effect of Gaussian noise:** when adding the Gaussian Noise to the watermarked image, we fixed the value of the variance to zero and changed the value of mean from 0 to 1 of a 0.2 scale; the results of the attacked watermarked image is shown in Figure 57.

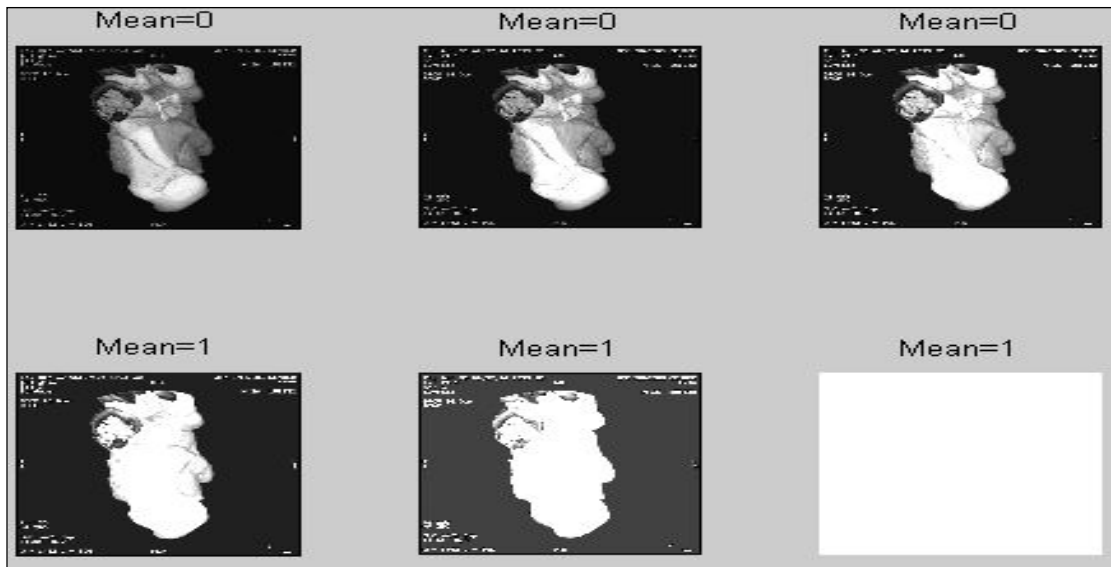


Figure 57. Gaussian attack with different mean values on the watermarked image

The extracted watermark (Patient information) for HL3 in addition to the correlation between the original and extracted watermark, and PSNR results at different values of the mean are shown in Figure 58, Figure 59 respectively.

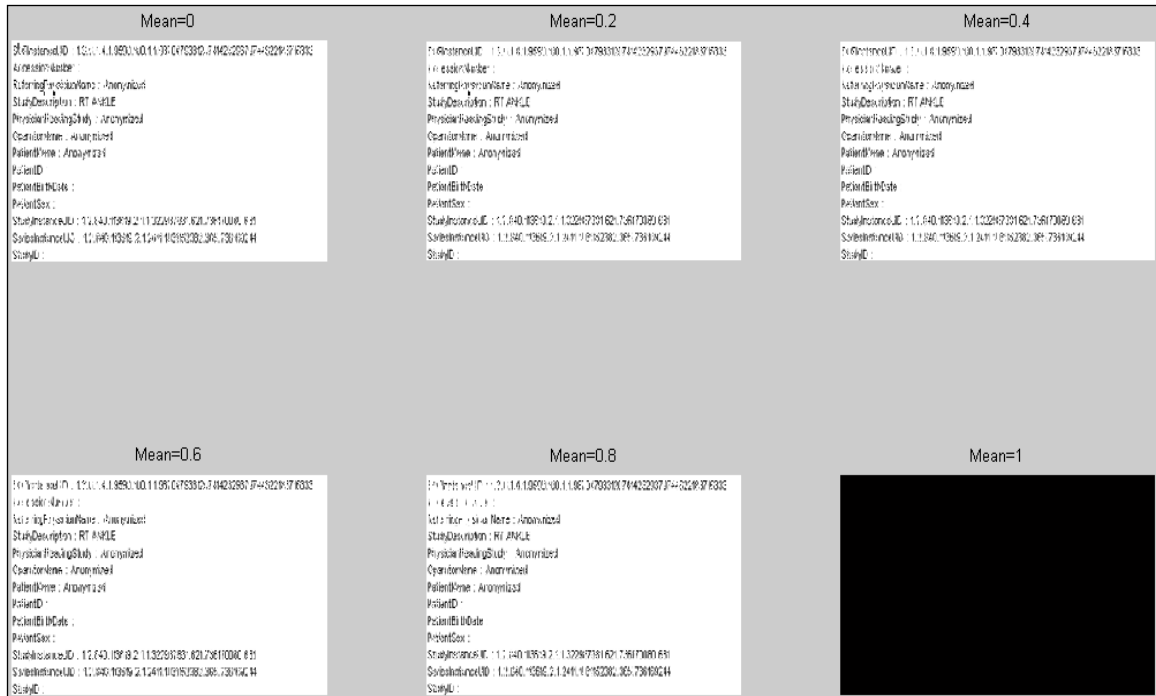
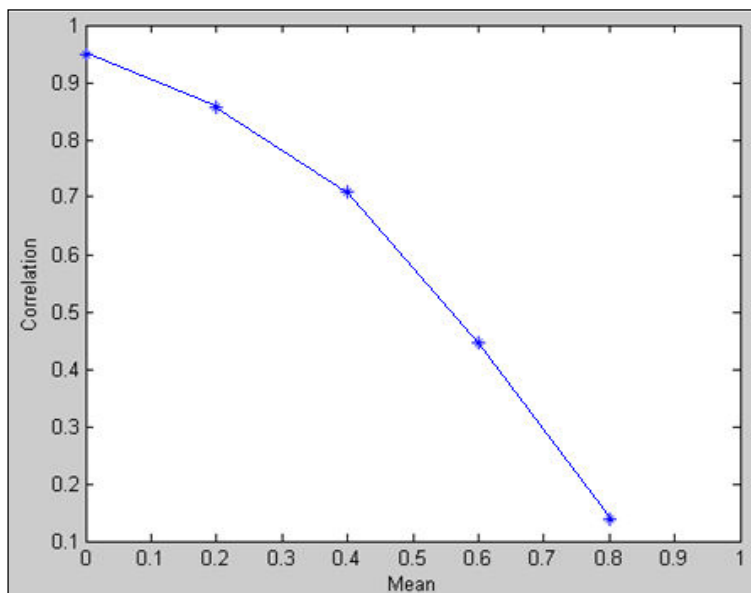


Figure 58. Extracted watermark (patient information) from HL3 after Gaussian attack



(a)

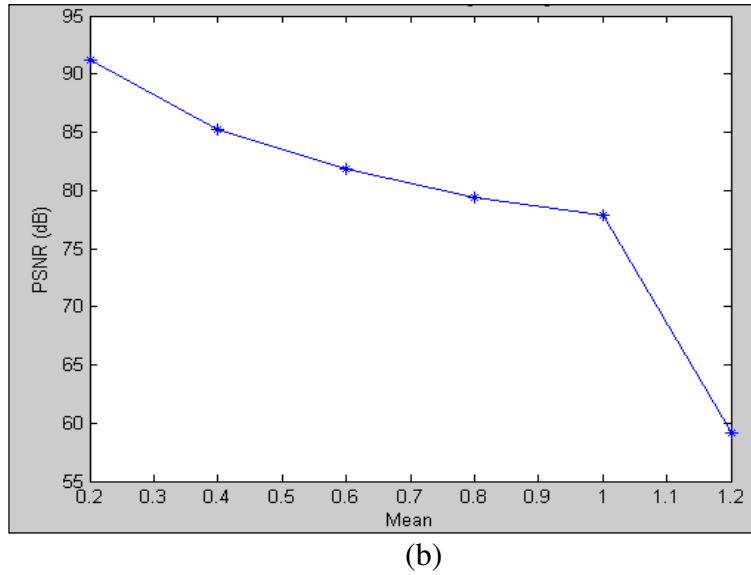


Figure 59. (a) Correlation values vs. mean and (b) PSNR vs. mean; after Gaussian attack

- **Effect of JPEG compression:** when applying the JPEG compression to the watermarked image, with different values of quality; the result of attacked watermarked image is shown in Figure 60.

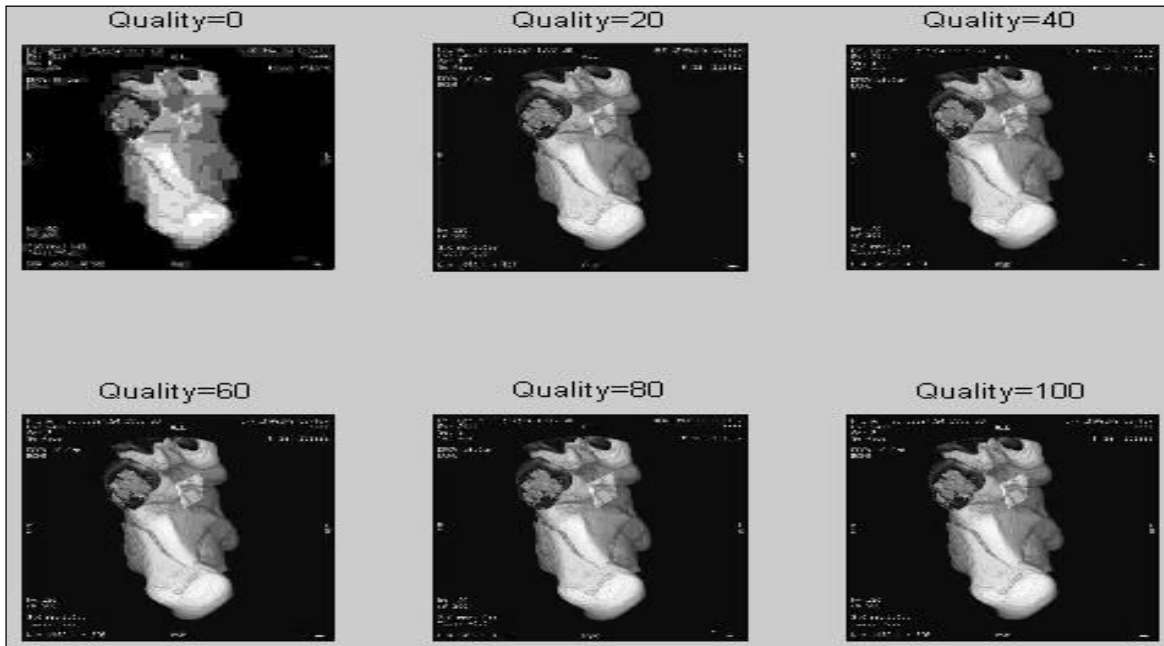


Figure 60. Compression attack of different quality values on the watermarked image

The extracted watermark (Patient information) for HL3 besides the correlation and PSNR results at different values quality are shown in Figure 61, Figure 62 respectively.

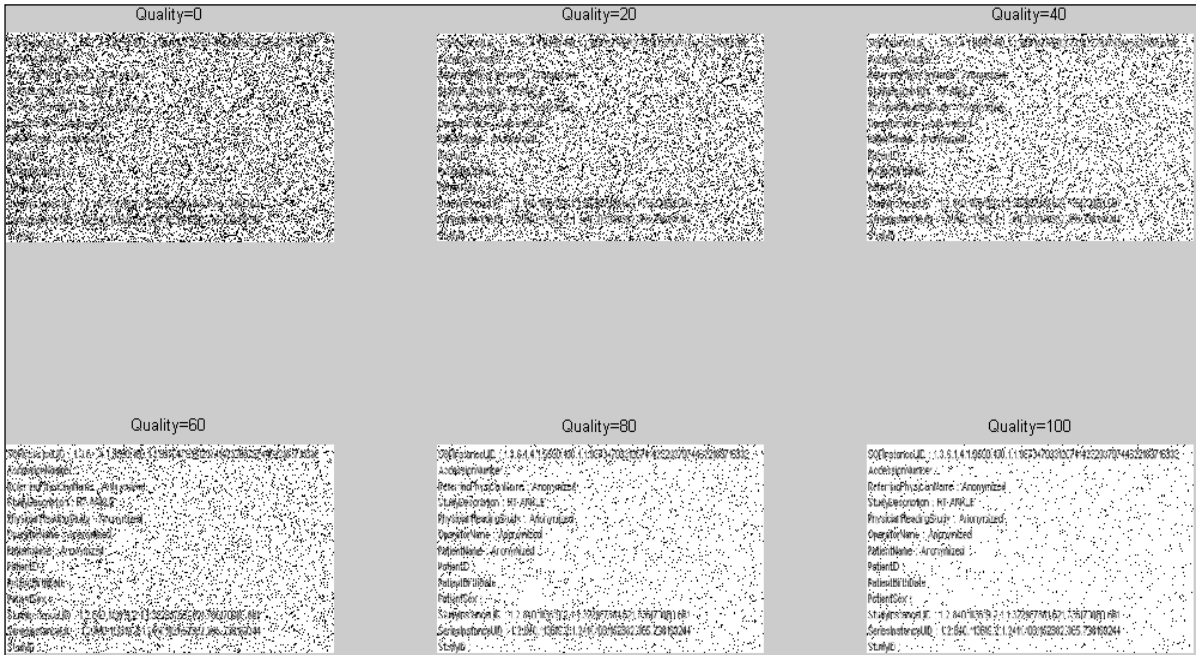
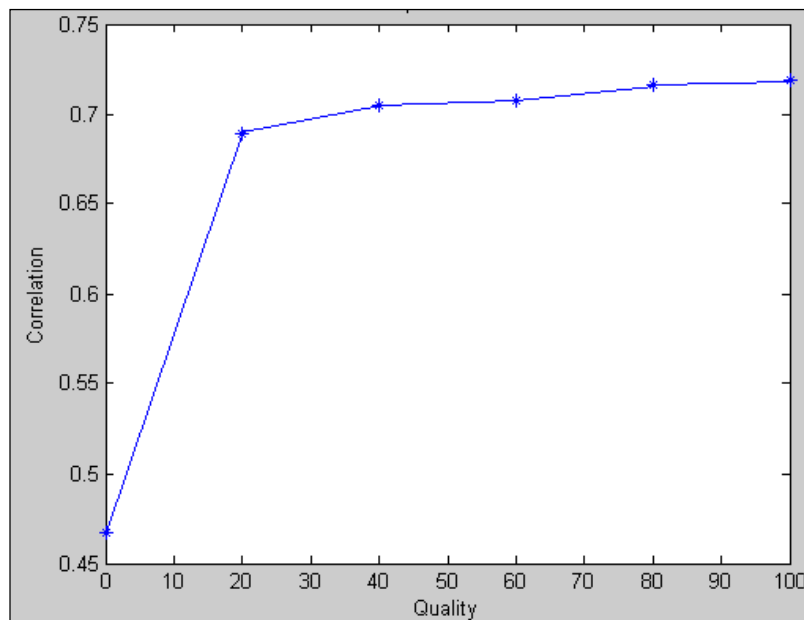
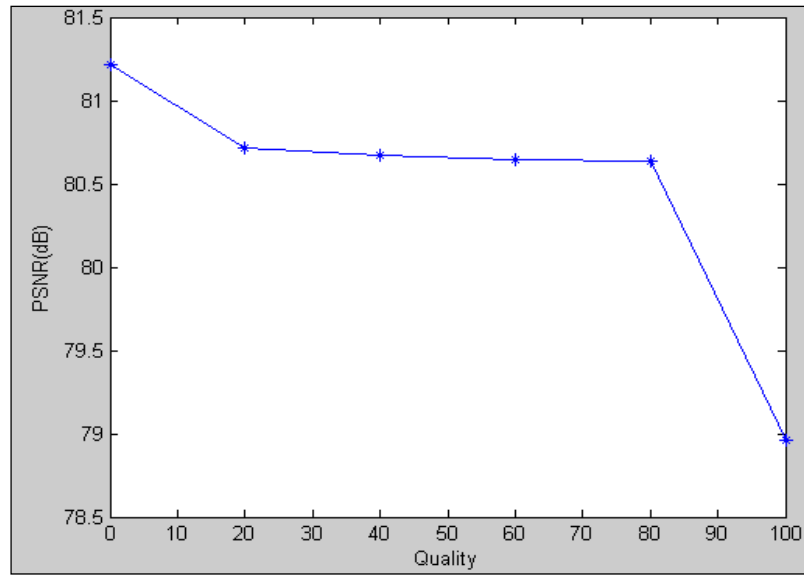


Figure 61. Extracted watermark (patient information) from HL3 after compression attack



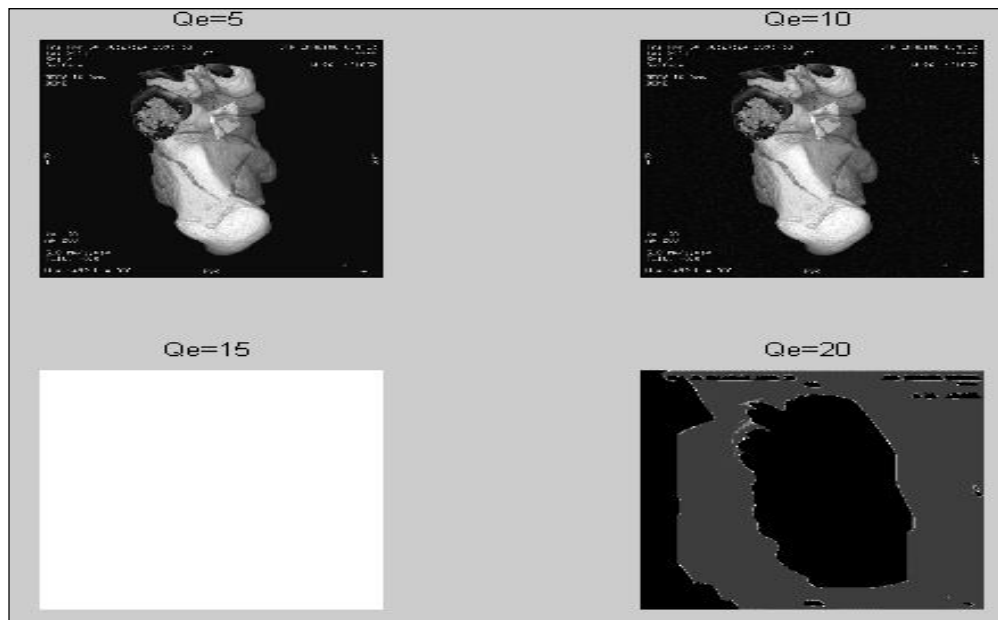
(a)



(b)

Figure 62. (a) Correlation vs. quality (b) PSNR vs. quality after JPEG compression attack

- **Effect of dithering:** when applying the dithering attack to the watermarked image, with different values of quality enhancement (Q_e); the result of attacked watermarked image is shown in Figure 63.

Figure 63. Dithering attack of different Q_e values on the watermarked image

The extracted watermark (Patient information) for HL3 with the correlation and PSNR values at different Q_e are shown in Figure 64, Figure 65 respectively.

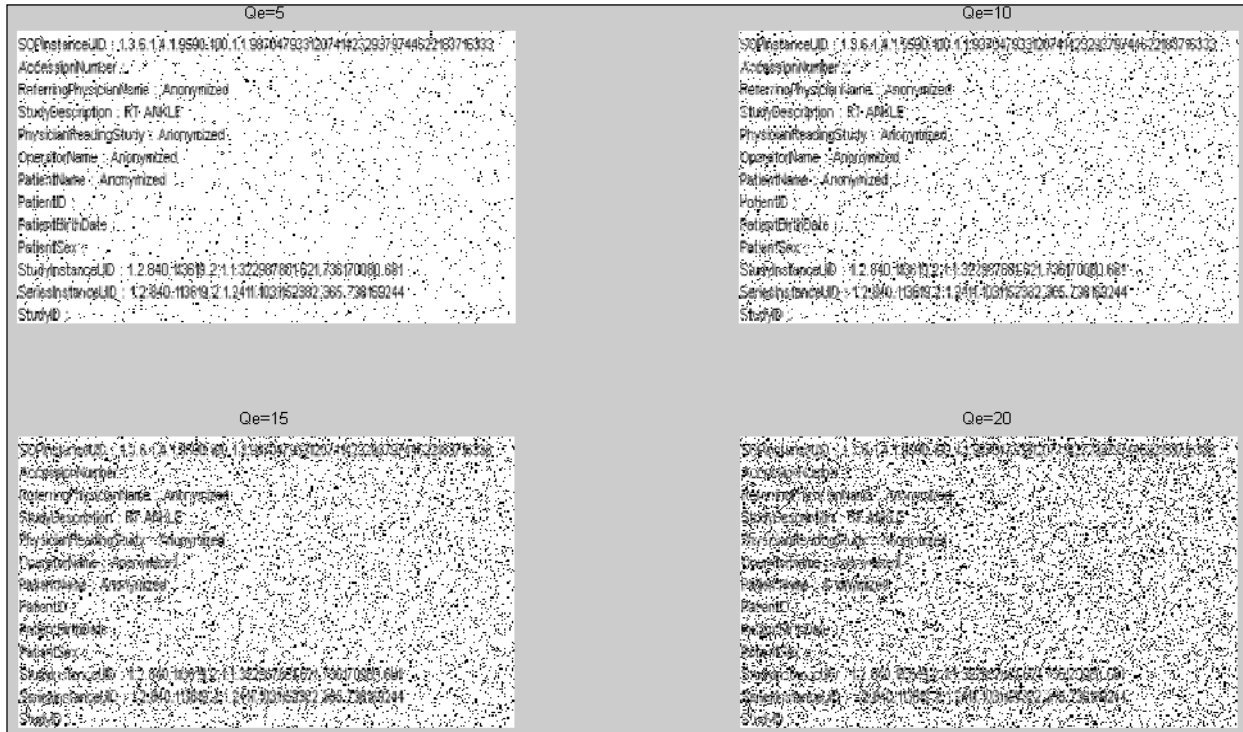
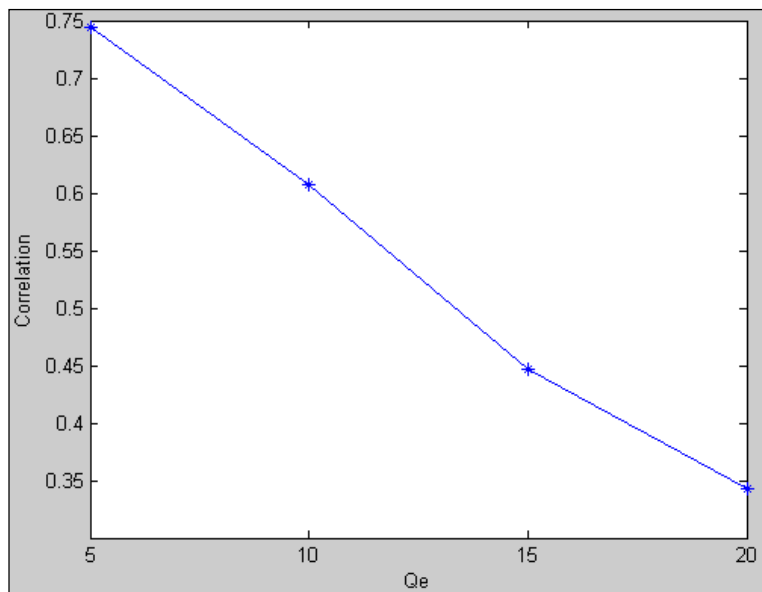


Figure 64. Extracted watermark (patient information) from HL3 after dithering attack



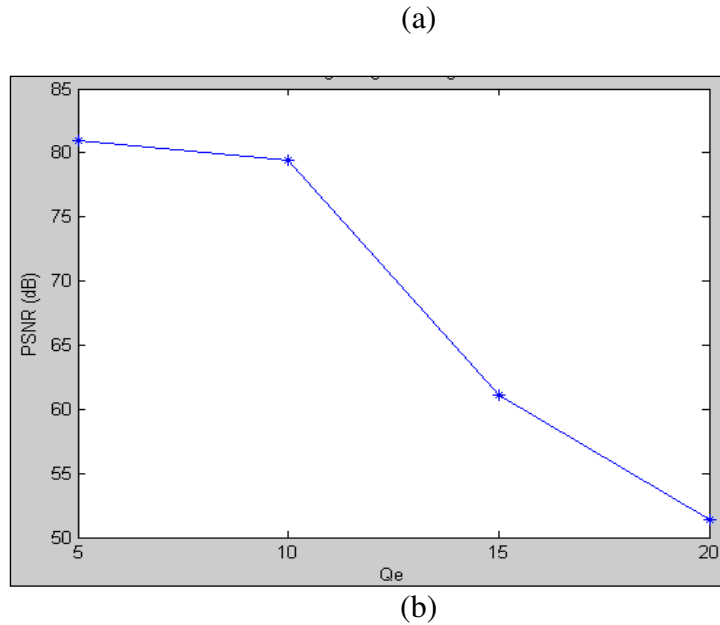


Figure 65. (a) Correlation vs. Q_e and (b) PSNR vs. Q_e after dithering attack

5.5.4 Integrity Verification

1) Without applying attacks

We extracted the fragile watermark from the ROI region. Then integrity verification is done; if the original watermark and the extracted fragile watermark were equal then restoring the original LSBs into ROI. The similarity between the extracted watermark and the original watermark was computed using the correlation factor. In the following Figure 66(a) the original fragile watermark image is shown, and Figure 66(b) the extracted watermark image is shown along with the correlation value.

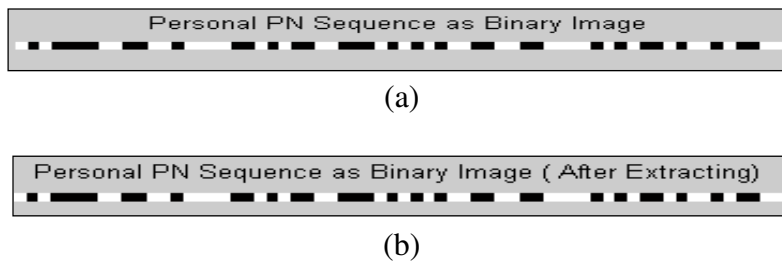


Figure 66. (a) Original fragile watermark, (b) extracted watermark, correlation = 1.0000

2) With attacks

We tested the effect of the attacks on the fragile watermark by assuming the Gaussian noise was added to the watermarked image in Figure 67 (a).

- **Effect of Gaussian noise:** when adding the Gaussian noise to the watermarked image, we fixed the value of the variance to zero and changed the value of mean to 0.8; the result the extracted watermark image is shown in Figure 67 (b).



(a)



(b)

Figure 67. Gaussian attack on the fragile watermark image

The correlation value between the original and the extracted watermark was 0.1849 confirming that an attack is applied on the watermarked image.

Chapter 6

Proposed Watermarking-Encryption based Secured Telemedicine

Algorithm

This chapter describes the proposed technique that is based on merging watermarking and encryption processes for a safe medical images transfer. Most of the existing medical image approaches related to this aspect uses a hash function to produce a digest of the image and embed it as watermark into the image. If the image is not tampered, the hash value at the receiver side must match the value embedded into the image. This algorithm is demonstrated to add a feature of tamper localization in addition to the tamper detection (hashing process). Briefly, in the proposed technique, the medical information is embedded and hidden in the cover image besides using some encryption processes to assure security and transferred over a public network. On the receiver side, the watermarked encrypted image is delivered and passed to the decryption and extraction processes respectively. Indeed, the proposed scheme is very sensitive. It can detect and localize even one bit of distortion in the image. The performance was evaluated by testing the imperceptibility by calculating the PSNR between the original image and the watermarked image. Also testing the robustness by applying different types of attacks and then calculated the correlation between the original and extracted watermarks.

6.1 Watermarks Generation Module

In the proposed algorithm, a combination of watermarking and encryption procedures is implemented where three watermarks are used so each one will be applied for a specific purpose.

6.1.1 Authentication Watermarks

The scheme embeds different purpose watermarks, starting with the patient information watermark for the purpose of achieving authentication requirement since the confidentiality is achieved by the embedding process itself. Also, as in the chapter 5, this watermark is generated from the DICOM header and shown as a gray-scale image which consists of the basic application level confidentiality profile attributes that defined in the image header. So the size of this watermark depends on the image size and related to the existing patient records that are defined, not a fixed one. In our case, the size of the watermark is (50×60) pixels which is equal to 3000 bits. Thus, this embedding is done in the DWT third layer of HL horizontal details decomposition of each block in the RONI. Figure 68 shows patient information watermark image related to one of the test medical image that we used in the algorithm.

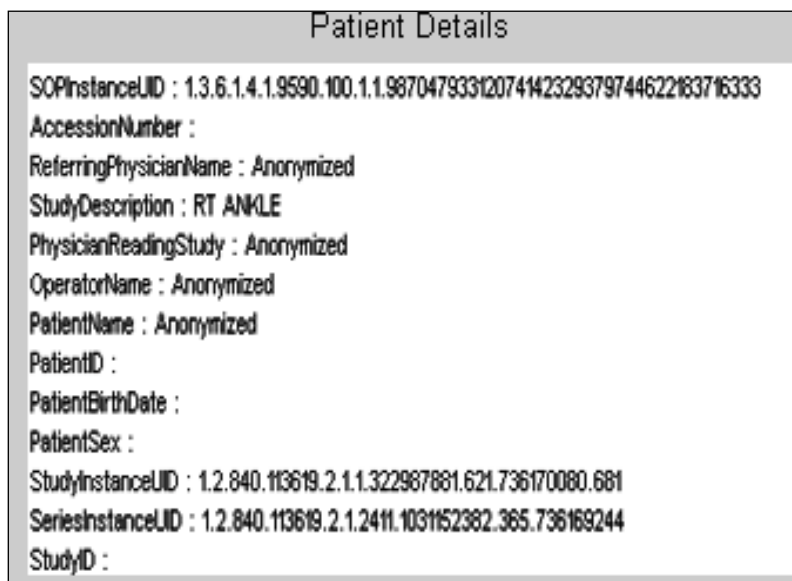


Figure 68. Image of the patient information watermark

6.1.2 Integrity Watermark

This type of watermark aims to check the integrity and determine whether and where the image has been modified. In the proposed hybrid technique two robust integrity watermarks are used:

- 1) Hash of ROI watermark: This watermark is generated from a hashing Whirlpool function that is applied to the ROI region for the purpose of tamper detection. The hash value of 512 bits output resulted as a PN sequence of 0's and 1's is embedded in the DWT second layer of HL sub-band horizontal decomposition of each block in the RONI region. The size of the watermark is fixed and is equal to 512 bits which returned by the Whirlpool hash output for ROI.
- 2) Cyclic redundancy check (CRC-16) watermark: an error detection code generated by a hash function that detects any change happened to the row of data and provides information where the image has been modified (tamper localization purpose). This watermark is generated by applying the CRC-16 function over the ROI area, where each ROI block has a computed CRC-16 output consisting of 16 bits, based on the remainder of a polynomial division of their pixels (Thaler and Pat, 2009). The result (CRC-16 output) from each block acted as a CRC-16 watermark consists of 0's and 1's is embedded in the DWT first layer of HL sub-band horizontal decomposition of each block in the RONI region, till all the bits are inserted. However, the size of the CRC-16 is always fixed and equal to 16 bits, but how many CRCs is computed depends on the size of the selected region of interest blocks.

To explain the CRC-16 procedure, take the generator polynomial $G(x)=x^{16}+x^{12}+x^5+1$. Such a message is [0100 0000 0000 0000 0101 0110]

(b0...b23). Firstly, remainder register 'r' is initialized to 0. Then the message is shifted into the divider (b0 first). Operations are done in the order: a) XORs, b) left shift of r register and c) r3 and r10 update. Finally, the r register is appended to the message.

6.2 Image Preprocessing

Before embedding process, the original image was pre-processed by some other operations. The following concepts in this subsection are applied.

The original image is divided into two regions: ROI that defined the important diagnosis region as a polygon shapes, and RONI that defined the rest of the image as shown in Figure 42 in chapter 5. The Figure illustrate that the selection of the ROI is done by a MATLAB roipoly tool to be formed with a small size. Then the ROI is separated from the RONI while dividing the plain image into blocks of equal size (16×16) and the blocks that enter the boarders of the ROI even with just one pixel, it will be considered as an ROI block. The remaining blocks will be considered as RONI blocks. Figure 43 in chapter 5 explains how the plain image is divided into blocks and determining ROI/RONI blocks.

6.3 Watermarks Embedding/Extraction in RONI

The watermarking algorithm consists of two procedures; watermark embedding and watermark extraction that applied to this algorithm in the RONI region only. The two procedures are described in the following subsections. It is noticed to mention that the encryption/decryption approach is applied into the two procedures.

6.3.1 The Embedding Procedure

In general, the embedding operation is just done in the RONI, so the ROI is separated from the embedding area, but at the end they will be combined together to perform the watermarked image. Figure 69 shows the embedding procedure for RONI region, before moving into details.

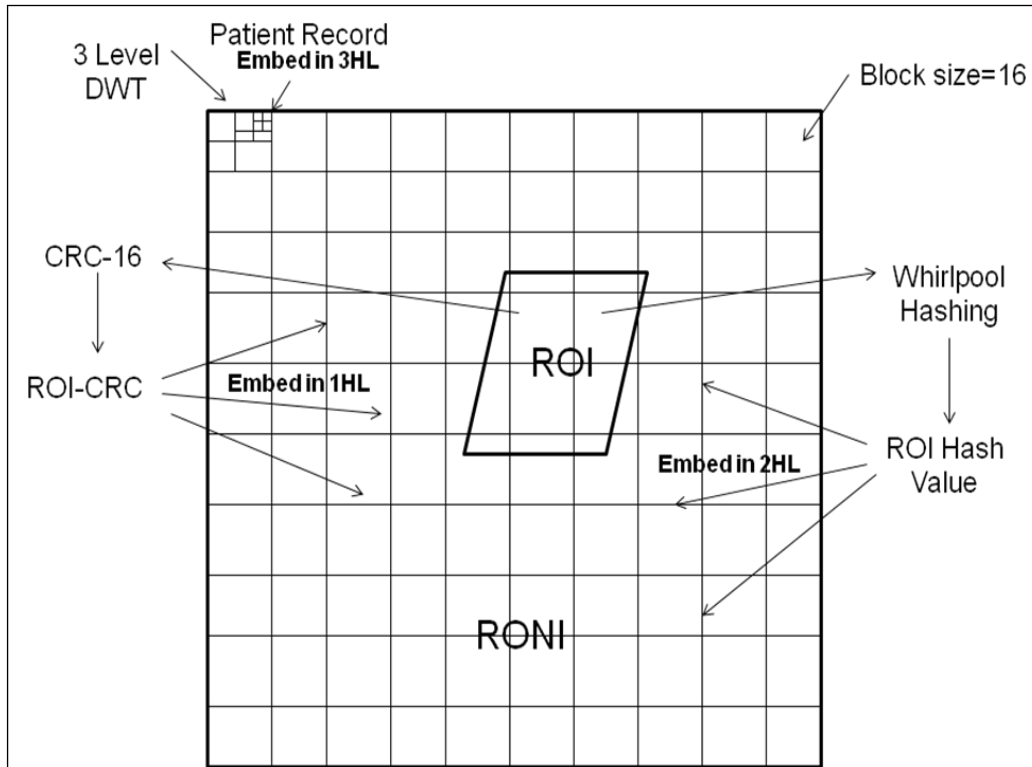


Figure 69. Embedding procedures for RONI

After segmented the image by ROI and RONI, and dividing it into blocks of size 16x16 pixels, we take the RONI region and the 3-levels DWT are applied to each block. So each block of size 16x16 has a corresponding block of size 8x8 in the first decomposition level, a block of 4x4 coefficients in the second level, and a block of 2x2 in the third level. The Haar wavelet is selected as the mother wavelet for the image blocks decomposition. A block diagram shows the steps of embedding the multiple watermarks in a cover medical image as seen in Figure 70.

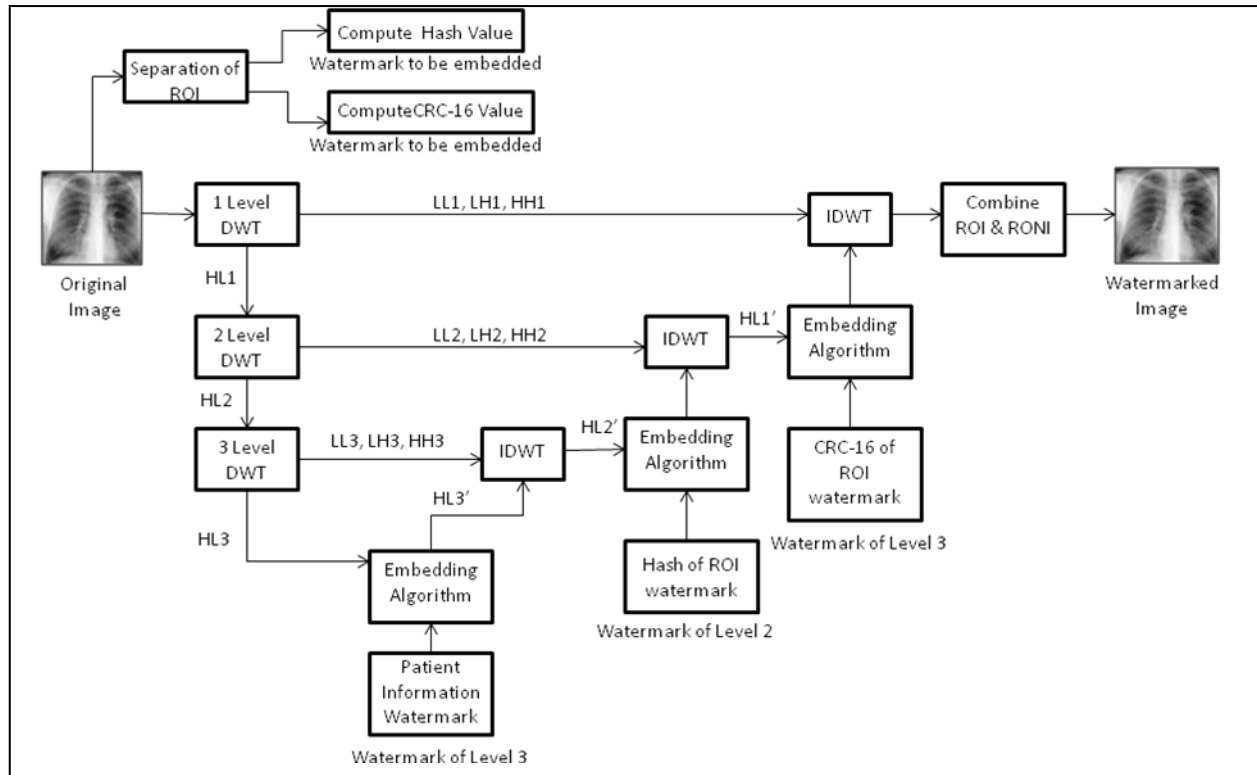


Figure 70. A block diagram of RONI embedding procedure

The RONI blocks are prepared for the following embedding steps after the previous image processing steps. Based on the block diagram above:

Step 1: for a 1-level DWT, decompose each RONI blocks into 4 sub-bands: LL_1 , HL_1 , LH_1 , and HH_1 .

Step 2: for a 2-level DWT, apply DWT to the HL_1 sub-band to get another 4 sub-bands (LL_2 , HL_2 , LH_2 , and HH_2) and choose the sub-band (HL_2).

Step 3: for 3-level DWT, we applied DWT to the HL_2 sub-band to get 4 sub-bands (LL_3 , HL_3 , LH_3 , and HH_3) and chose the sub-band (HL_3).

Step 4: the patient information watermark that will be embedded in HL_3 is reformulated into sequence of ones and zeros in order to make it a binary matrix,

Step 5: the embedding algorithm is applied by; generating PN sequences to designate “1” and “0”. Then finding two highly uncorrelated PN sequence: $pn_sequence_1$ and $pn_sequence_0$. The size of both sequences will be the same as the size of the embedding block (in our case in the third level, it is equal to 2×2) in order to apply the matrix addition property.

When the watermark bit = 0; then the addition is done between $pn_sequence_0$ matrix of size 2×2 and the block of HL3 of size 2×2 . The addition result will be a matrix of size 2×2 embedded in the block of HL3 with a gain factor K.

When the watermark bit = 1; then the addition is done between $pn_sequence_1$ matrix of size 2×2 and the block of HL3 of size 2×2 . The addition result will be matrix of size 2×2 embedded in the block of HL3 with a gain factor K.

This method will be applied until embedding all the patient information watermark bits.

Step 6: apply the IDWT using the 4 sets DWT coefficients. Apply IDWT to the modified coefficients of level 3 (LL_3 , HL_3 , LH_3 , and HH_3) to reconstruct the chosen sub-band of level 2 (HL_2).

Step 7: the hash of ROI watermark is embedded in the HL2 by applying the same method for the patient information watermark that mentioned in step 5. But the size of both sequences in this case to be embedded in the second level, will be equal to 4×4 , and so the result of matrix addition will be a matrix of size 4×4 too, embedded in the block of HL2 with a gain factor K. Repeat the embedding process with one bit each time of embedding, until the watermark bits are handled.

Step 8: apply IDWT to the modified coefficients of level 2 (LL_2 , HL_2 , LH_2 , and HH_2) to reconstruct the chosen sub-bands of level 1 (HL_1).

Step 9: the CRCs of ROI blocks watermark is embedded in the HL1 by applying the same method for the patient information watermark that mentioned in step 5. But the size of both sequences in this case to be embedded in the first level, will be equal to 8×8 , and so the result of matrix addition will be a matrix of size 8×8 too, embedded in the block of HL1 with a gain factor K. Repeat the embedding process with one bit each time of embedding, until the watermark bits are handled.

Step 10: apply IDWT to the modified coefficients of level 1 to reconstruct the watermarked medical image (cover object).

Step 11: combine the ROI and RONI regions, to reconstruct the watermarked medical image.

In this algorithm, the medical image was of size 512×512 . The size of each block is 16×16 , so the image has 1024 blocks. After applying 1-level DWT, the resulted four sub-bands were each of size 8×8 . When we applied DWT to one of these sub-bands; the resulted four sub-bands were each of size 4×4 . At last we applied DWT to level 3 to one of the sub-bands; and the resulted four sub-bands were each of size 2×2 . For 1 bit each time of embedding, the chosen sub-band of level 1, resulted in 256×256 maximum message size that can be embedded, and the chosen sub-band of level 2 resulted in 128×128 maximum message (ROI watermark) size that can be embedded to HL₂ and finally a 64×64 maximum message (patient information) size that can be embedded to HL₃.

According to the hash of ROI watermark where the size of hash output value is 512 bits, and by the embedding process which is done in HL₂, the maximum message size for this sub-band will be able to handle the watermark.

Related to the CRC watermark, the size of check value is 16 bits/ROI block, and by the embedding process which is done in the HL_1 , the maximum size for this sub-band will be able to handle the watermark with a condition of ROI selection region that must not exceeds the size of embedding in the first level.

6.3.2 The Extraction Procedure

In general, the extraction process is done for the RONI as shown in Figure 71.

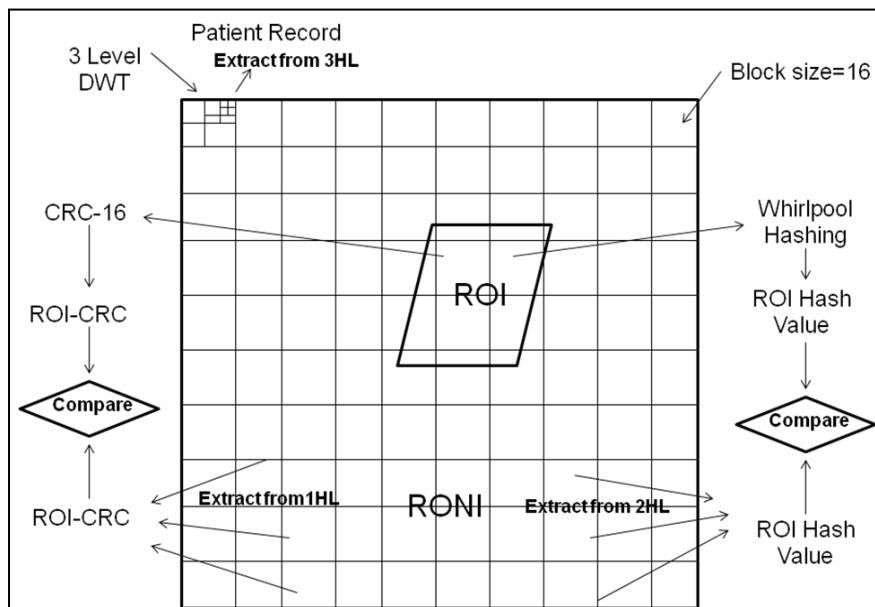


Figure 71. The extraction procedures for RONI

A block diagram below is shown the steps of extracting the watermarks from watermarked image in the RONI in Figure 72.

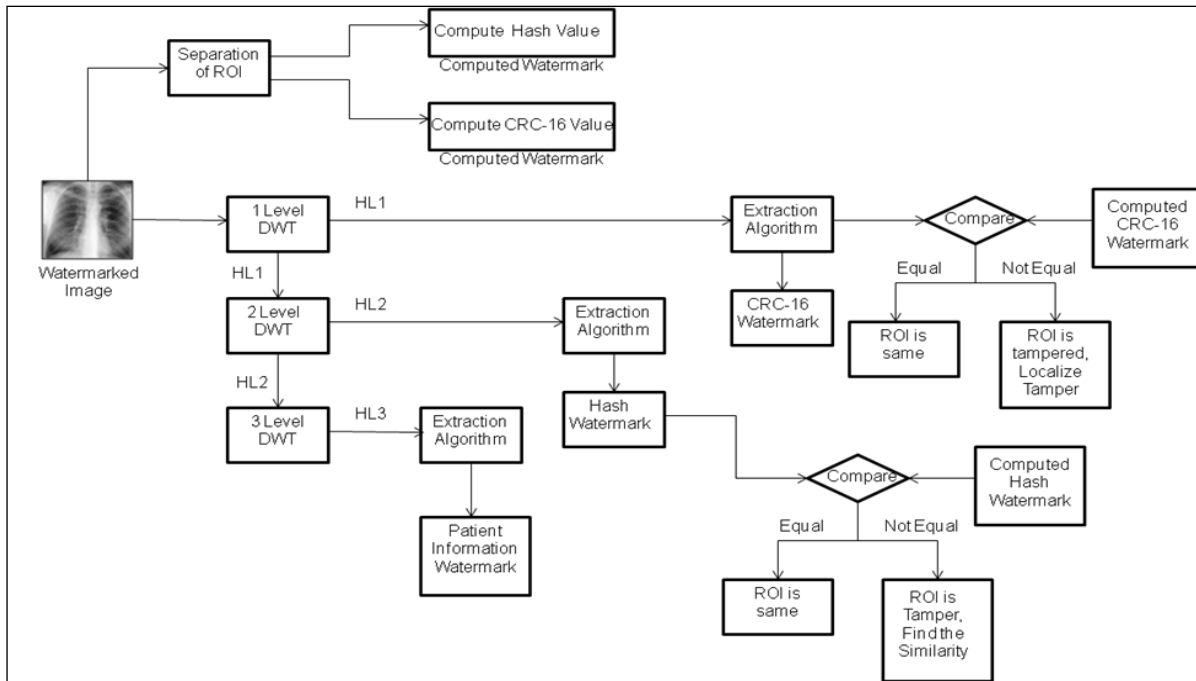


Figure 72. A block diagram of RONI extraction procedure

The extraction steps based on the block diagram above are:

Step 1: Separate ROI region from the watermarked image, in order to apply the procedure on the RONI only.

Step 2: divide the watermarked image into blocks of size 16×16.

Step 3: apply DWT to the watermarked image 3 times and determine the 4 sub-bands: LL, HL, LH, and HH for level 1, 2 and level 3 respectively, where HL₃ sub-band contains the patient information watermark that has to be extracted, HL₂ sub-band contains the hash of ROI watermark. And HL₁ sub-band contains the CRC-16 watermark.

Step 4: when recovering the watermarks, the same pseudo-random noise generator algorithm is defined its correlation with the noise pattern and seeded with the same key. Throughout detection, the pattern with the higher resulting correlation is used. The recovery procedure is repeated through the entire PN sequence till recovering all the bits of the watermark.

Step 5: An integrity check is done twice, as a last step to assure and detect if any tamper has been done on the ROI region. The first check is to compare between the extracted hash value and the hash value of the ROI in the extracted image. That is proved if the image is authentic or not.

Step 6: Another check in order to achieve the tamper localization purpose, is done by comparing every CRC-16 watermark extracted (which represents a CRC output for every block of ROI) with the CRC-16 output for the ROI blocks in the extracted image. The comparing is accomplished when it passed over each ROI blocks. So this check allowed the receiver to determine if there is a tamper happened on the ROI and localized exactly where the different bits are.

6.4 Performance Evaluation of the Algorithm

The algorithm was tested on different medical images (MRI and X-ray) of different sizes using MATLAB 7.6. The performance of this algorithm was evaluated by studying the visibility of the watermarked image and the robustness of this algorithm to different kinds of attacks. In this section we will deal with many types of attacks.

6.4.1 Setup of the MATLAB-based Simulation Experiments

Several simulation experiments are done in order to test and evaluate the effectiveness of the proposed hybrid algorithm. The main performance evaluation metrics are: imperceptibility, authentication, and integrity verification. Imperceptibility is measured by the PSNR between the original image and the watermarked image and it is observed later, that the high PSNR values obtained represent the better quality image of the proposed technique.

The performance in terms of robustness of the watermark without applying attacks was evaluated through measuring the correlation between the extracted watermark and the original to determine how closely the original resembles the extracted watermark. The patient information watermark were extracted from the RONI and subsequently compared with the originally embedded one; showing the percentage of similarity in the extracted watermark confirming on the authentication metric. Besides the integrity verification focused on two watermarks. For the hash watermark to find the similarity between the extracted watermark and the computed hash of ROI in the extracted image. In addition, the CRC watermark to find the similarity between the extracted watermark and the computed CRC for the ROI in the extracted image.

Furthermore, a test is done to show whether a watermark can survive against different modifications to the image it is embedded in, such as cropping, white Gaussian noise, JPEG compression, and dithering attacks of the watermarked images.

Also, the StirMark benchmark 4.0 is used for testing the proposed algorithm where StirMark system carries out a series of attacks on the watermarked image. Then it is tried to extract watermarks from the obtained attacked watermarked image.

6.4.2 Imperceptibility Results

The visibility of this algorithm was tested by calculating the PSNR between the original image and the watermarked image. By taking the same image applied in chapter 5 (RT ankle) medical image as an original image shown in Figure 73(a), and embedding all the watermarks to get the watermarked image as shown in Figure 73(b), the PSNR value was calculated as shown below. Note that in Figure 73(b) a series of images shown the ROI/RONI selection and separation before getting the final image: watermarked image.



(a)



(b)

Figure 73. (a) The original image, (b) the watermarked image, PSNR value = 98.1093 db

As shown from the experimental result that we did above, embedding the watermarks in HL sub-bands has shown high PSNR value and high imperceptibility as well. The sub-bands didn't affect the visibility of the image.

6.4.3 Authentication Results

1) Without applying attacks

We studied the robustness of the extracted patient information watermark from the sub-band HL3 in RONI. Then the similarity between the extracted watermark and the original watermark was computed using the correlation factor. In the following Figure 74(a) the original patient information watermark image is shown, and Figure 74(b) the extracted watermark image is shown along with the correlation value.

<p>SOPInstanceUID : 1.3.6.1.4.1.9590.100.1.1.98704793312074142329379744622183716333 AccessionNumber : ReferringPhysicianName : Anonymized StudyDescription : RT ANKLE PhysicianReadingStudy : Anonymized OperatorName : Anonymized PatientName : Anonymized PatientID : PatientBirthDate : PatientSex : StudyInstanceUID : 1.2.840.113619.2.1.1.322987881.621.736170080.681 SeriesInstanceUID : 1.2.840.113619.2.1.2411.1031152382.365.736169244 StudyID :</p>	<p>SOPInstanceUID : 1.3.6.1.4.1.9590.100.1.1.98704793312074142329379744622183716333 AccessionNumber : ReferringPhysicianName : Anonymized StudyDescription : RT ANKLE PhysicianReadingStudy : Anonymized OperatorName : Anonymized PatientName : Anonymized PatientID : PatientBirthDate : PatientSex : StudyInstanceUID : 1.2.840.113619.2.1.1.322987881.621.736170080.681 SeriesInstanceUID : 1.2.840.113619.2.1.2411.1031152382.365.736169244 StudyID :</p>
--	--

(a)

(b)

Figure 74. (a) Original watermark, (b) extracted watermark, correlation = 0.9784

2) With attacks

- Effect of cropping attack:** we cropped the watermarked image by different block sizes. The cropped block is done on the four corners: up left, up right, down left, and down right. The attacked watermarked image at different values of block size is shown in Figure 75.

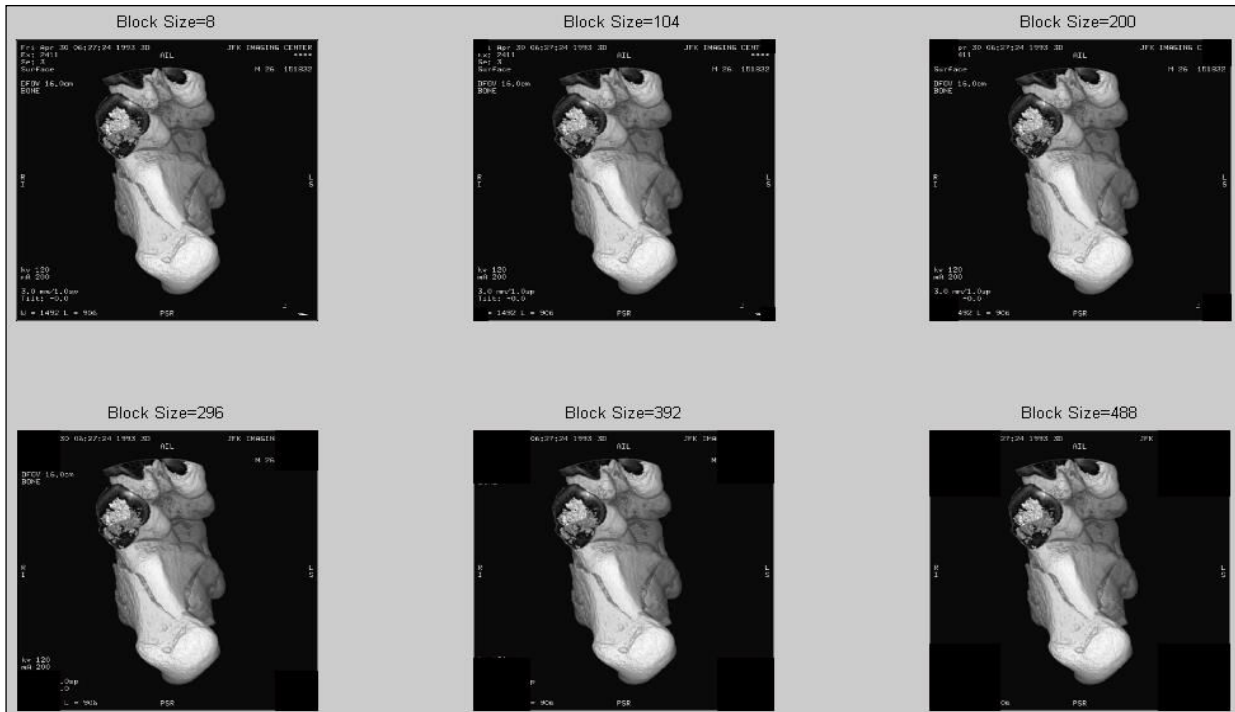


Figure 75. Watermarked image after cropping attack

The extracted watermarks (Patient information) for HL3, the correlation, and PSNR at different values of block size are shown in Figure 76, Figure 77 respectively.

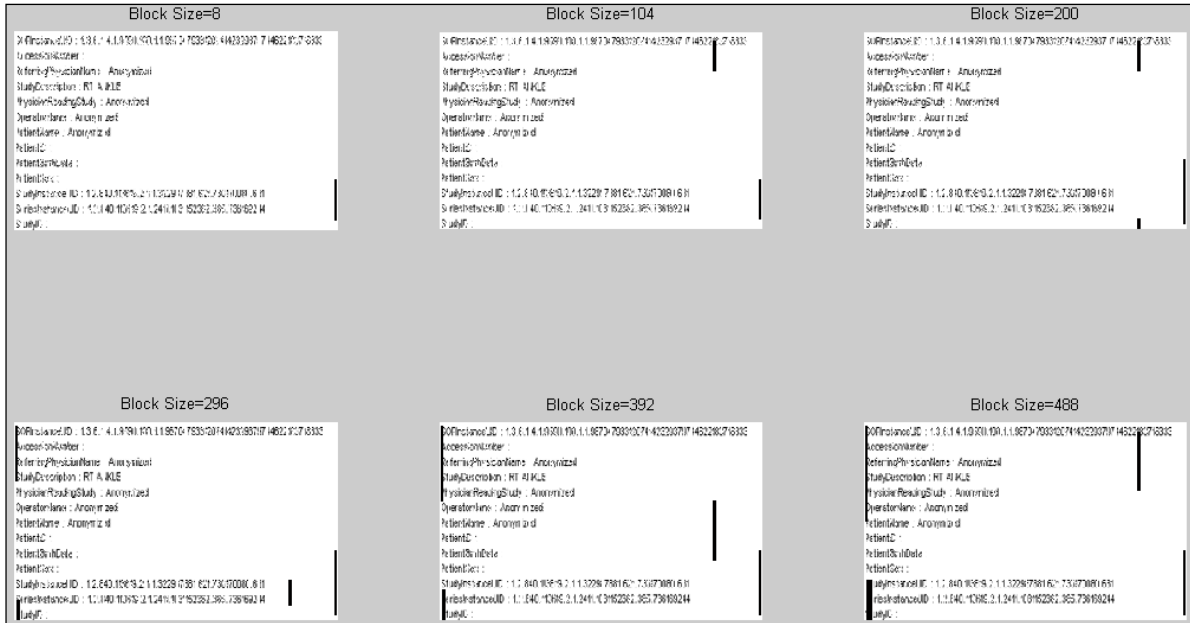
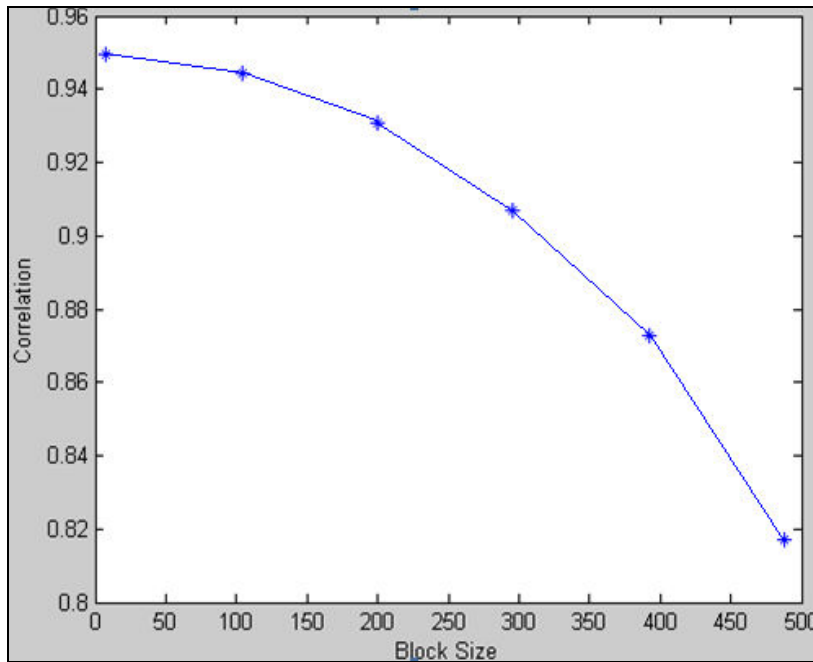
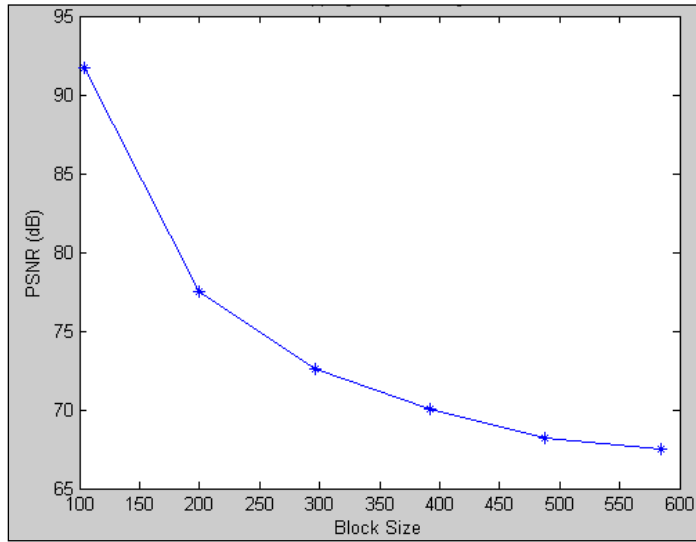


Figure 76. Extracted watermark (patient information) after cropping attack



(a)



(b)

Figure 77. (a) Correlation vs. block size and (b) PSNR vs. block size after cropping attack

- Effect of Gaussian noise:** when adding the Gaussian Noise to the watermarked image, we fixed the value of the variance to zero (as default) and changed the value of mean from 0 to 1 of a 0.2 scale; the results the attacked watermarked images are shown in Figure 78.

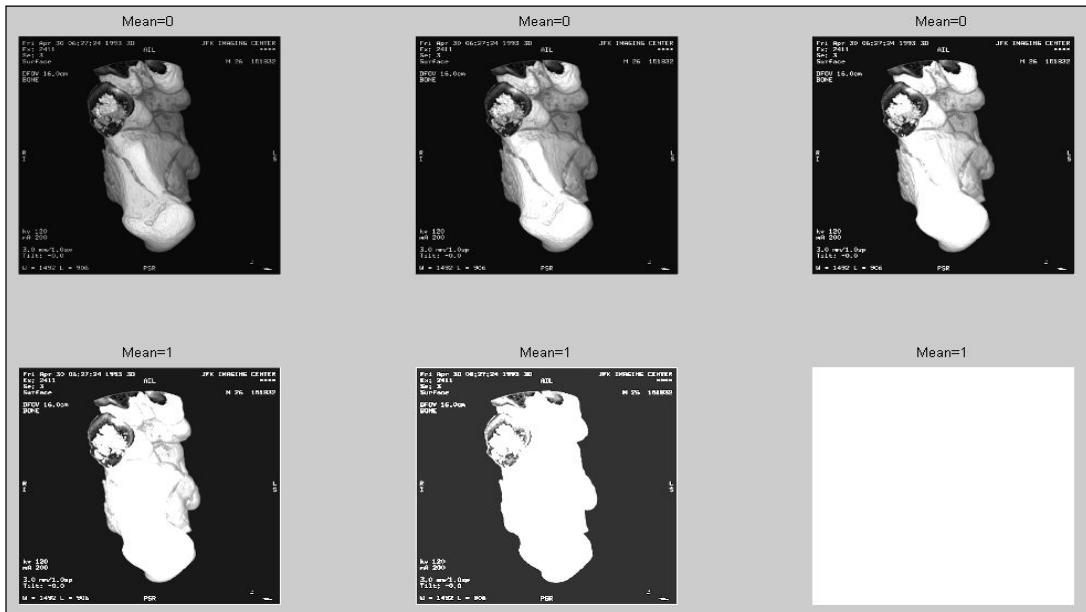


Figure 78. Gaussian attack of different mean values on the watermarked image

The extracted watermark (Patient information) for HL3, correlation, and the PSNR at different values of the mean are shown in Figure 79, Figure 80 respectively.

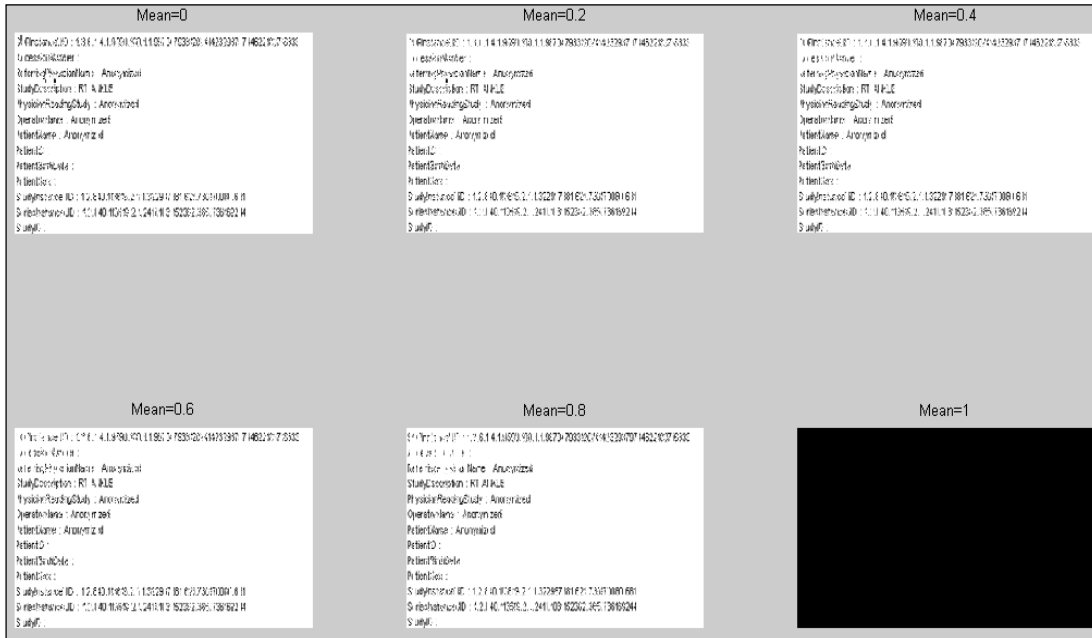
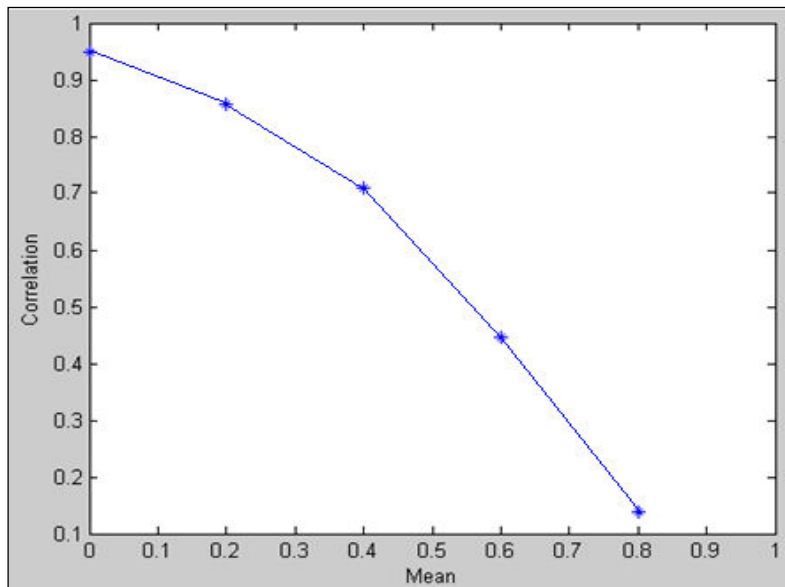
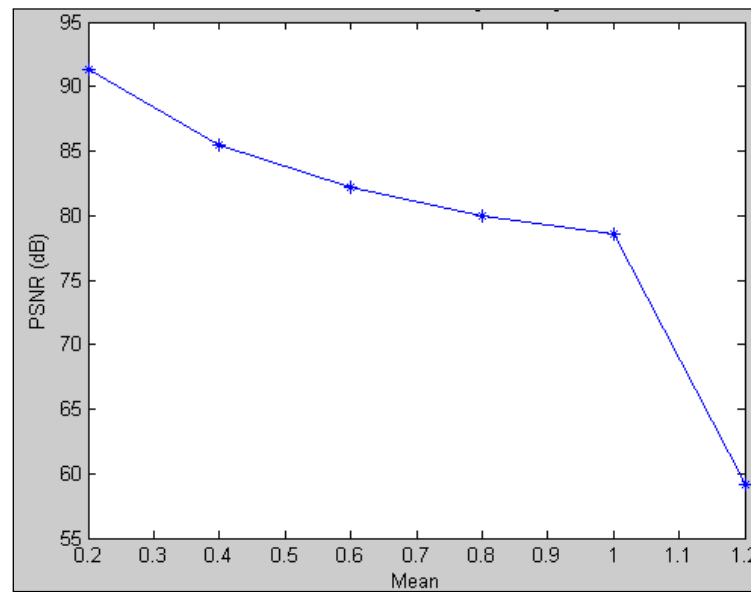


Figure 79. Extracted watermark (patient information) from HL3 after Gaussian attack



(a)



(b)

Figure 80. (a) Correlation vs. mean and (b) PSNR vs. mean after Gaussian attack

- **Effect of JPEG compression:** when applying the JPEG compression to the watermarked image as shown in Figure 81.

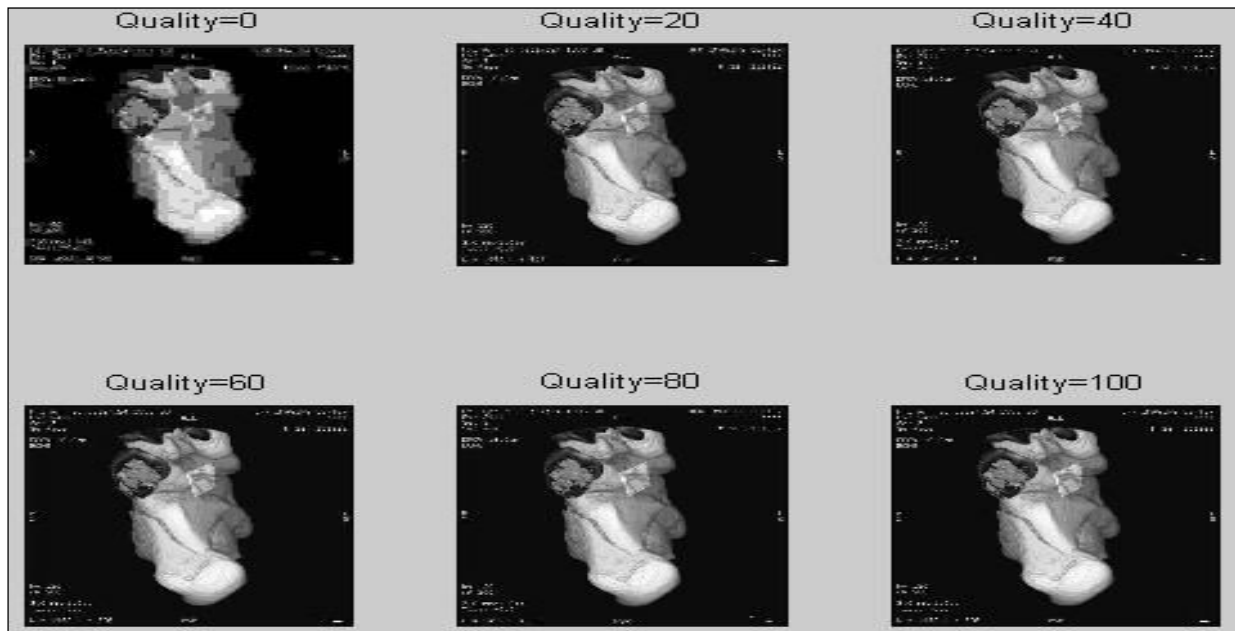


Figure 81. Compression attack of different quality values on the watermarked image

The extracted watermark (Patient information) for HL3 in addition to the correlation and PSNR results at different values quality are shown in Figure 82, Figure 83 respectively.

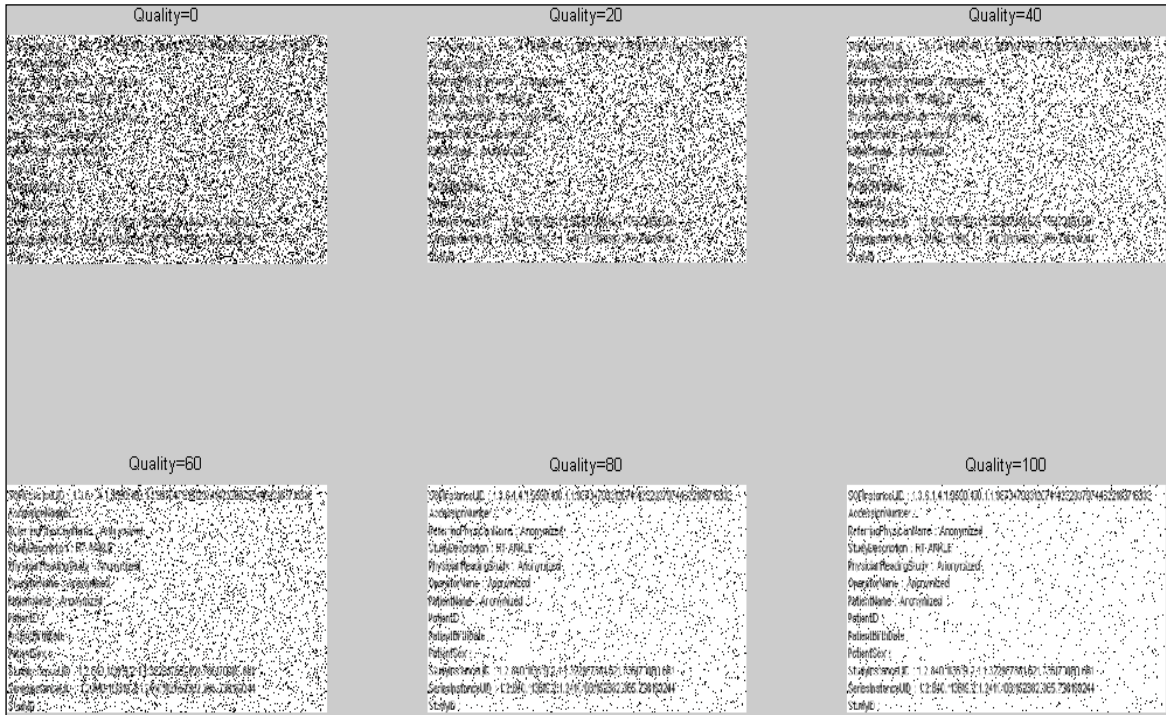
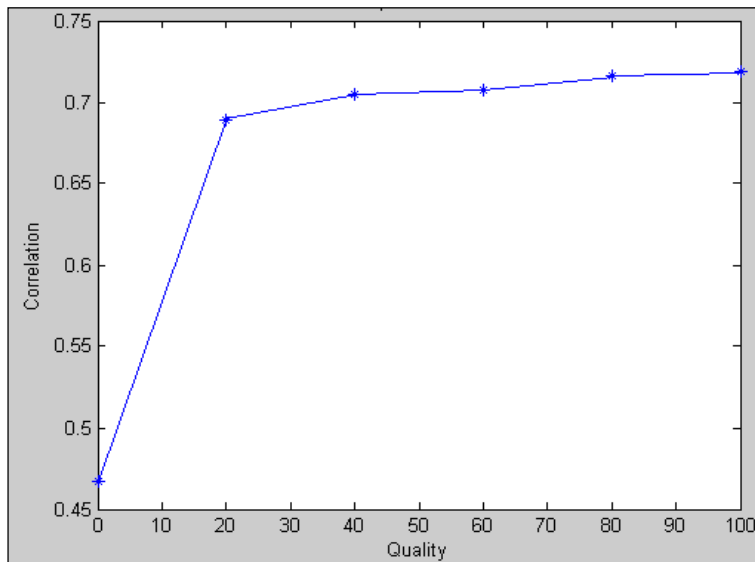
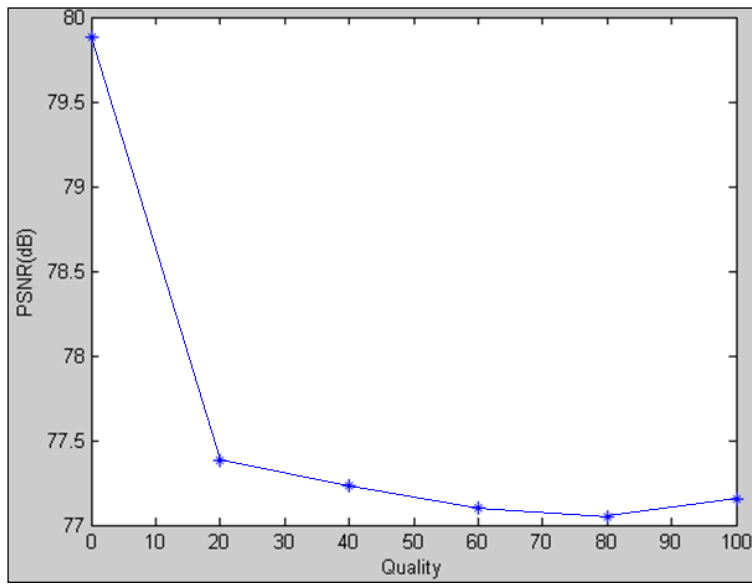


Figure 82. Extracted watermark (patient information) from HL3 after compression attack



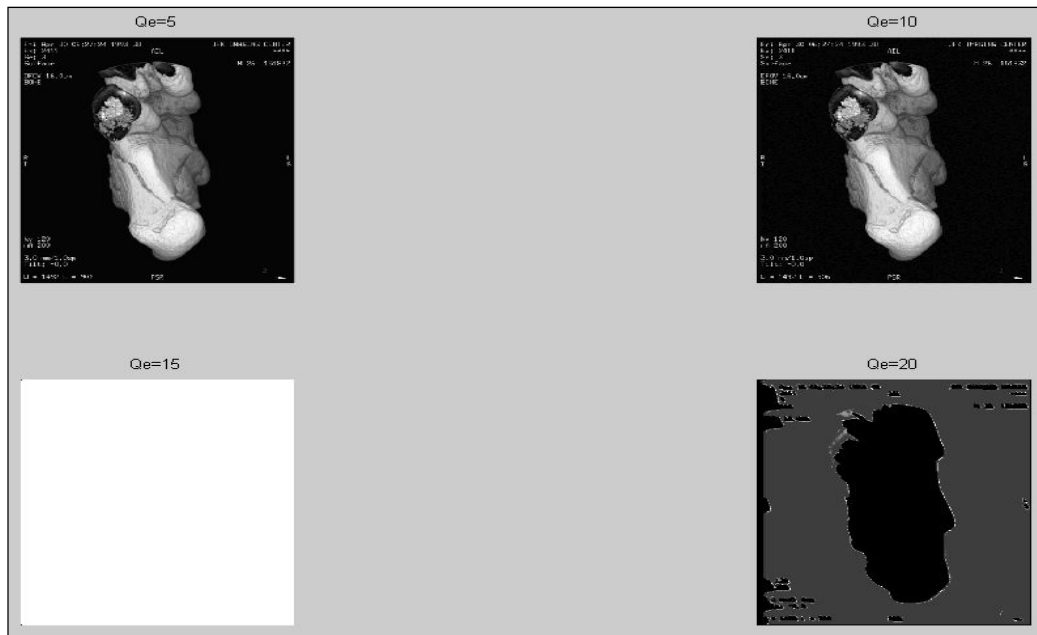
(a)



(b)

Figure 83. (a) Correlation vs. quality (b) PSNR vs. quality after compression attack

- **Effect of dithering:** when applying the dithering attack to the watermarked image as shown in Figure 84.

Figure 84. Dithering attack of different Q_e values on the watermarked image

The extracted watermark (Patient information) for HL3 in addition to the correlation and PSNR values at different Q_e values are shown in Figure 85, Figure 86 respectively

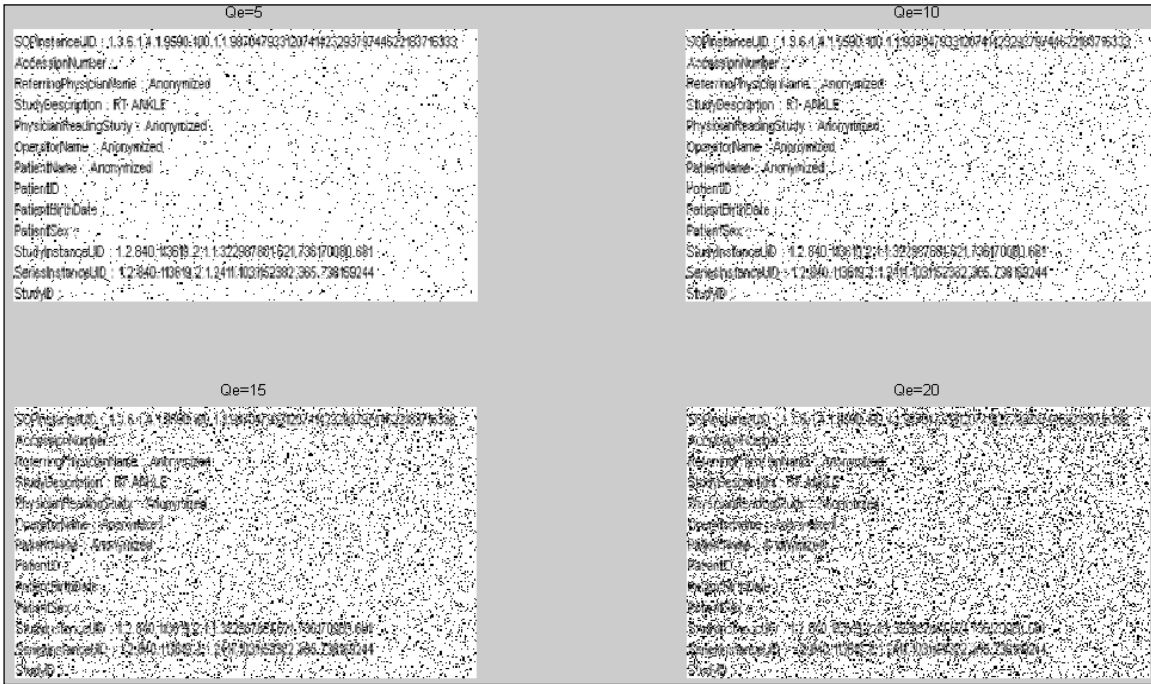
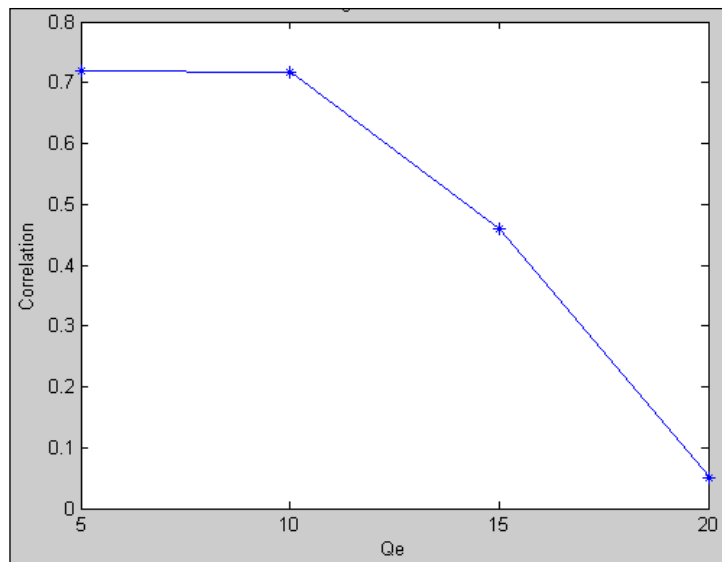
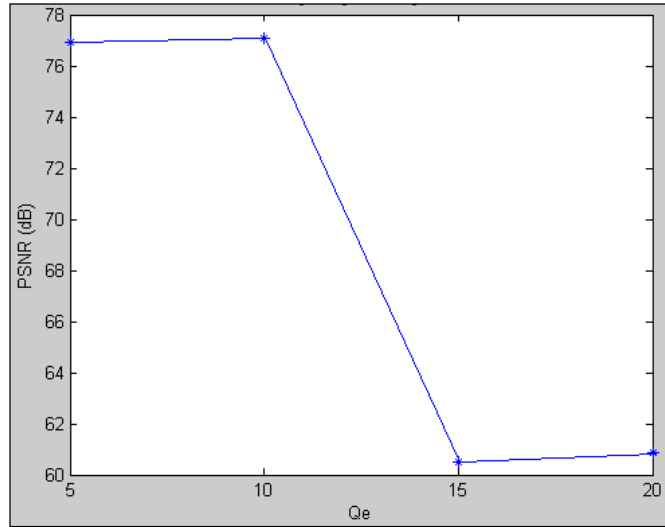


Figure 85. Extracted watermark (patient information) from HL3 after dithering attack



(a)



(b)

Figure 86. (a) Correlation vs. Qe (b) PSNR vs. Qe after dithering attack

6.4.4 Integrity Verification

1) Without applying attacks

For the hash watermark: we extracted the hash watermark from the RONI region. Then compute the hash of the received ROI in order to make an integrity verification check; if they were equal. Otherwise, the similarity percentage between the extracted and computed hash values will be calculated. About our result, as shown in Figure 87, a portion of the computed hash and the extracted hash values are presented. Thus, they are not similar, the percentage was 55.5625%.

```

Computed_Hash_Code =
01110111001000110111001011010111100101100100101110000001101100010101010111100011000110110000

Extracted_Hash_Code =
11010101001110010110101001100010111001100011001111101001110110001011110101001101100001100001

```

Figure 87. Computed and extracted hash comparison

For CRC watermark: after the unsimilarity percentage that is resulted between the hash values, we extracted the CRC watermark from the RONI. Then computed the CRC for each block of the received ROI in order to make an integrity verification check. This checking determines where the tamper localizes exactly at the bit location. About our result, in Figure 88 a portion of corresponding locations of our CRC values is compared with each other to clarify where the exact tamper happened.

Extracted_image_CRC =														
0	1	0	0	0	1	0	0	1	1	0	1	0	0	0
0	0	0	0	0	0	0	1	0	0	1	0	1	0	0
0	1	1	1	0	1	0	0	1	0	0	0	0	0	1
0	1	0	0	0	1	1	0	0	1	0	0	0	0	1
0	1	1	1	0	1	1	0	0	1	0	1	0	0	0
0	0	0	1	0	0	0	0	1	1	0	1	0	0	0
0	1	1	1	0	1	0	0	0	1	0	1	0	0	0
0	1	0	1	0	0	1	0	1	0	0	1	0	0	1
0	1	0	0	0	1	1	0	0	0	0	1	0	0	0
0	1	0	1	0	0	0	0	1	0	0	1	0	0	0
0	0	1	0	0	1	1	0	0	1	0	0	1	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	1	0	0	1	0	0	0
0	0	0	1	0	0	1	0	1	1	0	1	0	0	0
0	1	1	1	0	0	0	0	1	0	0	0	0	0	0
0	0	0	1	0	1	0	0	0	0	0	0	0	0	1
0	1	1	0	0	0	1	0	1	1	0	0	0	0	0
0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
0	1	1	1	0	1	0	0	1	1	0	0	0	0	1
0	0	0	0	0	1	1	0	1	1	0	1	0	0	0

(a)

CRC_out =														
0	0	0	1	1	0	1	0	0	0	0	0	0	0	1
0	0	0	0	1	0	0	0	0	1	0	0	0	1	0
0	0	0	0	1	0	1	0	0	0	0	0	0	1	1
0	0	0	1	1	0	0	0	1	1	0	0	0	1	1
0	0	0	0	1	0	1	0	1	1	0	0	0	0	1
0	0	0	1	0	0	1	0	0	1	0	0	0	0	1
0	0	0	0	1	0	0	0	1	1	0	0	0	0	1
0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
0	0	0	1	1	0	1	0	1	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	1	0	0	0	1	1
0	0	0	1	1	0	0	0	1	0	0	0	0	0	1
0	0	0	0	0	0	1	0	1	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	1	0	1	1	0	0	0	1	0
0	0	0	1	1	0	0	0	1	0	0	0	0	0	1
0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	1	0	0	0	0	1

(b)

Figure 88. Comparison of CRC values; (a) extracted one, (b) computed one

2) With attacks

- **Effect of cropping noise:** we tested the effect of applying a cropping noise attack on the watermarked image with cropped block of size 8, and notice the extracted hash watermark from RONI and the computed hash watermark of received ROI, the similarity percentage was 49.6500%.
- **Effect of Gaussian noise:** we tested the effect of applying a Gaussian noise attack on the watermarked image, and notice the extracted hash watermark from RONI and the computed hash watermark of received ROI, the similarity percentage was 20.1890%.

Chapter 7

Discussion and Conclusions

This thesis has demonstrated that applying encryption and/or watermarking can provide a secure telemedicine application for medical images. Three schemes have been investigated on DICOM standard images that extended the current technologies and developed them in such a way to achieve the three secure transfer requirements. They overcome the security problems associated with the previous algorithms in the literature review. The contributions of this thesis are highlighted for each proposed scheme. The results have shown successful confidentiality, integrity, and authentication of medical images with respect to the three proposed techniques. From the results and evaluation, it can be concluded that this research has met the objectives outlined in chapter 1.

7.1 Attributes of the Proposed Algorithms

The main conclusions derived from the work implemented in this thesis can be summarized as follow:

- The encryption-based algorithms achieved the secured telemedicine requirements for the header level and the image level.
- The watermarking-based algorithm provided the security requirements, and robustness against counterfeiting attacks.
- The hybrid algorithm has met the three requirements too, and a feature of accurate tamper localization.

7.2 Limitations of the Proposed Algorithms

It is worthwhile to mention limitations of the proposed schemes that must be taken into considerations.

- For the watermarking scheme and the hybrid scheme, both algorithms are only applicable to images with ROI/RONI separation. Besides that, they are not allowable to change any bits in the ROI and this implies that any legitimate image processing changes the spatial value of the image will result in the image being considered as tampered.
- About the encryption schemes, they have a limitation because of their long execution time they needed for the encryption and decryption operations compared to the watermarking or the hybrid schemes that not exceed 1 minute for each of them.

7.3 Future Research

Based on the findings of this work, the schemes could open up a number of possibilities for the future work and expanded by:

- Improvement on security and the quality of recovery bits by applying different error correction (such as: Hamming codes, turbo codes, Reed Solomon ECC code, and trellis codes). This can be represented as a watermark.
- To apply reversible watermarking techniques.
- A lossless compression technique could be used to compressed the image and implement as a watermark that can be restored if the image was detected as tampered.
- Apply the schemes on other image modalities such as computed tomography (CT), positron emission tomography (PET), nuclear medicine (NM).
- New encryption-based algorithm with reduced run time.

REFERENCES

- Acharva U. R., Bhat P. S., Kumar S., and Min L. C., (2003), Transmission and Storage of Medical Images with Patient Information. **Comput. Biol. Med.**, Vol. 33, Pages: 303–210.
- Ahmet M. Skicioglu, (2003), Protecting Intellectual Property in Digital Multimedia. **IEEE Computer**.
- Alvarez G., Li. S., and Hernandez L., (2007), Analysis of Security Problems in a Medical Image Encryption System. **Computers in Biology and Medicine**, Vol. 37, No. 3, Pages: 424–427.
- Andrew H., (2007), Article: What is the strongest hash algorithm?. Kellerman Software. <http://www.KellermanSoftware.com>.
- Ashley. R.C., (2002), Telemedicine: Legal, Ethical and Liability considerations. **Journal of the American Dietetic Association**. Vol 102, No.2.
- Bousslimi D., and Coatrieux G., (2011), A joint Watermarking/Encryption Algorithm for Verifying Medical Image Integrity and Authenticity in Both Encrypted and Spatial Domains. **33rd Annual International Conference of the IEEE EMBS Boston**, Massachusetts USA.
- Brahimi Z., Bessalah H., Tarabet A., and Kholadi M. K., (2008), Selective Encryption Techniques of JPEG2000 Codestream for Medical Images Transmission. (**WSEAS Transactions on Circuits and Systems**, Vol. 7, No. 7, Pages: 718-728.
- Barreto P. S. L. M. and Rijmen V., (2000), The Whirlpool Hashing Function. **First Open NESSIE Workshop**, Leuven, Belgium, Pages: 13-14.
- Barreto P. S. L. M., and Rijmen V., (2003), The WHIRLPOOL Hashing Function [Online]. Available: <http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip>.
- Bendel, and Mike, (2010), **Hackers Describe PS3 Security as Epic Fail, Gain Unrestricted Access**. Exophase.com. Retrieved 5 Jan. 2012.
- Bidgood WD, Horil SC, Prior FW, and Van Syckle DE., (1997), Understanding and Using DICOM. **The Data Interchange Standard for Biomedical Imaging. J. Am. Med. Inform. Assoc.** No. 4, Pages: 199-212.
- Buchmann J A., (2001), **Introduction to Cryptography**. New York: Springer-Verlag.
- Cao F., Huang H.K., and Zhou X.Q., (2003), Medical Image Security in A HIPAA Mandated PACS Environment. **Computerized Medical Imaging and Graphics**, Vol. 27, No.2-3, Pages: 185-196.

Chakraborty D., and Rodriguez-Henriquez F., (2008), Block Cipher Modes of Operation from a Hardware Implementation Perspective. In **Koç, Çetin K. Cryptographic Engineering, Springer**. ISBN 9780387718163, Page: 321.

Chao HM, Hsu CM, Miaou SG, (2002), A Data-Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records. **IEEE Trans Inf Technol Biomed**. Vol. 6, Pages: 46–53.

Chen-RiPiao, Dond-Min, and al., (2008), Medical Image Authentication Using Hash Function and Integer Wavelet Transform. **Image and Signal processing, Congress**. Vol. 1, Pages: 7-10.

Choudhury A.K., Maxemchuk N.F., Paul S., and Schulzrinne H.G., (1994), **Copyright Protection for Electronic Publishing over Computer Networks**. AT&T Bell Laboratories.

Christof Paar, Jan Pelzl,, (2009), **Introduction to Public-Key Cryptography**. Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". Companion web site contains online cryptography course that covers public-key cryptography, Springer.

Christof Paar, Jan Pelzl, (2009), **Stream Ciphers**. Chapter 2 of "Understanding Cryptography, a Textbook for Students and Practitioners". Companion web site contains online cryptography course that covers stream ciphers and LFSR, Springer.

Coatrieux G., Maitre H., Sankur B., Rolland Y., and Collorec R., (2000), Relevance of Watermarking in Medical Imaging. **IEEE EMBS Conf on Inform Tech Appl in Biomedicine**, Arlington.

Coatrieux G., Sankur B., and MaËrtre H., (2001), Strict Integrity Control of Biomedical Images. **Electronic Imaging, Security and Watermarking of Multimedia Contents III**.

Cox I. J, Miller M. L., and Bloom J. A., (2001), **Digital Watermarking**. Morgan Kaufmann, San Francisco, Calif, USA.

Craig J, Patterson V., (2005), Introduction to the Practice of Telemedicine. **J Telemed Telecare**. Vol. 11, Pages: 3–9.

Cruz C., Reyes R., Mendoza J., Nakano M., and Pérez, H., (2008), A Novel Verification Scheme for Watermarking Based Image Content Authentication Systems. **Telecommunications and Radio Engineering**. Vol. 67, No. 19, ISSN: 0040-2508, Pages: 1777-1790.

Darshana Mistry, (2010), Comparison of Digital Watermarking Methods. **International Journal on Computer Science and Engineering**. Vol. 02, No. 09, Pages: 2905-2909.

Denning D., (1982), Cryptography and Data Security. **Addison-Wesley, Reading, MA**.

Diffen, (2012), **CT Scan vs. MRI: Comparison Chart**. Retrieved 27 April 2012.

Digital Imaging and Communications in Medicine (DICOM) (2001). **National Electrical Manufacturers Association (NEMA)**. Rosslyn, VA, <http://medical.nema.org/dicom/2001.html>, Part 15: Security Profiles, PS 3.15-2001.

Digital Imaging and Communications in Medicine (DICOM) Supplement 55: Attribute Level Confidentiality DICOM Standards Committee, Working Group 14 Security 1300 N. 17th Street, Suite 1847 Rosslyn, Virginia 22209 USA VERSION: Final Text (Draft), 5 Sept. 2002 Security Supplement. Available at <http://medical.nema.org/>. Accessed June 2013.

Dolley Shukla and Manisha Sharma, (2012), Watermarking Schemes for Copy Protection: A Survey. **International Journal of Computer Science & Engineering Survey (IJCSSES)**. Vol. 3, No.1.

Dworkin M., (2007), Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. **NIST Special Publication 800-38D**.

Elbirt J., (2009), **Understanding and Applying Cryptography and Data Security**. Book ISBN 978-1-4200-6160-4.

Emergency Medicine Education Website, <http://www.emedu.org> / Accessed on 21 July 2012.

Flor, Alexander, (2012), **ICT4D: Information and Communication Technology for Development (PDF) 1 (1)**.

Frerking M. E., (1994), **Digital Signal Processing in Communication Systems**. New York: Chapman & Hall.

Fridrich J., (1999), Methods for Tamper Detection in Digital Images. **Proceedings of the Multimedia and Security Workshop at ACM Multimedia'99**. Pages: 29 -33.

Giakoumaki A., Pavlopoulos S., and Koutsouris D., (2006), Multiple Image Watermarking Applied to Health Information Managemen. **IEEE Trans. Inf. Technol. Biomed.**, Vol. 10, No. 4, Pages: 722–732.

Gueron, Shay., (2013), **AES-GCM for Efficient Authenticated Encryption – Ending the Reign of HMAC-SHA-1?**. Workshop on Real-World Cryptography. Retrieved 8 Feb. 2013.

Gueron S., Michael E. Kounavis., (2012), **Intel® Carry-Less Multiplication Instruction and its Usage for Computing the GCM Mode**.

Hamilton D. L., (1992), Identification and Evaluation of the Security Requirements in Medical Applications. **In Proc. 5th Annu. IEEE Symp. Computer Based Med. Syst., Session 2B: Pictural Archival Commun. Syst.**, Pages: 129-137.

Hammond W. E. and Cimino J. J., (2001), Standards in Medical Informatics. In E. H. Shortliffe, L. E. Perreault, G. Wiederhold, and L. M. Fagan: **Medical informatics – Computer applications in health care and biomedicine**. Springer, New York.

Hartung F. and Kutter M., (1999), Multimedia Watermarking Techniques. **Proc. IEEE**, Vol. 87, No. 7, Pages: 1079-1107.

Hellman Martin E., (2002), An Overview of Public Key Cryptography. **IEEE Communications Magazine**, Pages: 42-49.

Huang HK., (2002), **Development of A Digital Medical Imaging Archiving and Communication System (MIACS) for Services of Department of Health**. HKSAR Government—Final Report.

Image Processing Place Website, http://www.imageprocessingplace.com/root_files_V3/image_databases.htm/ Accessed on 21 July 2012

Jerrold T. Bushberg, J. Anthony Seibert, Edwin M. Leidholdt, and John M. Boone, (2002), **The Essential Physics of Medical Imaging**. Lippincott Williams & Wilkins, ISBN 978-0-683-30118-2, Page: 42.

Jones P., (2001), **RFC3174: US Secure Hash Algorithm 1 (SHA-1)**. <http://www.faqs.org/rfcs/rfc3174.html>.

Kahn David, (1972), **The Codebreakers**. Macmillan Company, New York.

Katz J. and Lindell Y., (2007), **Introduction to Modern Cryptography**. CRC Press. ISBN 1-58488-551-3.

Kobayashi, L.O.M.; Furuie, S.S.; Barreto, P.S.L.M., (2009), Providing Integrity and Authenticity in DICOM Images: A Novel Approach. **IEEE Transactions on Information Technology in Biomedicine**. Vol. 13, Issue: 4, Pages: 582- 589.

Kumar. Neeraj, Veenita Gupta, and Praveen Kumar., (2013), Analysis and Implementation of Different Digital Image Watermarking Techniques for Secure Data Transmission. **International Journal of Computer Trends and Technology (IJCTT)**. Vol. 4, Issue 5.

Laskar, Tahera Akhtar, and K. Hemachandran., (2013), Digital Image Watermarking Techniques and its Application. **International Journal of Engineering 2**, No. 3.

Lin C., and Chang S., (2001), A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation. **IEEE Transactions on Circuits and Systems of Video Technology**, Vol. 11, No. 2, Pages: 153-168.

Lin E.T., and Delp E.J., (1999), A Review of Data Hiding in Digital Images. **Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS '99**. Pages: 274-278.

López, J. and Dahab, R., (2000), **An Overview of Elliptic Curve Cryptography, Technical Report**. IC-00-10, State University of Campinas.

McGrew D. A., and Viega J., (2005), The Galois/counter mode of operation (GCM). **NIST Comput. Security Div. Comput. Security Resour. Center**, Gaithersburg, MD, Tech. Rep.

McGrew David A., and Viega John., (2004), The Security and Performance of the Galois/Counter Mode (GCM) of Operation. **Proceedings of INDOCRYPT 2004**, LNCS 3348.

Miaou S.G., Hsu C.H., Tsai Y.S., and Chao H.M., (2000), A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability for Electronic Patient Records. **Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Healthcare Records**.

Mildenberger P., Eichelberg M., and Martin E., (2002), **Introduction to the DICOM Standard**. Eur. Radiol. Vol. 12, No. 4, Pages: 920-927.

Misiti M., Misiti Y., Oppenheim G., and Poggi J., (2006), **Wavelet Toolbox User's Guide**, the Math Works, Inc.

Mitreă M., Prêteux F., Petrescu M., and Vlad A., (2005), The StirMark Watermarking Attack in the DWT Domain. **Proc. of the 12th International Workshop on Systems, Signals and Image Processing**, Chalkida, Greece, Vol. 2, Pages: 2-5.

Mustra Mario, Delac Kresimir, Grgic, and Mislav, (2008), Overview of the DICOM Standard. **ELMAR, 50th International Symposium**. Zadar, Croatia. ISBN 978-1-4244-3364-3, Pages: 39-44.

Nambakhsh M.S., Ahmadian A., Ghavami M., and Dilmaghani R., (2006), A Novel Blind Watermarking of ECG Signals on Medical Images Using EZW Algorithm. **Proceeding of IEEE International Conference on Engineering in medicine and Biology Society**, New York, Pages: 3274–3277.

Neis U., Nickel K., and Tiehm A., (2000), Enhancement of Anaerobic Sludge Digestion by Ultrasonic Disintegration. **Water Science & Technology**. Pages: 42-73.

NEMA Standards Publication, (2008), Digital Imaging and Communications in Medicine (DICOM) Supplement 142: Clinical Trial De-Identification Profiles, Version 3, **National Electrical Manufacturers Association**, Washington.

Nilanjan Dey, Moumita Pal, Achintya Das, (2010), A Session Based Blind Watermarking Technique Within the NROI of Retinal Fundus Images for Authentication Using DWT, Spread

Spectrum and Harris Corner Detection. **International Journal of Modern Engineering Research**, Vol.2, Issue.3, Pages: 749-757.

NIST SP 800-38A, (2007), Recommendation for Block Cipher Modes of Operation: Methods and Technics. **NIST Special Publication 800-38A**.<http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C>. Updated-July20_2007.pdf.

Norcen R., Podesser M., Pommer A., Schmidt H.P., and Uhl. A., (2003), Confidential Storage and Transmission of Medical Image Data. **Computers in Biology and Medicine**, Vol. 33, Pages: 277–292.

Perera, Tom., (2004), **The Story of the ENIGMA: History, Technology and Deciphering**. 2nd Edition, CD-ROM, Artifax Books, ISBN 1-890024-06-6.

Petitcolas F. A. P., Anderson R. J., and Kuhn M. G., (1998), Attacks on Copyright Marking Systems. **In Proc. of the Int. Workshop on Information Hiding**, Pages: 218-238, 1998.

Pianykh O.S., (2012), **Digital Imaging and Communications in Medicine (DICOM)**. 243 DOI 10.1007/978-3-642-10850-1_11, © Springer-Verlag Berlin Heidelberg.

Popek, G. J., and Kline, C. S., (1979), Encryption and Secure Computer Networks. **Comput. Surv.** Vol. 11, No. 4, Pages: 331-356.

Puech William, (2008), An Efficient Hybrid Method for Safe Transfer of Medical Images. **2nd International Conference: E-Medical Systems**, TUNISIA, Pages: 29-31.

Puech W., Chaumont M., and Strauss O., (2008), A Reversible Data Hiding Method for Encrypted Images. **Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X**, San Jose, CA, USA, Vol. 6819, Pages: 68191E-1--68191E-9.

Rivest R., (1992), **The MD5 Message Digest Algorithm**. RFC 1321.

Roeder T., Pass R., and Schneider F., (2012), Multi-Verier Sgnatures. **Journal of Cryptology**. Vol. 25, Pages: 310-348.

Schilling D. L., Milstein L. B., Pickholtz R. L., and Brown R., (1980), Optimization of the Processing Gain of an M-ary Direct Sequence Spread Spectrum Communication System. **IEEE Trans. Commun.** Vol. COM-28, Pages: 1389 -1398.

Schnorr C. P., (1991), **An efficient Cryptographic Hash Functions**. In CRYPTO.

Sheil, W. C., (2012), **Magnetic Resonance Imaging (MRI Scan)**. MedicineNet.com. Retrieved 27 April 2012.

Silva J. E., (2003), **An Overview of Cryptographic Hash Function and Their Uses**. From the SANS Institute Reading Room site. Retrieved 15 Jan. 2003.

Soliman Mona M., Hassanien Aboul Ella, Ghali Niveen I., and Onsi Hoda M., (2012), An Adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent. **International Journal of Smart Home**, Vol. 6, No. 1.

Stallings, W., (1999), **Cryptography and Network Security**. Prentice Hall.

Swanson M.D., Bin Zhu, A.H.Tewfik., (1996), Transparent Robust Image Watermarking. **In Proceedings of International Conference on Image Processing**. Vol. 3, Pages: 211-214.

Thaler, Pat, (2003), 16-bit CRC Polynomial Selection. **INCITS T10**. Retrieved 11 Aug. 2009.

Trichili H, Bouhlel M, Derbel N, and Kamoun L., (2002), A New Medical Image Watermarking Scheme for A Better Telediagnosis. **Proceedings of the IEEE International Conference on Systems, man and cybernetics**, Hammamet, Tunisia, Vol. 1, Pages: 556–559.

Umaamaheshvari A. and Thanushkodi K., (2012), High Performance and Effective Watermarking Scheme for Medical Images. **European Journal of Scientific Research**, Vol. 67, No. 2, Pages: 283-293.

Umamageswari A., Ferni Ukrit A., and Suresh G. R., (2011), A Survey on Security in Medical Image Communication. **International Journal of Computer Applications**, Vol. 30, No. 3.

Viswanathan P. and Krishna P. Venkata, (2011), Randomized Cryptographic Fusion Watermarking Medical Image with Reversible Property. **International Journal of Computer Information Systems**, Vol. 2.

William J Caelli, Ed Dawson, and S. Rea. Pki., (1999), **Elliptic Curve Cryptography, and Digital Signatures**. Computers & Security. Vol. 18, No. 1, Pages: 47–66.

Wong S. T. C., Abundo M., and Huang H. K., (1995), Authenticity Techniques for PACS Images and Records. **Proc. SPIE**. Vol. 2435, Pages: 68–79.

Zhou X. Q. and Huang H. K., (2001), Authenticity and Integrity of Digital Mammography Images. **IEEE Trans. Med. Imag.** Vol. 20, No. 8, Pages: 784–791.

Zhou X. Q., Huang H. K., Lou S. L., Blaine G. J., and Siegel E. L., (2000), A Study of Secure Method for Sectional Image Archiving and Transmission. **In Proc. SPIE Med. Imag.** Vol. 3980, Pages: 390–399.

دراسة في طرق التشفير والدمغ الرقمي لتراسل طبي آمن

اعداد

نور حسين حاج عبدالله

المشرف

الدكتور غيث عبده

المشرف المشارك

الدكتور علي الحاج

ملخص

مؤسسات الرعاية الصحية في حاجة لتبادل البيانات الطبية ولا يمكن أن تعمل بشكل مستقل دون مشاركة المعلومات الطبية. التراسل الطبي يلعب دورا هاما في توفير حلول لهذه التحديات. ولكن يجب أن يكون تراسلا آمنا بحيث لا يسمح لأي تعديلات على المعلومات الطبية أثناء عملية النقل عبر الشبكة. وأي تطبيق لهذه العملية يجب أن يحقق المتطلبات التالية: التأكد من أن الشخص الذي تسلم البيانات هو الشخص المخول بذلك ، التأكد من أن البيانات المستلمة لم يطرأ عليها أي تعديل أو تغيير ووصلت كما أرسلت من المرسل ، و ضمان أن المعلومات الطبية تعود إلى المريض المعني وصادرة من المصدر الصحيح.

التطبيقات الحالية في مجال التراسل الطبي الآمن تصنف إلى قسمين: التراسل الطبي الآمن المعتمد على التشفير والتراسل الطبي الآمن المعتمد على الدمغ الرقمي. لكن التقنيات المعتمدة على التشفير لا تحقق تضمين معلومات المرضى داخل الصورة الطبية أما التقنيات المعتمدة على الدمغ الرقمي لا تحقق متطلب السرية بحيث لا يراها الشخص الغير مخول باستلام الصورة الطبية لأن الصورة نفسها غير مخفية.

في هذه الأطروحة ، تم تنفيذ ثلاثة أنواع من التقنيات لتلبية المتطلبات الضرورية لتراسل طبي آمن. بالنسبة لمجال التشفير ، تم اقتراح خوارزميتان لغرض تشفير الصورة الطبية والمعلومات الطبية والشخصية المتصلة بها ونجحنا في تحقيق المتطلبات السابق ذكرها. في مجال الدمغ الرقمي اقترحت خوارزمية لغرض إخفاء البيانات الطبية وحققت أيضا المتطلبات السابقة. وثمة تقنية ثالثة وهي تقنية الهجين التي تجمع بين التقنيتين السابقتين ، التشفير والدمغ الرقمي ، لزيادة الأمان في عملية النقل.

تم تنفيذ التقنيات المقترحة ومقارنتها مع خوارزميات سابقة من ناحية تحقيقهم للمتطلبات الثلاثة. تم عمل مقارنات في ما يتعلق بقدرة الخوارزمية على تحري عملية التعرض لأي تعديل أو تغيير في الصورة المنقولة ثم تقييم كل خوارزمية بمقاييس تقييم الأداء ونذكر منها: قياس وقت التنفيذ وقياس جودة الصورة الطبية.

أظهرت النتائج أن التقنيات الثلاثة المقترحة وما فيها من خوارزميات قد حققت متطلبات النقل الطبي الآمن جميعها ولقد تميزت تقنية النقل الطبي المعتمدة على التشفير بعملها على تحقيق المتطلبات على مستوى المعلومات المرتبطة بالصورة وعلى مستوى الصورة نفسها. أما بالنسبة لوقت التنفيذ فقد تفوقت التقنية المعتمدة على الدمج الرقمي مقارنة بالخوارزميات الأخرى. ومن ناحية التحري عن التعديل أو التغيير في الصورة ، جميع الخوارزميات عملت على تحقيق هذه الخاصية إلا أن تقنية الهجين بين الطريقتين كانت المفضلة لقدرتها على الكشف عن مكان التغيير الذي حدث على الصورة بدقة. وعلى النقيض من توقعاتنا أظهرت النتائج أن الخوارزميات المعتمدة على التشفير حاصلة على أفضل القياسات وأدقها ولها من الخصوصية ما يشابه تقنية الهجين ولكن أفضل من التقنية المعتمدة على الدمج الرقمي.