

UNIVERSITY OF BAHRAIN

College of Information Technology



The Development of Security System for Multimedia Information Systems Using Information Hiding

A Thesis Submitted in Partial Fulfillment of the Requirements for the
Master Degree in Information Technology

Submitted by

Amal Hasan AlSaqr

University number: 20114862

Supervised by

Dr. Wasan Shaker Awad

(Associate Professor)

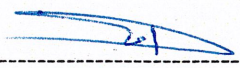
University of Bahrain

Kingdom of Bahrain

December, 2015

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it currently submitted for any degree.

Signed: 
Amal Hasan Isa Alsaqer (Candidate)

Date: 10 / 12 / 2015

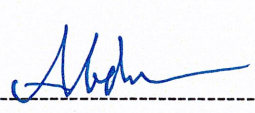
The Thesis defense committee considers the Thesis titled:

The Development of Security System for Multimedia Information Systems Using Information Hiding

Submitted by Amal Hasan Isa Alsaqer to the College of Information Technology is satisfactory and acceptable for the Master of Science in Information Technology.

Thesis Defense Committee:


Dr. Wasan Shaker Awad
(Supervisor)


Dr. Abdullah Al-Dhelaan
(Member)


Dr. Yousif AlBastaki
(Member)

Abstract

As multimedia applications are becoming an integral part of our daily life, the need to protect multimedia systems has become a major concern. The aim of this study is to investigate the use of information hiding for the development of secure multimedia information systems.

The study first examines the current security techniques employed to protect multimedia information systems. Subsequently, the study establishes a security engineering framework to support full security integration with multimedia information systems. The study then utilizes the proposed framework to design and implement a security system for multimedia information systems using information hiding. A case study is conducted to assess the security of a healthcare information system and accordingly demonstrate the use of the proposed framework to reduce risks. Moreover, the proposed security system is evaluated against the quality characteristics of the healthcare information system.

In conclusion, given that the proposed security system yields a lower risk level as compared with the current implemented system, the study findings support the contention that information hiding can considerably improve the security of multimedia information systems. Further, evaluation results demonstrate the superior performance of the proposed security system in terms of accuracy, time behavior, storage utilization, and usability. Nonetheless, the study emphasizes that a systematic approach must be followed through each phase of system development life cycle to ensure optimal utilization of information hiding.

Dedication

This thesis is dedicated to my family
for their love, endless support
and encouragement.

Acknowledgment

First and foremost, I must acknowledge my limitless gratitude to Allah, the Ever-Mighty, for His countless blessings and guidance.

I would like to express my deep appreciation to my supervisor, Dr. Wasan Shaker Awad, for her unending support and encouragement. This work would not have been possible without her generous guidance and unfailing patience.

I also would like to express my sincere thanks to all the institutes and individuals who participated in this study, for their assistance and contribution.

Last but certainly not least, I would like to express a special word of gratitude to my family, who tirelessly provided me with love, support, and inspiration for my scholarly work.

List of Content

Topic	Page
Declaration	I
Abstract	II
Dedication	III
Acknowledgment	IV
List of Content	V
List of Tables	VIII
List of Figures	IX
List of Appendix	X
List of Abbreviations	XI
Chapter One	
Introduction	
1.1 Overview	2
1.2 Statement of the Problem	3
1.3 Research Questions	3
1.4 Research Objectives	4
1.5 Significance of the Study	4
1.6 Limitations	5
1.7 Glossary	5
1.8 Report Structure	6
Chapter Two	
Literature Review	
2.1 Multimedia Information Systems	8
2.2 Methodologies for Secure System Development	9
2.3 Multimedia Information Systems Security	14
2.4 Information Hiding to Protect Multimedia Information Systems	20
2.4.1 Steganography in the Image Spatial Domain	20
2.4.2 Steganography in the Image Transform Domain	23
2.5 Summary	26

Chapter Three	
Security Engineering Process	
3.1 SecSDM Security Engineering	29
3.2 Multimedia Security Engineering Activities	33
3.2.1 Requirements Analysis Phase	34
3.2.1.1 Multimedia Requirements Identification	34
3.2.2 Design Phase	36
3.2.2.1 Multimedia Artifacts Development	37
3.2.2.2 Impact and Trade-off Analysis	38
3.2.3 Testing Phase	39
3.2.3.1 Performance Evaluation	39
3.3 Summary	40
Chapter Four	
Developing a Security System for a Healthcare Information System Using Information Hiding - a Case Study	
4.1 Case Study Overview	42
4.1.1 Research Methodology Justification	42
4.1.2 Research Process	43
4.1.3 Case Selection	44
4.2 Alpha Healthcare System – Data Collection	45
4.2.1 Alpha Healthcare Institute	45
4.2.2 General System Description	46
4.2.3 Security Description	47
4.3 Alpha Healthcare System- Security Risk Assessment	49
4.3.1 Security Risk Assessment Overview	50
4.3.2 Security Decision and Recommended Measures	51
4.4 Developing A Security System for Alpha	52
4.4.1 Requirements Analysis Phase	53
4.4.2 Design Phase	65
4.4.3 Implementation Phase	77
4.4.4 Testing Phase	82
4.5 Summary	89

Chapter Five Conclusion and Future Work	
5.1 Conclusion	92
5.2 Future Work	95
References	97
Appendix	
ملخص الأطروحة	

List of Tables

Number	Topic	Page
3.1	Multimedia Requirements Identification Example	36
3.2	Example of Impact and Trade-off Analysis Templates	39
4.1	Security Risk, Decision, Measure Association	52
4.2	Multimedia Requirements of Alpha	54
4.3	Organizational Impact / Asset Matrix of Alpha	55
4.4	Information Assets Valuation of Alpha	57
4.5	Likelihood of Common Threats in Alpha	58
4.6	Risk Identification of Alpha	60
4.7	Vulnerability Assessment of Alpha	61
4.8	Risk Assessment of Alpha	63
4.9	Risk Prioritization of Alpha	64
4.10	Required Security Services for Alpha	66
4.11	Required Security Mechanisms for Alpha	68
4.12	Vulnerability Assessment of the Proposed Security Architecture	72
4.13	Impact and trade-off analysis for steganography algorithms	76
4.14	Patient Dataset Experimental Results	83
4.15	Employee Dataset Experimental Results	84

List of Figures

Number	Topic	Page
3.1	The Ten-Step process of SecSDM	31
3.2	Security Engineering Activities of MMISs	35
4.1	Overall Research Process	43
4.2	The User Characteristics of Alpha's Information System	46
4.3	The Communication Infrastructure of Alpha	48
4.4	The Proposed Information Security Architecture	70
4.5	Customized Conceptual Representation of Database Tables	74
4.6	The Proposed User Registration Process	79
4.7	The Proposed User Verification Process	80
4.8	Cover and Stego-Images Histograms	88

List of Appendix

Number	Topic
(1)	Interviews – Alpha Case Study

List of Abbreviations

Abbreviation	Full Form
AACS	Advanced Access Content System
AEGIS	Appropriate and Effective Guidance in Information Security
AES	Advanced Encryption Standard
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DICOM	Digital Imaging and Communications in Medicine
DML	Data Manipulation Language
DRMS	Digital Rights Management System
DWT	Discrete Wavelet Transform
FCA	First Component Alternation
GA	Genetic Algorithm
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HSI	Hue-Saturation-Intensity
ISA	Integrated Security Architecture
IWT	Integer Wavelet Transform
JFE	Joint Fingerprinting and Encryption
LSB	Least Significant Bit substitution
LZW	Lempel–Ziv–Welch
MAS	Multimedia Authoring System
MCS	Multimedia Communication System
MDD	Model Driven Development
MISA	Multimedia Information Security Architecture
MMDBMS	Multimedia Database Management Systems
MMIS	Multimedia Information System
MODB	Multimedia Object Database
MPS	Media Processing System
MRBAC	Multi-Role Based Access Control

MSE	Mean Square Error
MSS	Media Sensing System
MVIS	Multimedia Visualization and Interaction System
NIS	Novel Image Steganography
OPAP	Optimal Pixel Adjustment Process
PACS	Picture Archiving and Communication Systems
PCM	Profile and Context Manager
PSNR	Peak Signal-To-Noise Ratio
PVD	Pixel Value Differencing
RBAC	Role-Based Access Control
RFE	Rewritable Fingerprint Embedding
SDL	Security Development Lifecycle
SDLC	System Development Life Cycle
SecSDM	Secure Software Development Model
SSDM	Secure Software Development Model
SWT	Stationary Wavelet Transform
WAN	Wide Area Network
XP	eXtreme Programming
XSE	eXtreme Security Engineering

Chapter One: Introduction

1.1 Overview

1.2 Statement of the Problem

1.3 Research Questions

1.4 Research Objectives

1.5 Significance of the Study

1.6 Limitations

1.7 Glossary

1.8 Report Structure

Chapter One: Introduction

This chapter provides an overview of the study, emphasizing the research problem, questions, objectives, significance, and limitations.

1.1 Overview

As per (O'docherty & Daskalakis, 1991), a Multimedia Information System (MMIS) can be defined as "a repository for all types of information objects". As the name would suggest, MMISs are capable of storing and representing a wide range of digital data including text, images, audio, and video. MMISs architecture consists of numerous components, namely: Multimedia content generation, storage, distribution, receiving, consuming, editing, and sharing (Lian et al., 2009).

Due to their significant role in multimedia management, MMISs are becoming an integral part of our daily life. Needless to say, as such systems become more and more accepted, various security concerns have emerged. As a countermeasure, many security solutions have been proposed to protect MMISs including cryptography and steganography mechanisms.

In (Cheddad et al., 2010), steganography is defined as "the science that involves communicating secret data in an appropriate multimedia carrier". The key idea behind steganography is that the very existence of secret information should be concealed in order to prevent any kind of attack. In steganography, the secret information is concealed within a host file such that the modifications made to the host are not evident. Types of hosts may include any form of media content. Broadly, data undergoes the following operations in steganography: 1. Detection of redundant data in the host file.

2. Allocation of a fragment of the redundant data to be substituted with secret data.

3. Data substitution (Provos & Honeyman, 2002).

1.2 Statement of the Problem

With the recent advances in information technology and the increasing quantity of media utilized by different applications, MMISs security assurance has become an essential public concern. Due to the rapid growth of security threats, it is crucial to establish a scheme that will enhance MMISs security. Key challenges in MMISs security may include confidentiality protection, integrity confirmation, and privacy enforcement. In the era of global networking, the need to protect multimedia content has become a major priority. With the exception of information hiding, security techniques generally do not utilize the specific features of multimedia content to achieve security. Accordingly, this research aims to investigate how information hiding techniques can be employed to improve the security of MMISs.

1.3 Research Questions

In order to resolve the research problem, the following research questions are formulated:

- Are the current security techniques - such as encryption - effective to protect MMISs?
- Can information hiding improve the security of MMISs?
- How does information hiding affect the quality characteristics of MMISs?

1.4 Research Objectives

In an effort to answer the research questions, the following research objectives are set:

- To identify, discuss, and review the current security techniques used to protect MMISs.
- To develop a security engineering framework to support MMISs security.
- To design and implement a security system for MMISs using information hiding.
- To evaluate the proposed security system against the quality characteristics of MMISs.

1.5 Significance of the Study

The significance of MMISs is ever-increasing with the growing amount of data generated, stored and shared by users globally. Societies worldwide are becoming progressively more dependent on multimedia applications such as teleconferencing, distance learning and virtual reality simulations. However, with popularity comes great risk as unauthorized operations may compromise the security of MMISs.

MMISs security assurance is rather complex task (Lian et al., 2009). Reasons for such fact may include the difficulty of security enforcement due to the diversity of multimedia types. The large size associated with multimedia content might be considered a limiting factor for many security techniques. Further, novel multimedia systems emerge periodically, causing new security concerns to surface.

Over the past decades, numerous methods have been introduced to protect MMISs. Nevertheless, the vast majority of such methods are concerned solely with the security of multimedia content. Upon

reviewing the literature, no studies were found to address the specific needs of MMISs with regards to security engineering. Further, to the best of my knowledge, no studies were identified that developed a security design utilizing information hiding to secure organizations in Bahrain. Hence, the purpose of this study is to develop a security system to protect MMISs using information hiding.

1.6 Limitations

The study is restricted in the scope owing to the following limitations:

- Given that the considered case study utilizes a private network, secure multimedia communication through open channels will not be discussed in this thesis.
- The study will solely consider images as the steganographic cover medium.
- The study will largely emphasize the design, implementation, and evaluation of information hiding, whereas the remainder security mechanisms will not be discussed as deeply.
- The proposed security architecture will not be implemented and deployed on target environment due to organizational constraints.

1.7 Glossary

Below is a glossary of terms used in this study:

- Multimedia information system: "A system capable of processing multimedia data and applications" (Ojha et al., 2011).
- Quality characteristics: "A set of properties of a software product by which its quality can be described and evaluated" (Bertoa et al., 2003).

- Security: "The protection of computing systems against threats to confidentiality, integrity, and availability" (Sundaram, 1996).
- Software system architecture: "A logical organization of its components" (Younis, 2011).
- Information hiding (steganography): "A technique that inserts secret messages into a cover medium, so that the existence of the messages is not apparent" (Hong et al., 2008).
- Cover medium: "The medium into which a secret message will be embedded" (Hansen, 2007).
- Stego-medium: "The medium created once the secret message is successfully hidden in the cover medium". (Memon et al., 2008)
- Cryptography: "A process which is associated with scrambling plaintext into ciphertext (encryption), then back again (decryption)" (Sarker et al., 2005).

1.8 Report Structure

This dissertation comprises five chapters. This first chapter provides a brief introduction of the study and presents the research problem, questions, objectives, significance, and limitations.

Chapter2 provides a context for the research by examining the relevant literature on the topics of multimedia systems, security engineering, multimedia systems security, and information hiding.

Chapter3 discusses the novel multimedia security engineering framework implemented in this study.

Chapter4 utilizes the proposed framework to develop a security system for a healthcare information system.

Chapter5 concludes the dissertation. It presents the study findings and recommendations for future research directions.

Chapter Two: Literature Review

2.1 Multimedia Information Systems

2.2 Methodologies for Secure System Development

2.3 Multimedia Information Systems Security

2.4 Information Hiding to Protect Multimedia Information Systems

2.5 Summary

Chapter Two: Literature Review

This chapter provides a thorough review of literature on the topics of multimedia systems, security engineering, multimedia systems security, and information hiding.

2.1 Multimedia Information Systems

Multimedia systems research investigates the means by which computer/human communication can be enhanced utilizing diverse forms of media. Types of data in multimedia systems vary from simple unstructured text to highly complex objects.

Multimedia systems research has benefited from two major facts. First, numerous daily life applications are multimedia applications in nature, which can be exemplified by libraries and education. Further, the technology required to build MMISs is becoming commonly accessible (O'docherty & Daskalakis, 1991). According to O'docherty and Daskalakis, the ideal MMIS is characterized by a set of features such as the ability to store all types of digital media, allowing the user to query and browse the stored media, managing media connections if made by users, maintaining a reasonable response time, providing editors to enable media creation/alternation, and offering compression techniques to enhance performance.

Sapino and Candan (2008) defined MMISs as the systems where data management (i.e. storage, indexing, querying, and retrieval) and media management capabilities (i.e. media representation, compression, and transmission) are coupled. Single-media objects of different data types (i.e. text, images, audio, and video) may unite to form complex multimedia objects. In contrast with conventional objects, multimedia objects are often described as temporal, spatial, and interactive. Due to

the distinctive nature of multimedia objects, MMISs are expected to offer two major components: A presentation component for multimedia objects viewing, and a storage/retrieval component for object maintenance. It is evident that database and multimedia systems originally appeared as separate fields involving different application domains. Nevertheless, the latest domains improvements have managed to narrow the gap between the former fields. Accordingly, activities within the discipline of MMISs have flourished and expanded since the mid nineties. Sapino and Candan (2008) assume that MMISs architecture consists of eight sub-systems, namely: Multimedia Authoring System (MAS), Media Sensing System (MSS), Media Processing System (MPS), Multimedia Communication System (MCS), Multimedia Visualization and Interaction System (MVIS), Multimedia Object Database (MODB), Profile and Context Manager (PCM), and Digital Rights Management System (DRMS).

2.2 Methodologies for Secure System Development

Security engineering is an engineering discipline that deals with the establishment of secure systems. Security engineering field entails a wide range of methods and procedures that tackles security concerns during system development. In recent years, researchers have extensively investigated the means by which security can be fully incorporated into system development. Numerous security enhanced models have been introduced in academic research with either alternation or insertion of security activities in the conventional development lifecycle (Moradian, 2012).

Motivated by the fact that many security engineering approaches do not sufficiently stress the overheads caused by security mechanisms, Markotten (2002) emphasized the importance of user-centered security engineering where users are involved in every aspect of security

development. The aim of Markotten's study was to establish a "usable security", where end users are capable of protecting themselves and their systems efficiently, effectively, and satisfyingly. The proposed approach combines the processes of security engineering and usability engineering into an integrated user-centered security engineering framework. The framework comprises five primary user-centered phases, namely analysis, threat and risk analysis, security strategy and model, design and implantation, and testing. To validate the applicability of the proposed framework, it was used to build the "Identity Manager", a security tool to protect users over the Internet. Nonetheless, the proposed approach lacks further details and refinement.

Another security model is eXtreme Security Engineering (XSE) (Beznosov, 2003). Beznosov investigated eXtreme Programming (XP) and its applicability in security engineering. XP has proven successful in terms of software development, especially when utilized with frequently varying requirements and budgets. Accordingly, XP practices were employed to establish XSE, a novel security engineering approach. In oppose to defining security at early stages of software development, XSE allows the customer of a security project to define security and adjust the definition at any stage. Beznosov argues that XSE can be effectively adopted to create "good enough security" solutions while maintaining high success rates and customer satisfaction. Despite the fact that XSE has not been implemented explicitly by the author, the success of interactive and incremental development approaches in manufacturing along with the technical evidence of XP success in software development have led to the conclusion that XSE is a better solution for numerous security engineering projects. However, not every project is expected to benefit from XSE as its scope was defined as "non safety-critical security engineering projects with volatile requirements".

Hatebur et al. (2006) introduced a novel approach to security engineering based upon problem frames. The utilization of problem frames enables security engineers to organize, characterize, evaluate, and eventually solve software development problems. The authors established two types of problem frames, namely security problem frames and concretized security problem frames. In the proposed approach, security problem frames are associated with the security requirements of a system, which are primarily identified as patterns to be instantiated. The Security requirements are then transformed into concretized security requirements, causing the security problem frames to evolve to concretized security problem frames. Utilizing the concretized security problem frames outlines broad security mechanisms, which require certain security protocols to function. Thus, each concretized frame is assigned to a security protocol representing a potential solution to the given security problem. The proposed security frames are intended to be a part of more comprehensive collection as means of assisting security engineers to select frames and protocols that apply for a given situation. Hence, such collection will prevent common omissions by addressing all security aspects associated with the given situation. Nonetheless, the security problem frames approach does not cover the entire development process of security-critical systems as it does not involve the later development stages.

Howard and Lipner (2006) introduced the Security Development Lifecycle (SDL) security assurance model. SDL attempts to reduce software vulnerabilities by integrating security and privacy into all phases of software development. SDL involves a set of security activities that are based upon three major concepts: Education, constant process improvement, and accountability. However, De Win et al. (2009) argue that SDL has very few analysis activities and lacks real implementation

Development Life Cycle (SDLC). The SecSDM process aims to minimize the security risks by early detection and removal of system vulnerabilities. Initial experiments confirmed the applicability of SecSDM where promising results were obtained. Further, SecSDM associated documentation guarantees that the entire security process is auditable.

Cabot and Zannone (2008) argued that current security engineering approaches merely address limited security aspects of software development. Thus, a Model Driven Development (MDD) framework was proposed to ensure security throughout the entire development process. MDD utilizes models throughout software development and offers automation during model execution, transformation, and code generation. The suggested model-driven development undergoes four fundamental phases, namely: Organizational context, system requirements, system design, and system implementation. The integrated framework is capable of identifying, modeling, and evaluating all security aspects of any given system, where each aspect is managed in the most suitable phase of the development process. Despite the numerous benefits introduced by the proposed framework, there are several issues of concern. The framework requires further efforts to overcome challenges such as horizontal and vertical integration of security mechanisms.

Kim and Cha (2012) proposed a layered security engineering model in an attempt to analyze, design, implement, test, and maintain secure enterprise information systems. The model utilizes three layers to secure enterprise information systems, namely: Security management, security architecture, and security mechanisms and services layers. Security management layer outlines the particular needs for security risk management, whereas enterprise security architecture layer describes the different aspects of security policies, mechanisms, and procedures.

Further, security mechanisms and services layer identifies the technology selected to secure the enterprise architecture. While Kim and Cha's proposed methodology specifies the security activities corresponding to each phase of SDLC; it does not illustrate the precise tasks needed in each activity.

As appears from aforesaid, many security engineering frameworks have been proposed over the years. Nonetheless, given its numerous advantages and adherence to international standards of good practice, SecSDM was chosen as the basis of our work.

2.3 Multimedia Information Systems Security

Due to their significance, MMISs must offer appropriate solutions to any probable security threat. Over the past decades, many approaches have been proposed to secure multimedia systems. To address the various aspects of security, multiple techniques can be used in conjunction to result in better overall protection. Such techniques are exemplified by: Digital rights management, fingerprinting, multimedia forensics, secure user interfaces, encryption, and information hiding.

Uludag and Jain (2003) established a security framework to protect multimedia content. The suggested framework combines biometrics and cryptography to achieve higher levels of security. To avoid vulnerabilities caused by illegal key exchange in cryptography, users' biometric features can be utilized for authentication purposes. In terms of cryptography, the proposed system uses a combination of symmetric and asymmetric key schemes. Nonetheless, given that the computational needs of asymmetric key schemes are considerably larger than that of symmetric key schemes, the system primarily uses the former for encrypting small amounts of data, while it uses the latter to encrypt the actual multimedia content. To initiate a secure multimedia transmission, the user must use the public

key of the server to encrypt his/her personal data (i.e. username, password, and biometric data) before sending it to the server. Upon receiving the encrypted data, the sever uses its private key for decryption, then checks the validity of the user. If user information was proven to be valid, the server creates a password, encrypt it, and send it back to the user along with the encrypted multimedia content. Finally, the user will decrypt the multimedia content using the encryption keys in reverse order. To showcase the proposed framework, Uludag and Jain (2003) utilized Data Encryption Standard (DES) algorithm and recorded the time required for encryption/decryption. The time measured was found acceptable.

Lin et al. (2006) investigated digital fingerprinting in scalable multimedia systems. Digital fingerprinting is a promising mechanism that is widely utilized to prevent illegitimate modification and redistribution of multimedia content. It labels each distributed copy of data with distinct ID, known as “fingerprint”. Multi-user collusion is an attack where multiple attackers collectively attempt to eliminate traces of the fingerprints. To defy multi-user collusion, Lin et al. examined the side information based fingerprinting techniques for scalable multimedia. The study confirms that the possession of attacks-related information throughout the colluder identification procedure can considerably enhance traitor tracing. The study also investigates the means by which the detector can explore side information from the colluded media. Such investigation allows researchers to develop a comprehension of the relation between the detector and the colluders in multimedia forensics, and facilitates more powerful multimedia security. Further, the authors proposed a method allowing fingerprint detectors to explore side information from the colluded media themselves. The study proved that the detector achieved optimum performance using the proposed method.

Thuraisingham (2007) outlined the security concerns associated with Multimedia Database Management Systems (MMDBMS). Thuraisingham examined various security measures utilized in MMDBMSs, namely: Adequate security policies, secure system architectures, and secure data models. Security policies are application-specific rules used to enforce security. Similarly, secure system architectures and data models can enhance security by considering security early in the system development. The study also describes the impact of security on the different aspects of MMDBMS such as management functions, distributed multimedia management, inference problem, and quality of service. As a final point, the study reviewed the security issues facing multimedia information management systems exemplified by digital libraries, E-commerce, semantic webs, multimedia publishing, and stream information processing.

In light of the fact that decrypted data loses the imposed security and may be unlawfully distributed, Sun et al. (2007) proposed the Joint Fingerprinting and Encryption (JFE) security scheme that incorporates fingerprinting with cryptography. The proposed scheme aims to accomplish two major security goals, namely multimedia access control and traitor tracing. JFE scheme was embedded into the Advanced Access Content System (AACS). AACS primarily include four key elements: Content owner, licensed replicator, key management, and licensed user end. Akin to other systems, security threats are expected to emerge in the proposed scheme. To deal with such threats, the paper applied multimedia encryption at various points to defy several attacks. Moreover, the paper suggested Rewritable Fingerprint Embedding (RFE) to tackle multi-point collusion attacks. Experimental results demonstrated that the transmitted images steadily remain in the encryption domain at the different ends of the scheme. In terms of resistance to single collusion attack, the catching

probability decreases when the number of colluders increases. Also, the results confirm that at least one colluder in multi-point collusion attack can be caught at the replicator end.

Zhao et al. (2008) established a multimedia extension to the Role-Based Access Control (RBAC) model to address the security requirements of multimedia applications. The proposed Multi-Role Based Access Control (MRBAC) model offers full support to distributed multimedia applications by enabling multi-level protection of multimedia content, restricting access by time and IP constraints, and decentralizing administration privileges. In their preceding studies, the authors established a security framework called SMARXO. SMARXO utilizes three stages to secure multimedia applications (i.e. multimedia indexing, security modeling, and DBMS management). The security modeling stage is primarily the stage responsible for MRBAC. As opposed to the traditional RBAC, MRBAC defines four major roles: User, object, temporal, and spatial. While RBAC model defines user roles as the range of actions prohibited to users, MRBAC model extends user roles definition to include the sets of accessing objects, access duration, and IP address. Further, MRBAC role categories are expressed in a hierarchical manner that is performed using the object-oriented concept. To evaluate the proposed MRBAC model, the authors showcased two scenarios that may occur in a multimedia system. The complicated nature of the suggested scenarios proves that RBAC is insufficient to manage particular multimedia applications.

Rednic and Toma (2009) conducted a study to investigate security management in multimedia systems. The study was initiated by examining the means of multimedia storage, management, and processing. Oracle database was selected to exemplify multimedia database management. The choice was based upon the fact that Oracle

utilizes the benefits of InterMedia objects to store graphics. In accordance with the study, multimedia security can be accomplished on the database as well as the user interface. Database security can be managed on two levels: The user and the data levels. Security measures on user level may include user roles, access control, and Data Manipulation Language (DML) operations. Further, security measures on data level may include watermarking and embedding links on metadata level. In an attempt to measure the security of a multimedia system, the study established a novel multimedia metrics system. The proposed matrices system utilized two data-level multimedia security measures namely watermarking and embedded links.

In an effort to develop multimedia information security architecture, Susanto and Muhaya (2010) reviewed various concepts related to information security, such as information security management systems, ISO 17799 security management standard, e-business security architecture, and information security architecture. In their study, Susanto and Muhaya extended Eloff's Integrated Security Architecture (ISA) to address multimedia security. Primarily, ISA model comprises five distinct components: security infrastructure, security policies, security culture, monitoring compliance, and security program. To tackle the complex nature of multimedia systems, the proposed Multimedia Information Security Architecture (MISA) appends three additional components to ISA, namely multimedia information sharing, enterprise security, and security awareness. While multimedia information sharing outlines mechanisms for secure multimedia communication, enterprise security ensures that the enterprise implements security solutions (e.g. access control, administrator monitoring, and content filtering) in a consistent manner. Further, security awareness aims to raise users' awareness

towards information security concepts, exemplified by security standards, policies, and procedures.

Venkateswaran Radhakrishnan and Venkatachalam (2011) founded a security model upon both cryptographic and steganographic principles. Authentication, secrecy, integrity, and availability are among the security goals of the model. The proposed security system primarily utilizes poly-alphabetic substitutions cipher to encrypt secret data prior to concealing it in a suitable multimedia carrier. The study emphasized on incorporating the cipher with audio and image LSB steganography. As the name would suggest, the poly-alphabetic substitution is achieved using multiple keys, which encrypt plaintext based upon letters placement in text. To provide an additional layer of security, the resultant cipher is then embedded into various media formats before being transmitted over networks. In conclusion, Radhakrishnan and Venkatachalam suggested various applications that may benefit from the proposed system.

In accordance to Govinda et al. (2013), current security mechanisms are insufficient for real time multimedia communication. Multimedia applications often generate continuous media streams, which may include sensitive data. Hence, developing security frameworks for real time multimedia communications is a necessity. Govinda et al. (2013) aimed to secure on-demand video streams over clouds. The proposed security model utilizes the Advanced Encryption Standard (AES) algorithm to partially encrypt video streams. The encryption key is exchanged among users via the Diffie-Hellman key distribution algorithm. To evaluate the proposed model performance, the time delay parameter was measured opposed to RC4 algorithm. Experiment results indicate that AES gives less delay and better performance as compared with RC4.

2.4 Information Hiding to Protect Multimedia Information Systems

The literature is rich with steganography techniques that share the common target of concealing the existence of secret data. In general, steganography techniques can be classified by two means: By the hiding method (i.e. injection, substitution, and generation) or by the type of host file (i.e. image, audio, and video). Motivated by the fact that image steganography is the most extensive steganographic research area, this study is solely dedicated to steganography in image files.

Image steganography can be subdivided into two major classes, namely spatial and transform. In the following sub-sections, an overview of image steganography will be presented classified upon steganography domains. Section 2.4.1 discusses spatial domain based techniques which embed secret data directly in the pixels of the cover image, such as Least Significant Bit substitution (LSB). Section 2.4.2 discusses the transform domain based methods which apply some transformations to the cover image before embedding the secret data, such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Integer Wavelet Transform (IWT), and Discrete Wavelet Transform (DWT).

2.4.1 Steganography in the Image Spatial Domain

Spatial domain steganography involves bit-wise manipulations that utilize bit insertion and noise addition. Lossless image formats are mostly associated with spatial domain steganography, whereas the spatial algorithms are primarily dependent on the image format. Despite their simplicity, high capacity, and low computational costs, spatial domain techniques are widely criticized for their low robustness against attacks and image processing.

Kumar (2012) established a novel two-tier security framework based upon cryptographic and steganographic mechanisms. The proposed framework relies on AES algorithm as means of cryptography. AES is a symmetric block cipher which performs iterations of rounds to encrypt private data. The encrypted data is then concealed within a cover image using alteration component steganography. In alteration component technique, the pixels of the cover image are replaced by a stego-key as well as the encrypted private data. Kumar claims that the suggested framework is effective for secret communication since the stego-images achieved good perceptual quality and the canceled data cannot be detected by naked eye.

Similarly, Phad Vitthal et al. (2012) incorporated spatial image steganography and cryptography into a two-tier security framework to achieve high-level security. The suggested security model utilizes AES to encrypt secret data prior to canceling it into RGB images using Pixel Value Differencing (PVD) with K-bit LSB substitution. PVD technique calculates the difference between two successive pixels in the cover image, whereas the difference corresponds to the embedding capacity. A small difference value (i.e. small embedding capacity) is typically located on a smooth area and a large difference value (i.e. large embedding capacity) is typically located on an edged area. Experimental results demonstrated that the proposed model excels in both image quality and embedding capacity criteria. Hence, the authors declared the two-tier security model effective for covert communication.

Kaur and Sardana (2013) proposed a spatial image steganography technique called Novel Image Steganography (NIS). NIS is an improved version of First Component Alternation (FCA) technique where secret data is hidden in the blue component of image pixels as the spatial perception of blue is less accurate than of red and green. Likewise, NIS

utilizes the blue component of a pixel in 24-bit RGB images to conceal secret data. However, In NIS, a secret key is employed to determine the actual embedding location. To conceal secret data, NIS performs XOR operation on the least significant bit of the red component of image pixel and one bit of the secret key. The result is then calculated to decide whether the secret data is embedded in the first or last four bits of the blue component. Since the embedding location is determined by the secret key, Kaur and Sardana (2013) claim that NIS is more secure than FCA and LSB techniques. Further, NIS allows better stego-image quality given that it merely utilizes four bits of the blue component for storage of one secret bit (in comparison to FCA that hides eight bits in one pixel and LSB that hides one bit in one pixel). Experimental results confirmed that the diminutive distortions caused by concealing large amounts of data using NIS are undetectable by the human visual system.

Based upon LSB replacement, Muhammad et al. (2014) introduced a novel approach for image steganography via Hue-Saturation-Intensity (HSI) color model. The HIS color model originates from RGB model as it corresponds to the means of color perception and interpretation. The proposed approach converts an image from RGB to HSI color space prior to embedding secret data into the intensity plane using LSB steganography. The image is then converted back to RGB color space. Experiments were conducted to evaluate the proposed technique both subjectively (i.e. via the human visual system) and objectively (i.e. via mathematical standards). Experimental results confirmed that the proposed technique surpassed LSB steganography in terms of imperceptibility, security, and image quality.

2.4.2 Steganography in the Image Transform Domain

Transform domain steganography concerns image transform algorithms which conceal secret data in more significant frequencies of the cover image. Unlike spatial domain steganography, transform domain techniques often support lossy image formats. One major benefit of transform domain steganography is its ability to resist a wide variety of attacks and image processing operations. Nonetheless, transform domain techniques generally suffers from high computational costs, and low embedding capacity.

In view of the fact that JPEG is a commonly utilized lossy image format, Muttoo and Kumar (2009) investigated information hiding in JPEG images. They established a novel steganographic technique Based upon Jsteg algorithm. When Huffman codes are employed in serial communications, a loss of synchronization may cause complicated resynchronization procedures. Accordingly, in oppose to Huffman codes in Jsteg, Muttoo and Kumar suggested utilizing T-codes to encode the secret data into cover images. Peak Signal-To-Noise Ratio (PSNR) values of the proposed technique were calculated and compared to those obtained using the original Huffman-based Jsteg. The comparison demonstrated that PSNR values of both techniques are almost identical. Further, due to the self-synchronization ability of T-codes, the proposed technique is more robust as it allows the extracted data to be decoded without destruction.

AbdulLatef (2011) developed a novel steganography scheme based on DCT and DWT. The scheme divides a given cover image into four equal parts. Depending upon the higher color ratio, a channel (i.e. red, green or blue) is selected from each part. DWT is performed on the selected channel to decompose it into four bands (i.e. LL, HL, LH and HH). On the contrary, a secret image is divided into four $n \times n$ blocks on

which DCT is performed. The proposed scheme concludes by embedding the four DCT blocks in the four high frequency sub-bands of the cover image. The resultant stego-image was found perceptually invisible with elevated quality. Further, to increase the embedding capacity of the proposed scheme, AbdulLatef suggests utilizing alternative DWT sub-bands such as HL and LH.

Ghasemi et al. (2011) introduced a novel image steganography scheme based upon Genetic Algorithm (GA) and Wavelet Transform. To embed secret data, the cover image is divided into 4x4 blocks, which are transformed to the frequency domain (via 2D Haar DWT). Each block is then mapped to 16 equivalent genes. Further, the message bits are embedded in k-LSBs DWT coefficients in accordance with the mapping function, whereas the best mapping function is determined by fitness evaluation. To improve the imperceptibility of the proposed scheme, Optimal Pixel Adjustment Process (OPAP) is performed after data embedding. The simulation results illustrated that the proposed scheme surpassed adaptive wavelet transform techniques in terms of imperceptibility and capacity. However, despite the increased robustness offered by GA, the proposed scheme suffers from high computational complexity.

Sheisi et al. (2012) introduced a modified version of JSteg algorithm, which they called DCT replacement. Broadly speaking, DCT replacement follows the embedding process of JSteg; However, DCT replacement manipulates DCT coefficients differently. In contrast to JSteg where secret data is embedded in all AC coefficients, DCT replacement embeds data merely in the middle frequencies. To illustrate further, DCT replacement initiates embedding from the last coefficient in the middle frequencies area, whereas the least significant bit of each coefficient is substituted with message bits. It is worthy of mentioning

that DCT replacement utilizes two major parameters: The number of embedded coefficients (n) and the number of bits in each coefficient (b). In order for the receiver to extract the secret message, these parameters must be known. Thus, n and b parameters are considered as keys resulting higher security level of the proposed algorithm. Experimental results demonstrated that the replacement algorithm outperforms Jsteg in terms of imperceptibility and robustness against statistical attacks. Nonetheless, JSteg excels in the capacity criterion.

Given the fact that stego-images may encounter noise and distortions during transmission, Singh et al. (2013) incorporated image enhancement and steganography into a single security framework. The primary goal of such framework is for the receiver to obtain noise-free stego-images that preserve the embedded secret data. To reach the required goal, two algorithms are utilized: The first algorithm is responsible for noise alimentation and contrast enhancement, while the second algorithm is responsible for information hiding (i.e. DFT steganography). PSNR values obtained using the proposed filter along with DFT were compared to those obtained using median filter with LSB. The results demonstrated that the proposed filter outperforms the median filter as it improves the contrast of stego-images.

Dalvi and Patil (2014) proposed a transform domain image steganography technique, where a grayscale image is concealed within an RGB image. The color planes of the cover image are separated prior to the extraction of either the DWT or the Stationary Wavelet Transform (SWT) coefficients of the blue plane of both the cover and the secret image. The extracted coefficients are then employed in the fusion process. Subsequently, inverse DWT/ SWT is performed to obtain the stego-image. The utilization of dual transforms in the proposed method primarily attempts to improve the robustness aspect of information

hiding. Upon measuring the imperceptibility of the proposed method, Dalvi and Patil (2014) affirmed that high invisibility can be achieved regardless of the size of secret data.

Goel et al. (2014) established a novel image stenography framework based upon IWT. To achieve high embedding capacity, secret data is compressed prior to embedding. Further, IWT steganography is initiated after color plane separation of the cover image whereas IWT is performed on each plane independently (i.e. red, green, and blue). To indicate the embedding capacity of each plane, the proposed framework utilizes modified pixel indicator technique (i.e. if the most significant bit of high frequency coefficients is 1 then embed three bits, otherwise embed one bit). The proposed framework concludes its processes by performing OPAP to reduce the error difference. In comparison with analogous techniques, the proposed approach offered better PSNR values and more simple computations. Experimental results confirmed the high imperceptibility and embedding capacity claimed by the authors.

2.5 Summary

The purpose of this review is to examine the fields of multimedia systems security, security engineering, and information hiding. Literature analysis has revealed several key findings as listed below:

1. Due to their complex nature, MMISs require special consideration in terms of security management.
2. To enforce stricter security, security must be introduced as early in the development lifecycle as possible. Further, security engineering activities should be fully incorporated into SDLC phases.
3. Current security techniques may offer diverse security services to MMISs. However, apart from information hiding, there is no other

security technique to utilize the unique features of multimedia content to accomplish further security.

4. There is no information hiding algorithm to satisfy all the quality characteristics of software systems. The process of algorithm selection is application dependant. Nonetheless, transform domain techniques generally offer greater security as compared to spatial domain techniques.

Accordingly, the following benefits were gained upon reviewing the literature:

1. SecSDM will be utilized as a basis for development of an extended MMISs security engineering framework.

2. The current literature on steganography algorithms will be further examined, whereas the key features of a given algorithm will be analyzed and compared against those of other algorithms. To develop a security system for MMISs, the analysis results will be used to support the algorithm selection decision.

3. Current objective image quality matrices (e.g. PSNR) will be employed to estimate the accuracy of the proposed steganographic system.

Chapter Three: Security Engineering Process

3.1 SecSDM Security Engineering

3.2 Multimedia Security Engineering Activities

3.3 Summary

Chapter Three: Security Engineering Process

This chapter discusses the security engineering methodology implemented in this work. The methodology is based upon SecSDM security engineering process (Futcher & von Solms, 2007). Nonetheless, novel activities are introduced to address the security needs of MMISs.

3.1 SecSDM Security Engineering

According to Futcher and von Solms (2007), SecSDM is a comprehensive set of security-centered activities that is driven by the need to build trust in computing. To reach the security goals of a system, SecSDM extends the core system development process to incorporate security procedures. In other terms, a range of security engineering activities is introduced in correspondence to each phase of SDLC. SecSDM is based upon Microsoft's security development lifecycle and adopts its viewpoint of a very detailed security development.

SecSDM was chosen as the foundation of this research as it reflects the principles of various international standards and best security practices including ISO/IEC 17799, the international code of practice for information security management, the risk analysis approach as determined by ISO/IEC TR 13335-3, the NIST SP 800-14, and ISO 7498-2. Moreover, SecSDM lifecycle strongly emphasizes security as early in the development lifecycle as possible, while other security models may merely focus on certain phases or may be too obscure to validate (Davenport, 2013). To confirm system security, SecSDM utilizes a checklist to guide the security process through requirements to implementation. A further positive aspect is that SecSDM was strictly validated through experiments and prior studies, where encouraging results were obtained.

SecSDM entails five phases, namely: Investigation, analysis, design, implementation, and maintenance. SecSDM investigation and analysis correspond to SDLC requirements phase, while the remainder of SecSDM phases correspond to the phases of the same name in SDLC. The general methodology of SecSDM is outlined in figure 3.1.

The ten-step process of SecSDM can be summarized as follows:

- STEP 1: Information asset identification and valuation.

In this activity, the critical information assets of an organization are identified and listed based upon checklists and judgment. Such assets are exemplified by customer records, financial transactions, and employee details. Asset identification is followed by asset valuation, where values are assigned to each information asset. The assigned values reflect the sensitivity and significance of the assets to the organization. SecSDM utilizes a five-point scale to assess the business impact of information assets, where the value 0 corresponds to negligible and the value 4 corresponds to critical. The values of information assets can be determined based upon the estimation of information owners and key users.

- STEP 2: Threat identification and assessment.

Threat identification and assessment is an essential step towards risk management. Threat identification aims to adequately guide successive security engineering decisions. To assist the process of threat assessment, SecSDM offers a checklist of common threats that is based on ISO/IEC TR 13335-3. Further, SecSDM estimates the potential impact of each identified threat by assigning threats to likelihood levels (i.e. low, medium, or high).

- STEP 3: Risk (asset/threat) identification.

In order to determine the potential risks to a system, risk identification process necessitates the definition of asset/threat

associations. Risk identification considers the key assets determined in step1 (i.e. impact value = 3 or 4), and the most likely threats determined in step2 (i.e. high impact).

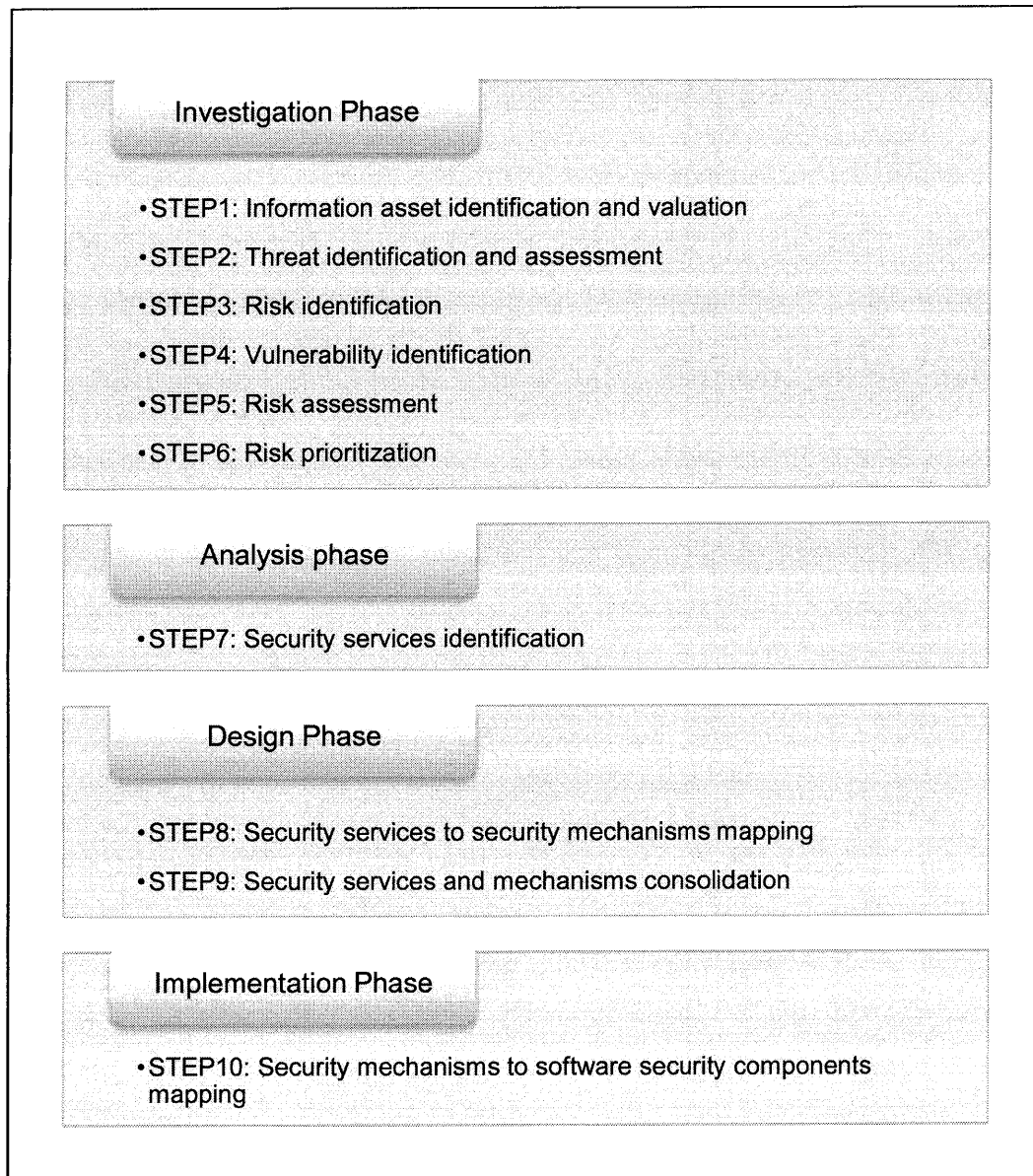


Figure (3.1)
The Ten-Step process of SecSDM

- STEP 4: Vulnerability level determination.

In light of the fact that many attackers compromise security by seeking system vulnerabilities, it is curtail to determine the level of

vulnerability for each critical risk identified in the preceding step. SecSDM offers three vulnerability levels, namely: Low, medium, and high. In order to estimate the level of vulnerability for each risk, the current system state and controls must be considered.

- STEP 5: Risk assessment.

Risk assessment process aims to determine the extent of risks on the basis of asset impact value, vulnerability level, and threat likelihood. The three factors are matched in a lookup table to measure risks on a scale of 1 to 8. SecSDM defines its risk values in accordance with ISO/IEC TR 13335-3 specifications.

- STEP 6: Risk prioritization.

Risk prioritization is a key process to provide a guideline for succeeding SDLC phases. Risk can be prioritized by merely listing each risk and its corresponding risk value as determined in the previous step.

- STEP 7: Security services identification.

In this step, security engineers map the most critical risks, as determined during the investigation phase, to security services. The main purpose of risk-to-service mapping is to establish an optimal level of protection as an attempt to reduce critical risks.

- STEP 8: Services to mechanisms mapping.

Security service-to-mechanism mapping describes the activity of choosing the most suitable security mechanism to implement a given security service. Such mapping is required for all security risks identified in the investigation phase. To support security engineers in selecting the most suitable mechanisms; SecSDM offers a defined set of security guidelines. For instance, if confidentiality service is needed, then encryption mechanism can be utilized.

- STEP 9: Security services and mechanisms consolidation.

Security services and mechanisms consolidation facilitate security implementation. Thus, security engineers are required to map security mechanisms to the suitable security services for each security risk, as determined in the preceding steps.

- STEP 10: Mechanisms to components mapping.

Mechanism-to-component mapping concerns implementing security mechanisms through software components. However, in order to ensure that the correct security characteristics are utilized, a priority list is required to determine the priority of the security mechanisms. Hence, security developers are responsible to determine the particular system components through which the security mechanisms will be implemented.

3.2 Multimedia Security Engineering Activities

Given the fact that multimedia systems are widely employed in critical organizational activities (e.g. customer support, sales, and technical support), several development concerns are expected to surface. Such concerns may relate to the means by which requirements are managed, development is controlled, or security is enforced. It is reasonable to assume that more sophisticated approaches are needed to resolve the various concerns associated with multimedia systems (Barry & Lang, 2003).

Upon a thorough examination of the literature, no studies were found to address the security engineering process in multimedia systems. It is evident that an extension in security engineering towards MMISs is needed. Thus, we attempt to establish a set of security-centered activities to tackle the particular needs of MMISs. Such activities will be

incorporated into SecSDM security engineering to build a comprehensive MMISs security engineering framework as illustrated in figure 3.2.

In the succeeding subsections, we will discuss our proposed multimedia security activities classified upon the development phase they correspond to.

3.2.1 Requirements Analysis Phase

In this phase, the detailed requirements of multimedia systems with respect to multimedia content should be specified. Identifying multimedia requirements at a later point in the life cycle makes dealing with them a lot more difficult. Further, inadequate requirements analysis may cause serious problems to surface in the subsequent development phases. Thus, special attention must be given to the requirement analysis phase.

3.2.1.1 Multimedia Requirements Identification

To construct further comprehension of multimedia systems and the mechanisms by which they should be secured, multimedia requirements must be clearly stated at early development stages. (Barry & Lang, 2001) emphasized the need for capturing multimedia systems requirements and integrating them within a systems development framework.

Multimedia requirements identification involves investigating the media types utilized by the system. Upon concluding this activity, the security engineer should develop a fundamental understanding of the types of media captured, stored, managed, or transmitted by the system, whether particular technologies are utilized for such propose (i.e. software and hardware equipment), and whether certain constrains are necessitated (e.g. compression, quality, or format requirements).

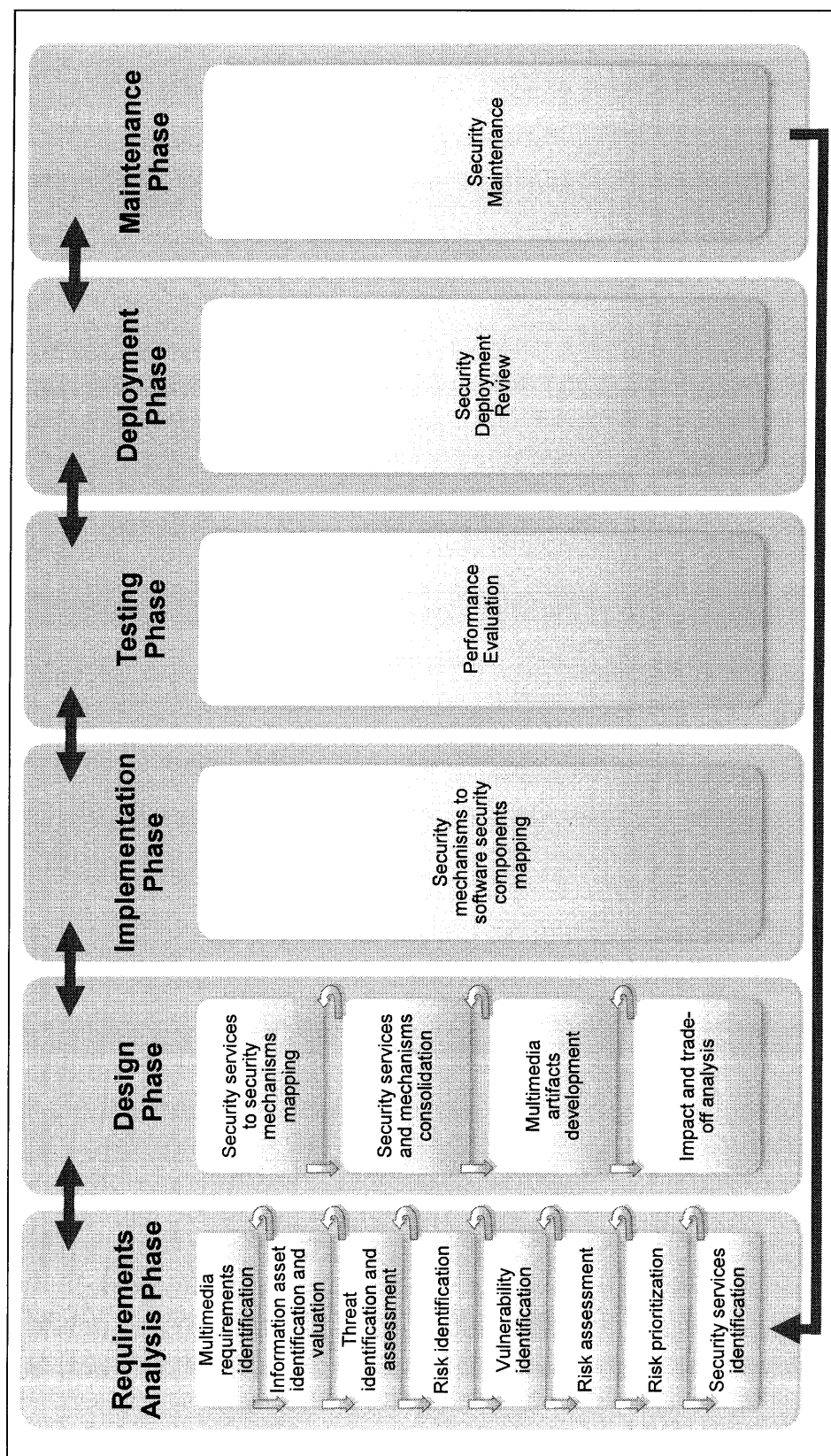


Figure (3.2)
Security Engineering Activities of MMISs

Multimedia requirements identification process may entail the queries to follow:

- What types of media are utilized by the system?
- Are there any restrictions on media files?
- What types of hardware and software resources are used to manage media, and what are their characteristics?

The output of multimedia requirement identification can then be classified in a tabular form indicating different media types (see table 3.1).

Table (3.1)

Multimedia Requirements Identification Example

Media Type	Input Device	Format	Volume	Transfer Rate
text	keyboard	ASCII	10 KB/page	2 KB/page
image	camera	JPEG	100 KB/image	0.5 MB/image
audio	microphone	MPEG	0.5 MB/min	7 KB/sec
video	webcam	PAL	4 GB/min	20 MB/sec

The identified multimedia requirements play an essential role in the design phase where an appropriate security mechanism can be selected based upon available media types and restrictions. For instance, restrictions on image size may render it unsuitable for concealing large volumes of data. Similarly, many steganography algorithms are format-dependent.

3.2.2 Design Phase

The design of MMISs primarily involves establishing a structure to large volumes of diverse data and ensuring its accessibility to users. Requirements confirmed in the analysis phase should guide the design phase. The design phase entails constructing artifacts and models to fulfill

system requirements. Thus, system modeling mechanisms offer goal-oriented tasks to establish the desired system design.

At the design phase, the following multimedia inquiries should be addressed:

- What multimedia storage/retrieval architecture is best suited for security purposes?
- How to manage heterogeneity in system requirements and media characteristics?
- How to minimize the costs introduced by the complex nature of multimedia content?
- How to estimate the expected impact of multimedia security mechanisms prior to implementation?

To sufficiently address such queries, further activities shall be conducted at the design phase as follows:

3.2.2.1 Multimedia Artifacts Development

Security in multimedia systems may not be fully interpreted in conventional system artifacts; hence comes the necessity of multimedia artifacts development. Multimedia artifacts development involves building customized artifacts to reflect security concerns in multimedia system. Types of conventional artifacts to be extended may include architecture diagrams, security models, and services assessment.

By the end of this activity, a complete set of multimedia artifacts must be generated. The set of developed artifacts represents an essential input to successive security engineering activities. Further, multimedia security artifacts allow maintaining strong communication among people involved in the security process (i.e. designers, users, etc.).

3.2.2.2 Impact and Trade-off Analysis (Balancing Costs Against Threats)

The unforeseen impacts of design decisions are often discovered belatedly in the system development life cycle, when they cost much higher to resolve.

Security has a direct impact on the runtime behavior of a system. Security often comes with a cost as security mechanisms may require additional computational power and resources. Thus, security may introduce increasing overhead in terms of performance (e.g. execution time, response time, and latency) as well as resource consumption. As a consequence, security engineering must offer a means by which quality attributes -including security - can be prioritized to achieve the desirable balance.

Security is interconnected with the reminder of non-functional requirements of the system. Thus, it is essential to evaluate the impact of security controls across multiple dimensions, as it allows the security engineer to assess diverse architectural variations prior to system realization, hence establishing confidence in the security architecture (Hansson et al., 2008).

Impact and trade-off analysis is especially important in multimedia systems, due to the complex and heterogeneous nature of multimedia content that places additional demands on system resources. Hence, suitable measures must be provided to estimate the potential impacts of MMISs security design decisions.

The outcomes of impact and trade-off analysis can be organized in a tabular form as illustrated in table 3.2.

The security technique column represents the potential security mechanisms to protect a given system. Moreover, the features (impact of security) columns represent the key quality requirements of the given

system, whereas each system will emphasize different range of requirements. The values inside the table will indicate the level/range associated with each quality requirement for each security technique.

Table (3.2)

Example of Impact and Trade-off Analysis Templates

Security Technique	Features (Impact of Security)			
	Speed	Accuracy	Robustness	File size
Private Key Encryption				
Public Key Encryption				
Transform Domain Steganography				

3.2.3 Testing Phase

The testing phase entails validating the performance of security against other quality attributes. During this phase, multiple tests are conducted to confirm the quality of implemented security.

3.2.3.1 Performance Evaluation (Quality of Security)

Aside from security, multimedia systems are required to offer additional quality attributes to its users. However, increased security is often associated with degraded performance. Hence, the key principle of performance evaluation activity is to assess the impact of security mechanisms on the performance of multimedia systems.

Once a certain level of security is agreed upon in the preceding engineering phases, the quality of implemented security must be measured. In performance evaluation process, security is measured against organization-critical quality attributes (e.g. usability, availability, etc.) either through experiments or simulations. Evaluating the performance of secured system prior to deployment is essential to avoid

further deployment issues. Moreover, this activity is particularly crucial in multimedia systems due to the complexity of multimedia security procedures that may negatively affect the runtime behavior of the system.

3.3 Summary

In this chapter, we introduced a novel multimedia security engineering framework that is based upon SecSDM security development process. The proposed framework extends the security activities of SecSDM to meet the particular needs of MMISs. Accordingly, the framework introduces further security activates in the requirement analysis, design, and testing phases.

In an effort to validate the proposed multimedia security engineering process, it will be utilized in the next chapter to design and implement an experimental MMIS. Our intent is to inspect, elaborate, and offer detailed solutions to secure the different aspects of multimedia systems.

Chapter Four: Developing a Security System for a Healthcare Information System Using Information Hiding - a Case Study

4.1 Case Study Overview

4.2 Alpha Healthcare System – Data Collection

4.3 Alpha Healthcare System – Security Risk Assessment

4.4 Developing a Security System for Alpha

4.5 Summary

Chapter Four: Developing a Security System for a Healthcare Information System Using Information Hiding - a Case Study

In the preceding chapter, we introduced a novel model for security engineering in multimedia systems. The different phases of the proposed model shall be further described and implemented with the aid of a case study; a healthcare information system.

4.1 Case Study Overview

In this section, details of the case study methodology followed in this study are described. The motivation behind the selection of the methodology is explained. Then, the research process is briefly discussed. Lastly, the factors for selecting the subject of the case study are elaborated.

4.1.1 Research Methodology Justification

A case study is a research approach that is primarily utilized to study a contemporary occurrence within its real life context (Schell, 1992). The case study approach was selected for our thesis to gain an insight of the current security practices within an elected organization.

Case studies are often viewed as an effective tool for the preliminary, exploratory phases of a research (Rowley, 2002); Hence it shall serve as a basis for the development of an effective multimedia security system. Further, case study research may benefit from multiple data sources that offer the ability to reinforce the study results and conclusions.

Case studies support a deeper investigation of a given situation; thus, case studies are best suited to answer how and why research questions. In the course of our thesis, a case study shall be utilized to answer the research questions below:

- Are the current security techniques - such as encryption - effective to protect MMISs? and why?
- How does information hiding improve the security of MMISs?
- How does information hiding affect the quality characteristics of MMISs?

4.1.2 Research Process

A research process is a logical path that connects the research questions to conclusions. It is an action plan that ensures research coherence (Rowley, 2002). Figure 4.1 outlines the different stages that will be followed to answer the research questions.

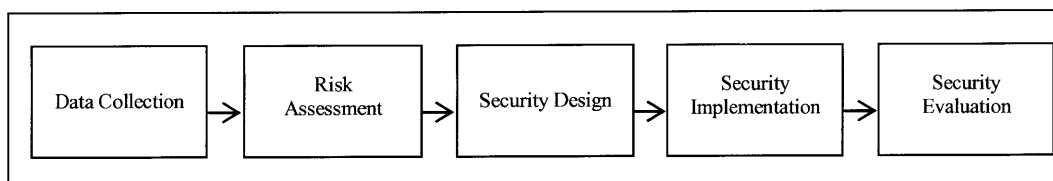


Figure (4.1)
Overall Research Process

Data collection is the cornerstone of reliable research. In the data collection stage, the research process will be initiated by an in-depth investigation of the information system of a selected organization. Subsequently, a security risk assessment will be conducted to expose the key threats to the current system and eventually assess the effectiveness of the implemented security measures. In response to assessment findings, a security system will be designed and implemented based upon

the security engineering model introduced in the previous chapter. Finally, the proposed security system will be evaluated based on a number of criteria to determine its effectiveness.

4.1.3 Case Selection

Healthcare information systems were selected as the subject of the case study. Such selection was strongly motivated by the factors to follow:

- Information security in the healthcare field is a concern of emergent significance. The adoption of electronic health records and the increasing health information exchange have lead to the need for improved information security.
- Governments worldwide have issued health information privacy regulations to protect the confidentiality of patients. Such regulations enforce tough penalties to organizations that fail to safeguard patient information.
- Electronic patient records can store a large amount of medical information in various forms (i.e. text, images, video). Modern medical equipment may generate diagnostic information in multiple forms and formats of digital media (e.g. X-ray, CT, and MRI are common image types in the medical sector). Hence, healthcare information systems are an ideal candidate for the study of security in multimedia systems.
- Besides security, healthcare organizations stress other critical quality attributes such as efficiency and usability. Therefore, healthcare is a suitable field for studying the trade-off among security and other quality attributes.

Since the foundation of this thesis is security, the confidentiality of the selected healthcare organization is required. Hence, the healthcare institute under investigation will be referred to as "Alpha".

4.2 Alpha Healthcare System – Data Collection

This section will delineate the data gathered throughout the data collection process including system description, user characteristics, and security practices.

The principal data were gathered through semi-structured interviews with employees of varying positions (see appendix1). Further, secondary data were collected through documentation and direct observation of daily operations.

4.2.1 Alpha Healthcare Institute

Alpha healthcare institute is located in the Kingdom of Bahrain. It offers wide-ranging medical services to general public with multiple clinics, laboratories, and pharmacies. The medical services are provided by highly qualified physicians and technicians as Alpha is keen on manpower training in order to fulfill its strategic plan, that is to “enhance the quality and quantity of health services”.

Alpha is fully committed to its mission, to “provide its clients an access to inclusive health care”. The technical liability for supporting this care lies with the development of an effective information system. The executive authority of Alpha had outsourced the information system development task to an abroad company. Alpha information system offers physicians, lab technicians, and clerical staff immediate access to patient's medical records. Despite Alpha had automated the majority of its sub-systems, few parts of the system still operate manually (e.g. pharmacy sub system).

4.2.2 General System Description

The information system of Alpha is utilized within the healthcare institute by the registered staff only. Administrators, patient records staff, doctors, and lab technicians are the principal users of the system. All registered users are required to undergo basic training prior to using the system. The system offers its users a user-friendly experience by enabling a Graphical User Interface (GUI). Figure 4.2 demonstrates the user characteristics of the information system.

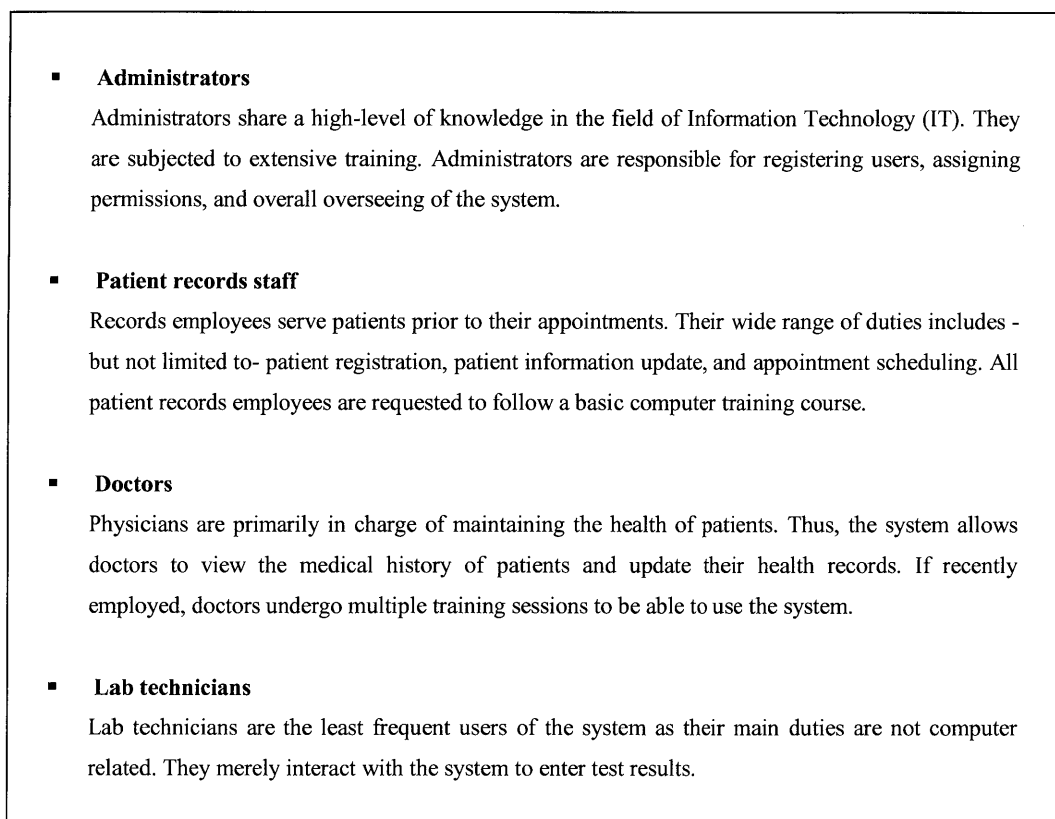


Figure (4.2)

The User Characteristics of Alpha's Information System

Within the existing system at Alpha, patient records are stored in multiple datacenters, and retrieved through patient IDs. To be able to benefit from Alpha medical services, a patient is required to schedule an appointment. An appointment can be scheduled by patient records employees either directly or via phone calls. In addition to scheduling

appointments, patient records staff are responsible for numerous services as demonstrated in figure 4.2.

Needless to say, when a patient is assigned to a doctor for an appointment, the patient is automatically added to the doctor patients list. Doctors are capable of accessing the medical records of the patients on their lists. Further, Alpha information system allows doctors to enter the diagnosis of patients along with other medical services.

Lab technicians are responsible for conducting basic medical tests to patients such as blood and urine tests. Lab technicians' sole interaction with the information system involves recording test results through patient IDs.

Alpha uses a client-server model, where a client requests healthcare services from the server and the server responds with the required services. The system's client-server architecture permits users of different roles to have access to Alpha's data centers.

In addition to the connectivity within Alpha (between the clients and the server), Alpha is inter-connected with external healthcare institutes via a Wide Area Network (WAN). Furthermore, Alpha is inter-connected to a third trusted party. The communication infrastructure of Alpha is outlined in figure 4.3.

4.2.3 Security Description

Security safeguards allow healthcare providers to offer their services to the public without any malicious actions. To prevent information security breaches, Alpha implements three categories of safeguards as follows:

1. Administrative controls:

Administrative controls refer to the administrative measures used to enforce security. Alpha administration implements a wide range of

controls to protect its information. Alpha's information system is guarded by means of an authentication scheme that utilizes unique user identifiers. System administrators provide each user with a password that should be changed at a maximum period of two months. Alpha stores user passwords in an encrypted form. Moreover, information security training is conducted to staff members to exercise safety measures against potential risks. In such training, system users are instructed to log-off from the system once their access is completed, not to reveal their login information, and so forth. Staff members can receive security related information, through training, meetings, and administration announcements. Further, audit trails are maintained in sufficient detail and analyzed periodically to track user operations.

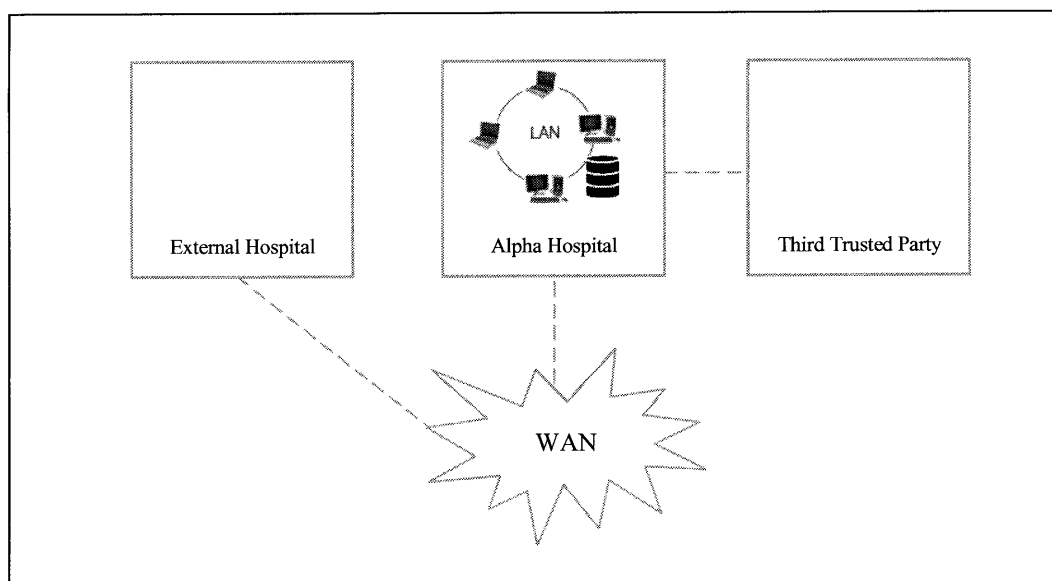


Figure (4.3)

The Communication Infrastructure of Alpha

2. Physical controls:

Alpha implements various physical measures to safeguard its information system from unauthorized access and environmental risks. Workstations, servers, and data centers are positioned in secured locations that are not accessible by unauthorized individuals. Each

secured location is protected by biometrics access doors where a valid fingerprint must be provided. As a supplement to the biometrics access system, alpha utilizes video surveillance cameras to trace any suspicious behavior. Furthermore, Alpha backs up its data periodically to support disaster recovery. Backups are stored in protected offsite locations.

3. Regulations, procedures and policies:

Broadly, the Health Insurance Portability and Accountability Act (HIPAA) outlines data protection laws in the healthcare sector. Regrettably, there are no such data protection laws in the Kingdom of Bahrain (global data privacy, 2014). However, Alpha grants its patients the right to confidentiality of medical records. In other words, the medical record of a patient can be viewed only by physicians who are directly involved in his/her treatment. Otherwise, the authorization of the patient or his/her legal representative is required. Needless to say, Alpha maintains written documentations of adopted security procedures and policies as a reference.

4.3 Alpha Healthcare System- Security Risk Assessment

Given the fact that the main purpose of security is to reduce system exposure to potential risks, it is crucial to estimate the effectiveness of the utilized security controls. To confirm the effectiveness of a security control, we shall calculate the control impact on the probability of risks realization.

In healthcare sector, the core objective is to deliver a superior healthcare experience to patients. Consequently, the risks that may compromise such objective must be minimized. For such purpose, a security risk assessment process shall be followed. Based upon the results

of the risk assessment, security decisions and actions must be made to highlight security shortcomings and eventually reduce security exposures.

4.3.1 Security Risk Assessment Overview

In accordance with SecSDM methodology, the process of security assessment entails five major tasks, namely: Asset valuation, threat assessment, risk identification, vulnerability identification, and risk assessment and prioritization.

The detailed process of risk assessment will be further discussed in the subsequent sections. However, we shall emphasize the major findings of the process in this section as below:

- Asset valuation: Health information, payment information, and user account information are declared critical information assets to Alpha based upon their organizational impact. If any critical asset were to be lost, damaged, or exposed, Alpha would face catastrophic consequences.
- Threat assessment: Theft of information, use of system by unauthorized users, and masquerading of user identity are identified as the most potential threats to the system. Through observation, many system users were seen leaving their workstations logged in and unattended. Further, the strict policy of not allowing unauthorized staff members to enter restricted areas (i.e. areas secured by biometrics access doors) was violated by a number of employees. Such actions are most likely to increase the probability of unauthorized system access resulting in higher possibility of information theft or damage.
- Risk identification: Risk identification entails establishing asset/threat associations. It determines which key assets are most

likely to be targeted by threats. Accordingly, the following risks are found the most critical to Alpha: Theft of user account information, payment information, or health information, disclosure of sensitive health information, payment information, or user account information through unauthorized access, and accidental insertion of erroneous health information.

- Vulnerability identification: Bearing in mind the current security controls of Alpha, the system is declared partially exposed to theft of critical assets, use by unauthorized users, and accidental insertion of erroneous health information.
- Risk assessment and prioritization: Risk assessment calculates the value of risks on the basis of asset impact value, threat likelihood, and vulnerability level. With respect to their risk values, the following risks are granted th higher priority: Theft of user account information, payment information, or health information, disclosure of sensitive health information, payment information, or user account information through unauthorized access.

4.3.2 Security Decision and Recommended Measures

For each identified risk, a security decision is made. The association among security risks, decisions, and recommendations is represented in table 4.1 as suggested by (INTOSAI EDP Audit Committee, 1995).

While high-level risks necessitate risk control, medium-level risks should be either controlled or avoided by the administration. Nonetheless, low-level risks requires less effort as they may be avoided, limited or accepted.

Risks can be controlled by implementing further security measures, avoided by modifying operational procedures, limited by acquiring insurance coverage, or accepted by maintaining the current security state.

In case of multiple possible decisions, the security action to be taken is dependent upon professional judgment and action costs.

Table (4.1)

Security Risk, Decision, Measure Association (INTOSAI EDP Audit Committee, 1995)

Risk level	Decision	Recommended Measure
High (6,7,8)	Risk control	Further countermeasures are required
Medium (3,4,5)	Risk control Risk avoidance	Further countermeasures are required Operational procedures modification / enhancement is required
Low (0,1,2)	Risk avoidance Risk limitation Risk acceptance	Operational procedures modification / enhancement is required Insurance coverage is required No modification is required

In view of what precedes, and given that the security of Alpha is compromised by numerous high-level risks, it becomes crucial to establish an improved security scheme to reduce the risks of the current system.

4.4 Developing a Security System for Alpha

Once the security of the current system is reviewed, suitable security actions must be adopted to improve its status. To determine which security solution is best suited for Alpha, we shall follow the integrated multimedia SecSDM framework as described in chapter3. Hence, this section will discuss the detailed security engineering activities required for developing a security system for Alpha grouped upon the development phase of occurrence.

4.4.1 Requirements Analysis Phase

This phase initiates the security engineering process by identifying the multimedia requirements of the information system and assessing the current security system.

Step1: Multimedia Requirements Identification

It is found upon interviews that two main types of media are utilized by the system, namely text and images. The majority of patient records are stored in a textual form. In contrast, images are the most utilized media in the radiology department. The following diagnostic imaging units are available at the radiology department:

- X-ray units.
- Computerized tomography scanning units.
- Magnetic resonance imaging scanning units.
- Ultrasound units.
- Nuclear medicine units.
- Bone mineral densitometry units.
- Mammography units.
- Thermo luminescent dosimeter units.

Digital Imaging and Communications in Medicine (DICOM) is the industry standard format for clinical imaging devices data. DICOM standard is used for the storage, distribution, and processing of medical images (Blackledge et al., 2013). DICOM files contain a header which holds a description of the image as well as basic patient information. Medical images are maintained in the radiology information system which is connected to the hospital information system via the Picture Archiving and Communication Systems (PACS).

In addition to medical images, Alpha stores identification photographs of its employees and patients. Given that JPEG is the most

common image format used by digital cameras, identification images are stored in JPEG file format. Table 4.2 outlines the multimedia requirements of Alpha.

Table (4.2)
Multimedia Requirements of Alpha

Media Type	Input Device	Format	Size Restrictions
Text	Keyboard	-	Dependant on the database attribute format
Diagnostic images	Medical imaging devices	DICOM	-
Identification images	Camera	JPEG	Size <100 KB

Step2: Assets Identification and Valuation

Information assets identification refers to the process of identifying the principal information assets of a system. Identifying valuable information assets is a matter of answering a few simple questions (e.g. which assets are crucial to the success of the system? Which assets generate the most revenue? Which assets would be the most expensive to lose? Which assets would cause more damage to Alpha if exposed?).

Findings from interviews suggest that Alpha's information assets are classified into six categories as follows:

- Patient basic information (e.g. name, age, gender, nationality, contact information).
- Patient health information (e.g. diagnosis, diagnostic images, test results, insurance information).
- Appointment information (e.g. date, time, assigned doctor).
- Payment information (e.g. payment amount, credit card number).
- Staff information (e.g. name, position, salary, contact information).
- User account information (e.g. username, password, fingerprint data).

Information valuation is the process of assigning an appropriate value to information assets. The assigned value reflects the significance of the asset to the organization. To evaluate Alpha's information assets, we study the assets impact on five key factors, namely: Service delivery, organizational reputation, patient health, organization finances, and legal obligations (see table 4.3). Such factors were derived from the interview findings and the review of healthcare literature.

Table (4.3)

Organizational Impact / Asset Matrix of Alpha

Information Assets	Impact Area				
	Service Delivery	Reputation	Patient Health	Finance	Legal Obligations
Asset A Patient Basic Info.	X		X		
Asset B Health Information	X	X	X	X	X
Asset C Appointment Info.	X	X	X		
Asset D Payment Info.	X	X		X	X
Asset E Staff Information					X
Asset F User Account Info.	X	X	X	X	X

Table 4.3 represents the organizational impact of Alpha's information assets. For each information asset, the impact value should be assigned based on worst case scenarios as follows:

- Patient basic information: If patient contact information were lost, it will be difficult to inform patients of their future appointments timing, which will impact the quality of service delivery. Moreover, if basic information such as age were altered, it may affect the medical treatment of patients causing potential damage to their health.

- Health information: If patient health information were not available, it will impact the delivery of medical service to patients. Furthermore, if health information were altered, it may affect the medical treatment of patients causing potential damage to their health and lives. Also, the disclosure of health information can severely damage Alpha's reputation and finances, as policies and regulations enforce patient privacy.
- Appointment information: If appointment information were altered or lost, the scheduling function will be affected which may negatively impact the delivery of Alpha's services. Further, latency in medical service delivery may cause negative consequences to the health of patients and ultimately harm the reputation of Alpha.
- Payment information: If payment information (e.g. credit card information) were disclosed or lost, it will cause devastating effects to the clinic's reputation and finances as such information is declared confidential by law. Moreover, unavailability of payment information may affect service delivery as some medical procedures require advance payment.
- Staff information: In the legal point of view, organizations are obliged to protect the personal information of their employees. Thus, staff information must be protected against disclosure.
- User account information: User account information controls the access to the system, its data, and services. Hence, losing such information may prevent the access to the system. Further, If user account information were disclosed, Alpha's reputation will face serious legal consequences as the patient health and finances will be compromised.

With respect to what precedes, we assign an impact value to each information asset as below:

- If the asset does not impact any of the impact areas indicated in table 4.3, the asset value is declared negligible.
- If the asset impacts merely one area, the asset value is declared low.
- If the asset impacts two areas, the asset value is declared medium.
- If the asset impacts three areas, the asset value is declared high.
- If the asset impacts more than three areas, the asset value is declared critical.

Accordingly, table 4.4 represents the information assets valuation of Alpha.

Table (4.4)
Information Assets Valuation of Alpha

Information Assets	Assets Impact Value				
	0 Negligible	1 Low	2 Medium	3 High	4 Critical
Asset A Patient Basic Info.			X		
Asset B Health Information					X
Asset C Appointment Info.				X	
Asset D Payment Info.					X
Asset E Staff Information		X			
Asset F User Account Info.					X

Step3: Threat Identification and Assessment

Many threats may compromise the security of Alpha's information system. Such threats can potentially damage the information assets identified earlier. Based on field notes from observations and interviews,

table 4.5 lists the common threats which may harm the system and their level of likelihood.

Table (4.5)

Likelihood of Common Threats in Alpha

Common Threats (ISO/IEC TR 13335-3:1998)	Level of Likelihood/Frequency		
	Low	Medium	High
Theft of information			X
Use of system by unauthorized users			X
Use of system in an unauthorized manner	X		
Masquerading of user identity			X
Malicious software attacks	X		
User errors		X	
Repudiation	X		
Technical software failures or errors	X		
Others: Equipment damage by natural disasters	X		

The assigned values reflect the probability that a particular threat may negatively impact organizational assets as follows:

- Given the observation that staff members occasionally leave their workstations unattended while logged in, in addition to the violation of restricted areas policy by a number of employees; information theft and use of system by unauthorized users are considered high potential threats.
- With regard to the current controls in Alpha (i.e. authorization and logging user actions), use of system in an unauthorized manner by authorized users is declared a low potential threat.
- In view of the fact that masquerade attacks can be perpetrated by bypassing the authentication process, and given that many system users were observed leaving their workstations unattended while

logged in; masquerading user identity is considered a high potential risk.

- Since Alpha operates a private network and employees are not permitted to connect their personal devices to the network, malicious software attacks are viewed as low potential threats.
- Wherever possible, the current information system of Alpha offers predefined inputs to choose from. However, few user error incidents have been reported over the past years. Hence, user errors are assigned a medium likelihood level.
- Alpha supports non-repudiation by means of authentication and secure audit logs. Thus, repudiation is declared a low potential threat.
- Technical software failures are assigned a low likelihood level due to the fact that Alpha frequently maintains its information system, and therefore has a low system failure rate.
- Due to the low natural disaster rate in Bahrain, the threat of equipment damage caused by natural disasters is assigned a low likelihood level.

Step4: Risk (Asset/Threat) Identification

Futcher and von Solms (2013) refer to risks as threats that exploit certain vulnerabilities thereby causing damage to assets. As a result, risk identification necessitates determining asset/threat relationships to establish which risks will presumably have harmful impacts.

Risk identification considers the key assets determined in step2 (i.e. impact value = 3 or 4), and the most likely threats determined in step3 (i.e. medium or high impact). With regard to the data collected through interviews and observation, table 4.6 highlights the most critical risks (i.e.

asset/threat associations) to Alpha. In accordance with SecSDM, it is generally adequate to define eight key risks.

Table (4.6)

Risk Identification of Alpha

Common Threats (refer to step3)	Information Assets (refer to step2)					
	Asset A	Asset B	Asset C	Asset D	Asset E	Asset F
Theft of information		Risk3		Risk2		Risk1
Use of system by unauthorized users		Risk4		Risk5		Risk6
Use of system in an unauthorized manner						
Masquerading of user identity		Risk4		Risk5		Risk6
Malicious software attacks						
User errors		Risk7				
Repudiation						
Technical software failures or errors			Risk8			
Others: Equipment damage by natural disasters						

Table 4.6 conveys what follows:

- The threat of information theft mainly jeopardizes user account information, payment information (i.e. credit card numbers), and health information.
- The threat of unauthorized system use mainly jeopardizes health information, user account information, and payment information.
- The threat of masquerading attacks mainly jeopardizes health information, user account information, and payment information.
- The threat of user errors mainly jeopardizes health information.
- The threat of technical failures mainly jeopardizes the availability of appointment information.

Further, it is noted that both system use by unauthorized users and masquerading of user identity threats were assumed analogous. This is mainly due to the fact that the system is protected by an authentication process, hence obliges unauthorized users to masquerade users identity to be able to access the system.

Step5: Vulnerability Level Determination

To initiate an attack, intruders seek system vulnerabilities and weaknesses. Thus, it is essential to calculate the level of weakness for each security risk identified in the preceding step (i.e. low, medium or high). Needless to say, the current security controls of Alpha must be taken into account when assessing vulnerabilities. Table 4.7 summarizes the process of vulnerability assessment.

Table (4.7)

Vulnerability Assessment of Alpha

Risks (refer to step4)	Vulnerability Level		
	Low (Protected Asset)	Medium (Partially Exposed Asset)	High (Exposed Asset)
Risk1		X	
Risk2		X	
Risk3		X	
Risk4		X	
Risk5		X	
Risk6		X	
Risk7		X	
Risk8	X		

The vulnerability levels assigned to each risk (refer to step4 for risks definition) can be justified as follows:

- Risk1: Alpha stores user passwords in an encrypted form. However, encrypted database attributes can be either decrypted or destroyed by attackers. Thus, additional security measures should be adopted to safeguard user account information.
- Risk2: Alpha stores credit card numbers in an encrypted form. Nonetheless, since encrypted database attributes can be either decrypted or destroyed by attackers, payment information are declared partially exposed to theft.
- Risk3: Alpha stores sensitive health information in an encrypted form. Nonetheless, since encrypted database attributes can be either decrypted or destroyed by attackers, health information are declared partially exposed to theft.
- Risk4: Alpha restricts the access to sensitive health information by means of user authentication and authorization. However, masquerading the identity of authorized users may compromise such information. Hence, health information is partially exposed to unauthorized access.
- Risk5: Alpha restricts the access to payment information by means of user authentication and authorization. However, masquerading the identity of authorized users may compromise such information. Hence, payment information is partially exposed to unauthorized access.
- Risk6: Alpha restricts the access to user account information by means of user authentication and authorization. However, masquerading the identity of authorized users may compromise such information. Hence, user account information is partially exposed to unauthorized access.

- Risk7: Errors by physicians or lab technicians might compromise health information. However, Alpha offers drop-down menus allowing users to choose from predefined inputs in some cases. Thus, the system is partially exposed to user errors.
- Risk8: The technical controls implemented by Alpha ensures the availability of appointment data to support day-to-day operations. Thus, scheduling information are declared protected against technical failures.

Step6: Risk Assessment

Risk assessment aims to estimate the value of risks on the basis of asset impact value, threat likelihood, and vulnerability level. The three factors are matched in SecSDM lookup table to measure risks on a scale of 1 to 8 as demonstrated in table 4.8. This step is merely a summary of steps 2 to 5.

Table (4.8)

Risk Assessment of Alpha

Asset Impact Value	Likelihood of Threat								
	Low			Medium			High		
	Vulnerability Level			Vulnerability Level			Vulnerability Level		
	Low	Medium	High	Low	Medium	High	Low	Medium	High
0 Negligible	0	1	2	1	2	3	2	3	4
1 Low	1	2	3	2	3	4	3	4	5
2 Medium	2	3	4	3	4	5	4	5	6
3 High	3 Risk8	4	5	4	5	6	5	6	7
4 Critical	4	5	6	5	6 Risk7	7	6	7 Risk1,2,3, 4,5,6	8

The Assigned values can be justified as follows:

- Risks 1 to 6 correspond to critical assets (i.e. health, payment, or user account information) that are partially exposed (i.e. medium vulnerability level) to high potential threats (i.e. information theft or unauthorized access). Hence, they are assigned to the value 7.
- Risk 7 is associated with a critical asset (i.e. health information) that is partially exposed (i.e. medium vulnerability Level) to a medium potential threat (i.e. user errors). Thus, it is assigned to the value 6.
- Risk 8 corresponds to a high impact asset (i.e. appointment information) that has a low vulnerability level against a low potential threat (i.e. technical software failures). Thus, it is assigned to the value 3.

Step7: Risk Prioritization

Risk prioritization sets the grounds for succeeding SDLC phases. Risks are prioritized by simply listing each risk and its corresponding risk value as determined in the previous step (see table 4.9).

Table (4.9)

Risk Prioritization of Alpha

Risk	Description	Value
Risk1	Theft of user account information	7
Risk2	Theft of payment information	7
Risk3	Theft of health information	7
Risk4	Disclosure of health information through unauthorized access	7
Risk5	Disclosure of payment information through unauthorized access	7
Risk6	Disclosure of user account information through unauthorized access	7
Risk7	Accidental insertion of erroneous health information	6
Risk8	Scheduling service not available due to technical errors	3

4.4.2 Design Phase

In the requirement analysis phase, we initiated the security engineering process by evaluating the risks associated with the current information system of Alpha. In the context of the design phase, we continue our security efforts by establishing a security design to mitigate such risks.

In correspondence to table 4.1, additional security measures are necessitated to reduce the possibility of high level risks. Hence, our security design must reflect how the security measures are utilized to diminish the most critical risks identified in the preceding phase. Further, to comply with the scope of the thesis, we shall emphasize the use of information hiding as a recommended security measure.

Step8: Security Services Identification

To minimize the most critical risks identified in the requirements phase, an adequate set of security services must be defined. Enforcing such services will eventually lead to elevated protection. The ISO 7498-2 standard defines five essential security services to secure software systems, namely: Identification and authentication, authorization, confidentiality, integrity, and non-repudiation. Table 4.10 outlines the process of selecting security services in accordance with their ability to mitigate risks.

The assigned services are based upon (Davenport, 2013) and (Kouns & Minoli, 2011), where the following guidelines were recommended:

- Theft of information (i.e. risks 1 to 3) can be avoided by means of authentication, authorization, and confidentiality.
- Use of system by unauthorized users (i.e. risks 4 to 6) can be avoided by means of authentication, authorization, and confidentiality.

Table (4.10)**Required Security Services for Alpha**

Risks (refer to step7)	Security Services				
	Identification & Authentication	Authorization	Data Confidentiality	Data Integrity	Non- Repudiation
Risk1	X	X	X		
Risk2	X	X	X		
Risk3	X	X	X		
Risk4	X	X	X		
Risk5	X	X	X		
Risk6	X	X	X		
Risk7		X		X	
Risk8				X	

- User errors (i.e. risk7) can be avoided by means of authorization, and data integrity.
- Technical software failures (i.e. risk8) can be avoided by means of data integrity.

Step9: Security Services to Security Mechanisms Mapping

This step implements the previously identified security services by means of security mechanisms. In SecSDM methodology, ISO 7498-2 guidelines are adopted to define eight security mechanisms to achieve security services (i.e. encryption, digital signatures, access control mechanisms, data integrity mechanisms, authentication exchange, traffic padding, routing control, and notarization). However, in light of the fact that novel security mechanisms have emerged recently, we recommend the use of additional security mechanisms (e.g. steganography) to provide the necessary security services. Accordingly, we define a range of possible security mechanisms to each security service as below:

- Digital signatures, encryption, steganography, or authentication exchange can be implemented to enforce authentication.
- Access control mechanisms and restricted permissions can be implemented to enforce authorization.
- Encryption, steganography, traffic padding, or routing control can be implemented to enforce data confidentiality.
- Encryption, steganography, digital signatures, routing control, notarization, or other data integrity mechanisms can be implemented to enforce data integrity.

Step10: Security Services and Mechanisms Consolidation

Security services and mechanisms consolidation facilitate security implementation. It involves mapping security mechanisms to the suitable security services for each security risk, as determined in the preceding steps (see table 4.11). The numbers within the table represent the security risks, whereas the columns and rows represent the recommended security services and mechanisms respectively.

Table 4.11 can be summarized as follows:

- Risk1 and Risk6: To protect user account information against theft and disclosure by unauthorized access, a combination of authentication exchange, access control, encryption, and steganography will be implemented (i.e. biometric templates will be extracted, encrypted then hidden in user ID photos).
- Risk2 and Risk5: To protect payment information against theft and disclosure by unauthorized access, a combination of authentication exchange, access control, encryption, and steganography will be implemented (i.e. Credit card information will be encrypted then hidden in patient ID photos).

Table (4.11)

Required Security Mechanisms for Alpha

Security Mechanisms	Security Services																			
	Identification & Authentication				Authorization				Data Confidentiality				Data Integrity				Non-Repudiation			
Authentication Exchange	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8
Access Control Mechanisms	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8
Encryption	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8
Steganography	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8
Data Integrity Mechanisms	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8

- Risk3 and Risk4: To protect health information against theft and disclosure by unauthorized access, a combination of authentication exchange, access control, and encryption will be implemented. Steganography was not suggested here as a confidentiality mechanism due to the large amount of health information that makes it difficult to be hidden within patient photos which do not exceed 100 KB. Further, health information cannot be hidden in diagnostic images as they are not necessarily available for each patient.
- Risk7: To protect health information against accidental insertion of erroneous data, a combination of access control, data integrity mechanisms, and encryption will be implemented.
- Risk8: To protect scheduling information against technical errors, data integrity controls will be implemented.

Step11: Security Design Review

In the former design steps, we have defined a set of required security controls based upon risk assessment results and good practices. Here, we review our security design decisions by establishing an information security architecture for the healthcare system.

Table 4.11 conveyed the need for five key security mechanisms to reduce high-level risks, namely: Authentication mechanisms, access control, encryption, steganography, and data integrity mechanisms. Accordingly, we will utilize such mechanisms to develop an improved security architecture for Alpha. The proposed architecture will adopt the current good security practices of Alpha and implement further controls where necessary.

Thorn et al. (2008) define security architecture as “a cohesive security design, which addresses the requirements and the risks of a particular environment/scenario, and specifies what security controls are to be applied ...”. Accordingly, a security architecture must portray how the security mechanisms are positioned in relation to the overall IT architecture.

Based upon the preceding definition, the security architecture demonstrated in figure 4.4 is proposed. The architecture enforces a strict security framework on the healthcare information system. When a user attempts to access the system, a valid username/password combination must be provided. The system also includes a biometric sensor that detects the fingerprints of authorized users. If valid inputs were supplied (i.e. username, password, and fingerprint), the application server will show the appropriate user interface according to the job role and permissions of the user. When possible, the application will offer the users drop down menus to choose the desired input. Otherwise, user input is strictly validated for type, length, and format.

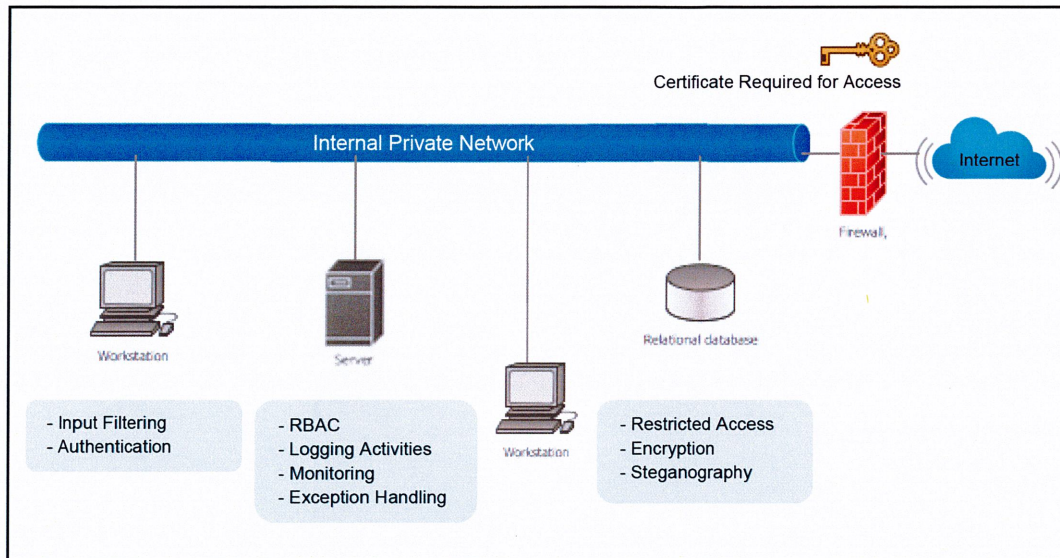


Figure (4.4)
The Proposed Information Security Architecture

The application server will monitor user actions by utilizing a security log that records any suspicious behavior. Further, the application will provide exception handling mechanisms to prevent system failures. The hospital datacenter will be secured using multiple mechanisms. The mechanisms were selected based on the previously conducted risk assessment. The design suggests that most valuable data should be secured using a combination of techniques. For instance, user biometric templates are encrypted then hidden in the bits of ID images.

As regards to network security, Alpha operates a private local network that is protected by firewalls and requires a valid certificate to be accessed by external entities.

The proposed security architecture implements the security services required to reduce high-level risks as detailed below:

- **Authentication:** The proposed authentication process builds on the current password-based authentication by incorporating biometrics-based authentication. Subsequently, instead of acquiring biometrics at access doors, user biometrics will be verified upon login.

- Authorization: Akin to the current system, role-based access control is utilized by the proposed system. Two key factors were considered while implementing RBAC, namely: Least privilege principle and segregation of duties.
- Data confidentiality: While the current architecture primarily uses encryption to secure confidential data, the proposed architecture employs steganography to protect sensitive information. To confirm higher data confidentiality, we integrate steganography with encryption when possible.
- Data Integrity: In the current system, data integrity is addressed by means of reviewing audit logs and implementing database integrity constraints. Nevertheless, most erroneous data occurrences in Alpha were caused by incorrect data entry. Thus, we support the current data integrity controls by enforcing strict input validation and raising staff awareness.

Further, we recommend establishing strict information security awareness programs to minimize risky employee behavior and enhance the effectiveness of the implemented security mechanisms.

Upon designing the new security architecture for Alpha using information hiding, the following question arises:

Can the proposed security system improve the security of Alpha's information system?

To seek an answer to such a question and evaluate the security of the proposed architecture, a risk assessment must be conducted. In order to assess the risk level of the proposed system, we will estimate the impact of the proposed architecture on the vulnerability level associated with each risk. If the proposed security system yields a lower vulnerability level as compared with the current system, the level of information risks will decrease resulting in improved security.

From what precedes, we believe that implementing the proposed security architecture will reduce the level of system vulnerability as indicated in table 4.12.

Table (4.12)

Vulnerability Assessment of the Proposed Security Architecture

Risks (refer to step4)	Vulnerability Level		
	Low	Medium	High
Risk1	X		
Risk2	X		
Risk3		X	
Risk4	X		
Risk5	X		
Risk6	X		
Risk7	X		
Risk8	X		

With reference to table 4.7, it is noted that the proposed security architecture has affected the risks assigned to a medium vulnerability level as follows:

- Risk1: Since the proposed architecture implements an additional layer of confidentiality through hiding the encrypted fingerprint templates into the employee image field, we declare user account information less exposed to the threat of theft.
- Risk2: Since the proposed architecture implements an additional layer of confidentiality through hiding the encrypted credit card numbers into the patient image field, we declare payment information less exposed to the threat of theft.
- Risk3: Since the proposed architecture does not implement steganography on encrypted health information, we declare it

partially exposed to theft. However, we believe that the proposed biometrics-based login procedure will reduce assets exposure to theft by unauthorized users.

- Risks 4 to 6: Since the proposed architecture suggests stricter authentication through requesting user biometrics in system login procedure, we declare critical information assets (i.e. health information, user account information, and payment information) less exposed to the threat of unauthorized access.

It is evident that the proposed security architecture has managed to reduce the vulnerability level associated with information risks, which in turn will contribute to decreasing the likelihood of threats. Accordingly, we conclude that the proposed security architecture will improve the overall security of Alpha's information system.

Step12: Multimedia Artifacts Development

Generally, the design phase involves constructing artifacts and models to achieve system requirements. However, security in MMISs may not be fully interpreted using conventional models; hence comes the necessity of multimedia artifacts development.

In multimedia artifacts development, customized artifacts are built to reflect security in multimedia systems. Such artifacts serve as powerful communication channels to those involved in the security process. Respectively, we extend the conceptual database model of Alpha to include security matters. Figure 4.5 represents the modified tables of the system's conceptual model where the use of steganography was emphasized.

The utilization of particular security mechanisms does not usually affect the conceptual model of the system. For instance, encrypting password fields does not impact the location of the original data field (i.e.

it maintains the same position at the database). However, steganography necessities hiding a database field within another; therefore, it is essential to establish a means to represent such occurrence.

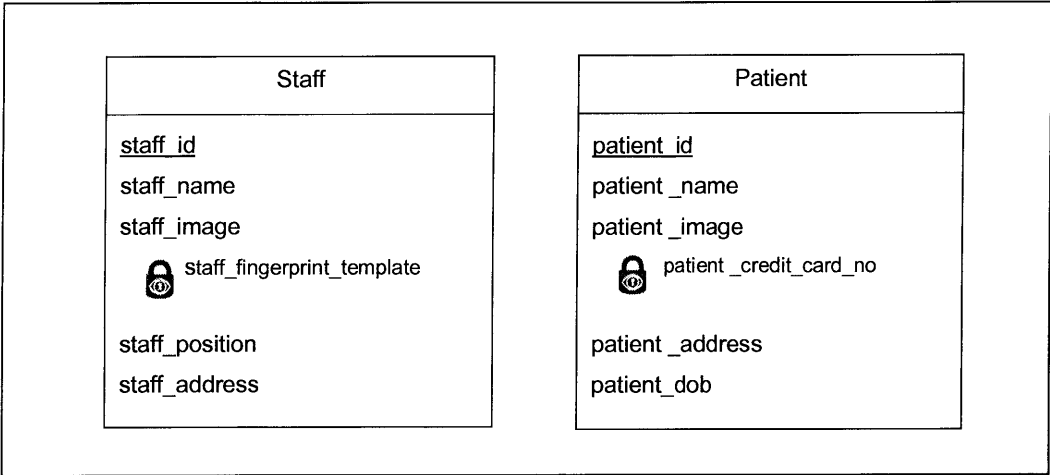


Figure (4.5)
Customized Conceptual Representation of Database Tables

Since no formal conceptual representation exists for steganography, we propose the eye-lock symbol () to denote steganography. Placing such symbol next to the attribute name indicates the existence of hidden fields, which are listed to the right of the symbol.

Step13: Impact and Trade-off Analysis

In the preceding steps, the key risks to the healthcare information system were identified along with the most suitable mechanisms to reduce them. Nonetheless, the unforeseen consequences of design decisions are often realized belatedly in system development, when they cost much higher to resolve.

Implementing security mechanisms in an inappropriate manner may introduce increasing overheads in terms of system performance as well as resource consumption. Security is interconnected with the reminder of non-functional requirements of the system. Hence, security engineering

must offer a means by which the potential impacts of security mechanisms can be estimated prior to implementation.

Impact and trade-off analysis is the process where diverse security variations are assessed prior to realization. By the end of such process, security engineers must be capable of selecting the most suitable approach to implement a desired security mechanism. Impact and trade-off analysis is particularly imperative in multimedia systems, due to the complex and heterogeneous nature of multimedia content that places additional demands on system resources.

with respect to the study scope, we will merely illustrate the process of impact and trade-off analysis in the context of steganography. Nevertheless, the process may be conducted in the same manner to estimate the impact of any security mechanism.

Multiple steganography algorithms exist with variant properties. However, choosing an algorithm which does not fit the security context of the system may introduce further issues to the organization. Thus, it is essential to evaluate the impact of the steganography algorithms across multiple dimensions, hence establishing confidence in the security choices (see table 4.13).

In accordance with the literature, there is no available steganography technique that is entirely capable of satisfying all non-functional requirements of information systems. Hence, a trade-off among such requirements must be achieved depending upon the system priorities. Table 4.13 attempts to evaluate some of the dominant image steganography techniques based on the following factors:

- Image quality: The quality of the stego-image after embedding the secret data, determined by PSNR.
- Payload capacity: The total number of bits that can be hidden within a given cover image.

Table (4.13)
Impact and Trade-Off Analysis for Steganography Algorithms

Algorithm	Quality	Capacity	Robustness	Invisibility	Speed	Complexity	File Size	Format	Applicability
LSB	Medium	High	Low	Low	Low	Low	High	Dependent	Systems that require hiding large amounts of information with lower security and computational power
PVD	Medium	Medium	Low	Low	Low	Low	High	Dependent	Systems with lower level of security and computational power
Patchwork	Medium	Low	High	High	Low	High	Low	Independent	Systems that require hiding a small amount of highly sensitive information
SSIS	Medium	Medium	Medium	High	Medium	Medium	Low	Independent	System that transmit stego-images over noisy channels, since it is highly robust against statistical attacks
DCT	High	Medium	Medium	High	Medium	Medium	Low	Dependent	Systems that require high quality stego-images with lower file size
DFT	Low	Medium	Medium	High	High	Medium	Low	Independent	Systems that require high speed information hiding and extraction, where the quality of the stego-image is not a priority
DWT	Low	Medium	High	High	Medium	High	Low	Independent	Systems with high computational power that require hiding highly sensitive information, where the quality of the stego-image is not a priority
IWT	Low	Medium	High	High	Medium	High	Low	Independent	

- **Robustness:** The ability of the embedded data to remain intact if the stego-image undergoes transformations.
- **Perceptual invisibility:** The extent to which the embedded data remains unnoticed.
- **Processing speed:** The amount of time required for embedding and extracting the secret data.
- **Complexity:** The computational complexity of the utilized algorithm.
- **File size:** The relative size of the stego-image after data embedding.
- **File format:** The extent to which a given steganography technique is dependent upon specific image formats.

The values assigned to each algorithm are based upon reviewing the literature including the studies to follow: (Amirtharajan et al., 2010), (Goel et al., 2013), (Hussain & Hussain, 2013), (Mazumder & Hemachandran, 2013), (Saejung et al., 2013), (Sharma, 2013), (Dagar & Dagar, 2014), (Desai et al., 2014), and (Tiwari et al., 2014).

In accordance with the literature, DCT algorithm was found best suited for our application as it achieves the key non-functional requirements of Alpha, namely: accuracy (high quality stego-files), storage utilization (low file size), and processing time (average speed).

4.4.3 Implementation Phase

In this phase, the selected security mechanisms and algorithms are implemented through suitable software components. Nonetheless, in line with the scope of this thesis, the emphasis of this section will be centered on the implementation of steganography.

Step14: Software Security Components Definition

The software development tools provided by the .Net framework were employed in this study. This is mainly due to fact that the .Net framework offers a wide verity of tools and guidelines to write secure applications. Code access security, role-based security, and cryptography models are few examples of the security services provided to developers by the .Net framework.

At this stage, Futchter and von Solms (2007) recommend constructing an implementation priority list to estimate the priority of the mechanisms to be implemented and ultimately guarantee that the proper security features are utilized. In accordance with table 4.11, authentication, authorization, and confidentiality mechanisms are at the forefront of our implementation priority list.

To exemplify security components definition, we will discuss the process of user authentication. Implementing user authentication requires two distinct components, namely user registration and user verification:

- User registration:

Figure 4.6 outlines the process of user registration. Upon registering new users, a fingerprint reader is utilized to capture fingerprint images. Then, SourceAFIS (Vazan, 2009) is employed to generate fingerprint templates. SourceAFIS is an automated fingerprint identification system that authenticate users via fingerprint recognition. Template extraction is followed by Lempel–Ziv–Welch (LZW) compression, where the template data is reduced in size. LZW compression is performed to enlarge the hiding capacity of JPEG compressed images, where redundancy is very limited. The compressed data is then encrypted using a private key. Subsequently, the encrypted data is embedded within employee ID photos via partial JPEG decoding. The resultant stego-image is ultimately stored in Alpha’s database along with the reminder of employee records.

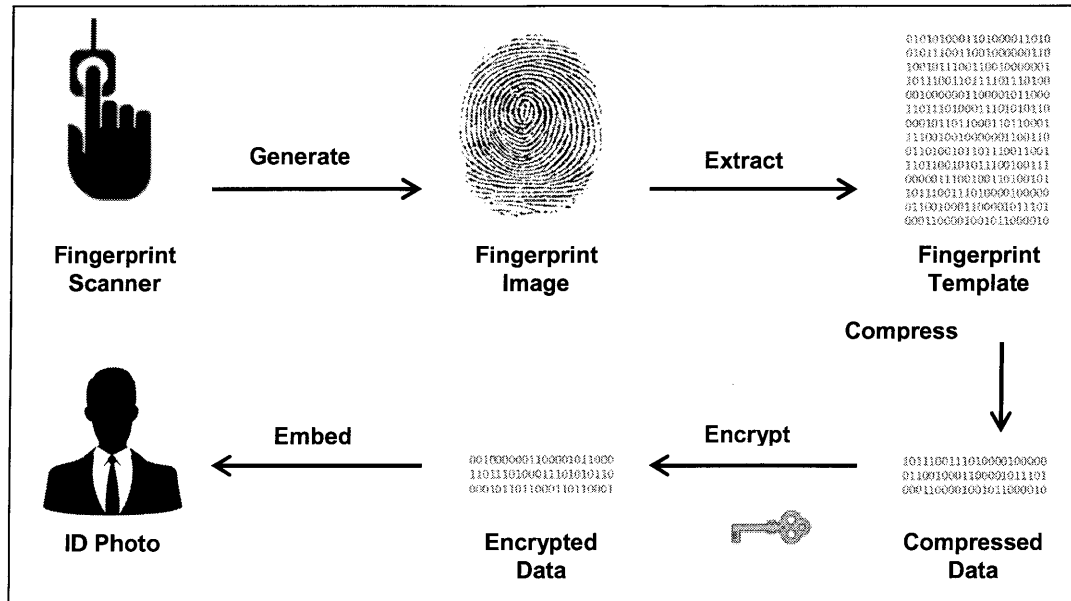


Figure (4.6)

The Proposed User Registration Process

- User verification:

Figure 4.7 outlines the process of user verification (authentication). When a user attempt to access the system, he/she is first required to provide a correct username/password combination. Then, the user's fingerprint is scanned and followed by the process of template extraction. The extracted fingerprint template is compared against the stored template associated with the given username. However, since the stored template is concealed within the ID photo, it is extracted, decrypted, and decompressed prior to template matching. If the two templates match, the user is allowed to access the system according to his/her job role.

Our implemented steganography approach is based upon the work of (Reddy et al., 2011), where the confidential data files are compressed and encrypted prior to concealment within the cover image.

By the end of security components definition, the developer must make certain that all security code is comprehensible, testable, and maintainable.

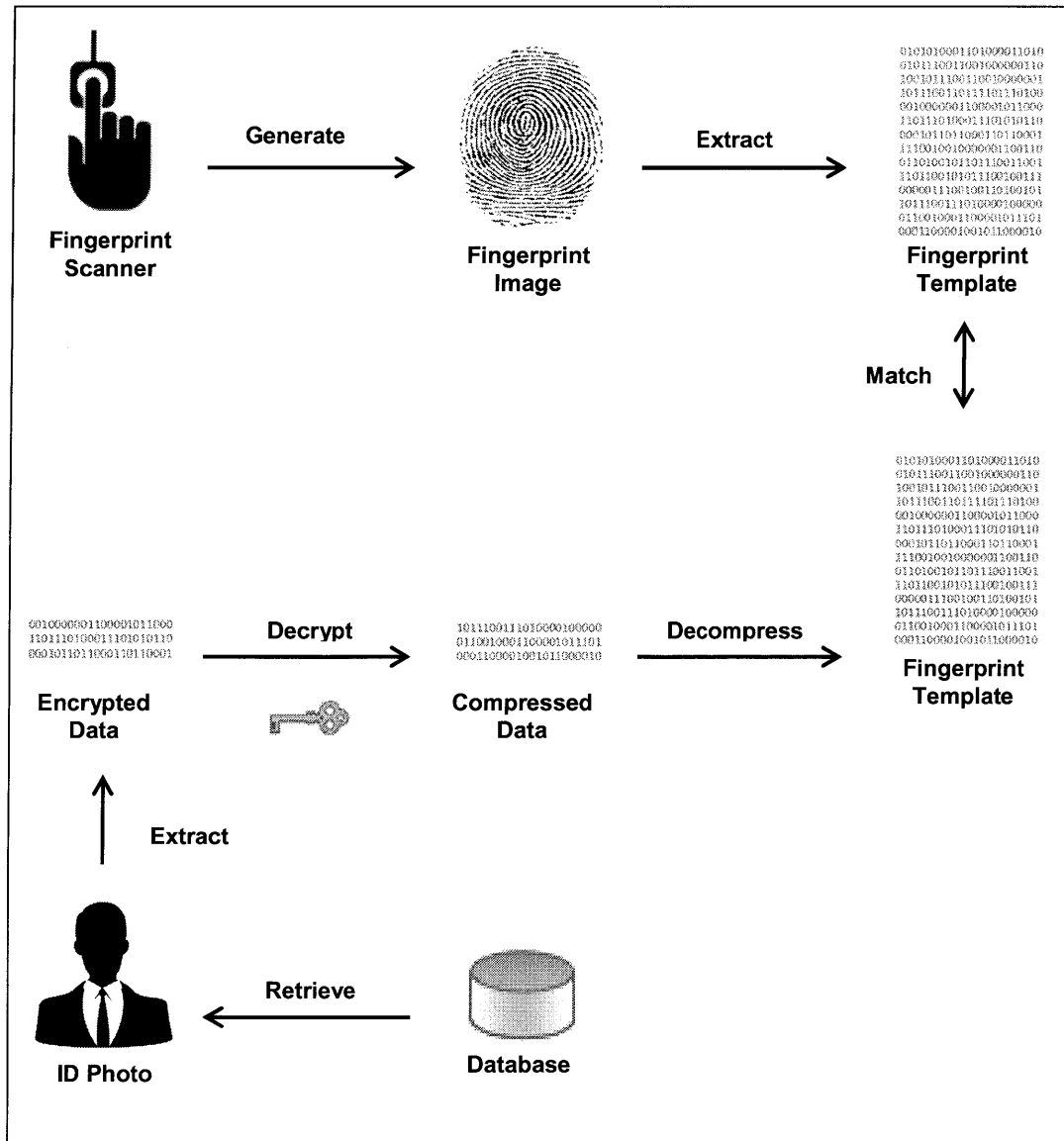


Figure (4.7)
The Proposed User Verification Process

Implemented Steganography Algorithm

One of the fundamental features of steganography is that it uses redundant bits to hide information. Thus, one might assume it is not applicable to JPEG images since JPEG lossy compression might cause the loss of embedded data. Nevertheless, researchers have benefited from the features of JPEG encoding to develop JPEG steganographic algorithms. In fact, JPEG encoding is divided into two phases: lossy and

lossless. Thus, information hiding can take place after the lossy phase (Morkel et al., 2005).

To further comprehend JPEG steganography, one must understand the process of JPEG encoding. JPEG image encoding entails six major stages, namely: Color space transformation, down-sampling, block splitting, discrete cosine transform, quantization, and entropy coding (Saab et al., 2012).

The initial three stages serve as transform-preparation stages, where an image is first converted to YCbCr color space (i.e. Y represents pixel brightness, Cb and Cr represent pixel chrominance), then its chrominance components are reduced to enable compression, and each image channel is divided into 8x8 blocks. In the discrete cosine transform stage, each block is converted to its transform-domain representation. The Quantization stage represents the lossy stage in JPEG encoding, it involves dividing each transformed block by a constant determined by JPEG quantization table then rounding the result to the nearest integer. Entropy coding is the last stage in JPEG encoding; it involves arranging block coefficients in a zigzag order. Then, run-length encoding algorithm is applied followed by Huffman coding.

The utilized steganography technique is known as “Partial DCT Decoding” (Reddy et al., 2011), it hides the confidential data within the DCT coefficients of JPEG images. The partial decoding algorithm uses the final phase of JPEG encoding (i.e. entropy coding) to insert data in such a manner that doesn’t considerably affect the original image both in terms of size and quality. The algorithm implements steganography by decoding the original JPEG image to 8x8 blocks, embedding secret data into the blocks, and writing the altered block back using entropy coding.

The implemented partial decoding technique merely modifies the AC coefficients in JPEG blocks; this is mainly due to the fact that any

modification to the DC coefficients significantly impacts the quality of the image. The JPEG standard assigns a Huffman code and a category value to each AC coefficient. Accordingly, data is embedded within the cover image by modifying the LSB of the Huffman code of the AC coefficients. All AC coefficients in matching categories occupy an identical amount of bits. Thus, in order to maintain the size of the cover image, an AC coefficient is modified in such a manner that preserves its category. Following the embedding of secret data, the block is subjected to entropy coding and all the modified blocks are written to the stego-image file.

4.4.4 Testing Phase

Since we were unable to deploy the system on the target environment, we implemented and tested the system locally using the configuration to follow:

- The VB.NET integrated development environment within the Microsoft Visual Studio Express 2012 was utilized to implement the application.
- The database was implemented using the Microsoft SQL Server 2012.
- The system was run under Windows7 development platform.

Step15: Security Performance Evaluation

In this step we shall examine the impact of the implemented security system on overall system performance. However, in accordance with the scope of this thesis, the performance evaluation will be approached with the emphasis on the steganographic sub-systems.

With respect to data collection findings, security, accuracy, efficiency (i.e. time behavior and storage utilization), and usability were

declared the most critical quality attributes to Alpha. Hence, only these quality attributes will be examined here.

Several experiments have been conducted to examine the performance of the proposed security system. Four datasets were mainly utilized in our experiments, namely: Patient, employee, Fingerprint, and Credit Card Numbers datasets. Both Patient and Employee datasets contain ten standard 200×250 JPEG images with different properties, and were used as cover media. Further, the Fingerprint dataset comprises ten 240×320 TIF images with equal file size of 75 KB and diverse features, which were used as secret data. Lastly, the Credit Card Numbers dataset contains ten randomly generated card numbers with 16 digits each.

For each evaluation criterion, two distinct sets of experiments were performed. While the first set involves hiding financial data (i.e. credit card numbers) in patient images, the other set concerns hiding fingerprints templates in employee images. Tables 4.14 and 4.15 outline the obtained results.

Table (4.14)
Patient Dataset Experimental Results

IMAGE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
File Size (KB)	59.2	55.2	51.4	50.8	57.4	63	43.4	49.4	55.0	47.7
Enc. Time (ms)	88	76	89	93	96	99	68	82	88	81
Dec. Time (ms)	70	68	71	75	77	83	60	70	74	70
MSE	0.0200	0.0317	0.0283	0.0194	0.0188	0.0317	0.0225	0.0191	0.0237	0.0174
PSNR (dB)	65.5076	64.4018	64.0976	65.2620	65.3807	63.5780	64.9355	65.6808	64.6688	65.7660

Table (4.15)**Employee Dataset Experimental Results**

IMAGE	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
File Size (KB)	57.0	41.9	53.6	45.1	53.2	55.7	58.7	57.2	52.8	56.4
Enc. Time (ms)	255	240	253	254	244	245	252	241	237	248
Dec. Time (ms)	88	80	84	81	82	83	84	79	80	83
MSE	0.0734	0.0799	0.1367	0.0657	0.0634	0.0746	0.1025	0.0600	0.0752	0.0860
PSNR (dB)	59.8155	59.1252	57.2594	59.9785	60.1842	59.7819	58.3083	60.3809	59.7643	58.9261

A. Accuracy

In order to measure the impact of the utilized steganographic mechanism of on data accuracy, the accuracy of hidden data and stego-medium were measured.

The accuracy of hidden data was estimated by embedding different sets of data within images, the extracted data were found identical to the embedded data at all attempts.

The accuracy of a stego-medium is strictly associated with the imperceptibility of steganography. Numerous metrics can be employed to measure the imperceptibility of steganography. However, all imperceptibility metrics share the common purpose of determining the degree of similarity between the cover and the stego-medium. In accordance with the literature, four primary metrics will be used to measure imperceptibility as follows:

- Subjective Quality Evaluation (Visual Inspection)

The majority of objective image quality evaluations do not entirely reflect the perception of humans. Thus, a subjective quality evaluation is required as a genuine benchmark for image steganography (Stoica et al., 2003).

The subjective evaluation is based upon the visual examination of an image by independent assessors. Subjective quality evaluations are built upon the fact that the majority of steganographic techniques tend to distort the cover medium to a certain extent. An evaluator is advised to look for multimedia content inconsistencies. In case of digital images, evaluators typically seek grainy structures, lack of continuity in colors, lack of texture, and subtle distortions of any sort (Bailey & Curran, 2006).

In this study, ten independent assessors were asked to differentiate cover and stego-images. Despite their fair knowledge of image processing, the assessors did not have exhaustive knowledge of steganography. The assessors were provided with brief explanation of steganography and distortion classes, they were then asked to identify the stego-images among a diverse range of images. The provided images were analogous in terms of content, size, and lighting. Nine out of ten assessors were unable to identify the stego-image. Hence, we declare our steganographic system subjectively accurate.

- Mean Square Error (MSE)

The mean square error refers to the square of the difference between the pixels sharing the same position in the carrier image and the stego-image respectively, divided by image size (Garg & Jangra, 2014). In steganographic systems, MSE measure is used to quantify the variation between the initial and the resultant images. MSE is mathematically calculated using the following formula:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x_{ij} - y_{ij})^2$$

Where M and N represent the number of rows and columns of the image respectively, x represents the cover image, and y represents the stego-image.

Lower values of MSE are preferable, as they indicate lesser error in the stego-image (i.e. better image quality).

The image quality level of the stego-images with regard to cover images was quantitatively evaluated via Image Compressor image processing tool (Image Compressor, 2008). Tables 4.14 and 4.15 demonstrate MSE values for both experiment sets. While the first experiment set had an average MSE of 0.02326, the second set had an average of 0.08174. We believe that such increase in error ratio is caused by the increased amount of payload in the second set.

- Peak Signal to Noise Ratio (PSNR)

The peak signal to noise ratio is a measure to estimate the quality of the stego-medium as opposed to the cover medium. PSNR is mathematically derived from MSE, and can be calculated in decibels (dB) using the following formula:

$$\text{PSNR} = 10 \log_{10} \left(\frac{\text{MAX}^2}{\text{MSE}} \right)$$

Where MAX is the maximum pixel value and MSE is the mean square error.

The mathematical equation declares PSNR inversely proportional to MSE, which implies that lower MSE values yield higher PSNR. Hence, higher PSNR values are preferable, as they indicate lesser error in the stego- image (i.e. better image quality).

The first experiment set accomplished higher stego-image quality with an average PSNR of 64.92788 dB. As might be expected, the second set scored lower PSNR values with an average of 59.35243 dB (see tables 4.14 and 4.15). However, both values have managed to far exceed the minimum acceptable image PSNR value of 30 dB (Gupta et al, 2013).

- Histogram Analysis

An image histogram is a graphical representation of the tonal distribution in digital images (Krutsch & Tenorio, 2011). Histogram analysis is a powerful tool in image steganography as inspecting the histogram of an image offers an insight into image statistical features. Histogram analysis can detect image distortions that are declared undetectable by the human visual system. Thus, a major goal of steganography techniques is to minimize the differences in the stego-image histogram as opposed to the cover image.

Since our steganographic system operates in the transform domain of an image, embedding data within the cover image will yield minimal histogram changes that are barely discernible. Figure 4.8 Confirms such statement as it demonstrates the histogram of two images (i.e. one of each experiment set) prior to and following the process of data embedding. It is evident that pixel distortions were negligible as the difference in mean intensity for both cases did not exceed 0.002. From such minimum differences in image histograms, it is difficult to infer the existence of secret data.

B. Time Behavior

Time is a significant factor for efficiency assessment. In our study, processing time will be evaluated with respect to embedding and extraction operations. To calculate the processing time, time was measured in milliseconds for both encoding and decoding processes.

Table 4.14 indicates the processing time of the first set of experiments. With an average encoding time of 86 milliseconds, encoding periods fluctuated from 99 to 68 milliseconds. Decoding process however required less time in all cases, with an average decoding time of 71.8 milliseconds.

In contrast, table 4.15 indicates the processing time of the second set of experiments. Due to the fact that fingerprint template extraction is a

part of the proposed steganographic framework, template extraction time was included in the embedding time measurement. Therefore, it is evident that the second experiment set achieved higher embedding time with an average of 246.9 milliseconds. However, since this process is carried out once for each new user at account creation, such time costs can be tolerated. In addition, average decoding time for the second set was 82.4 milliseconds with a slight increase of 10 milliseconds compared to the first set. We believe that the higher amount of payload in the second experiment set have contributed to such increase.

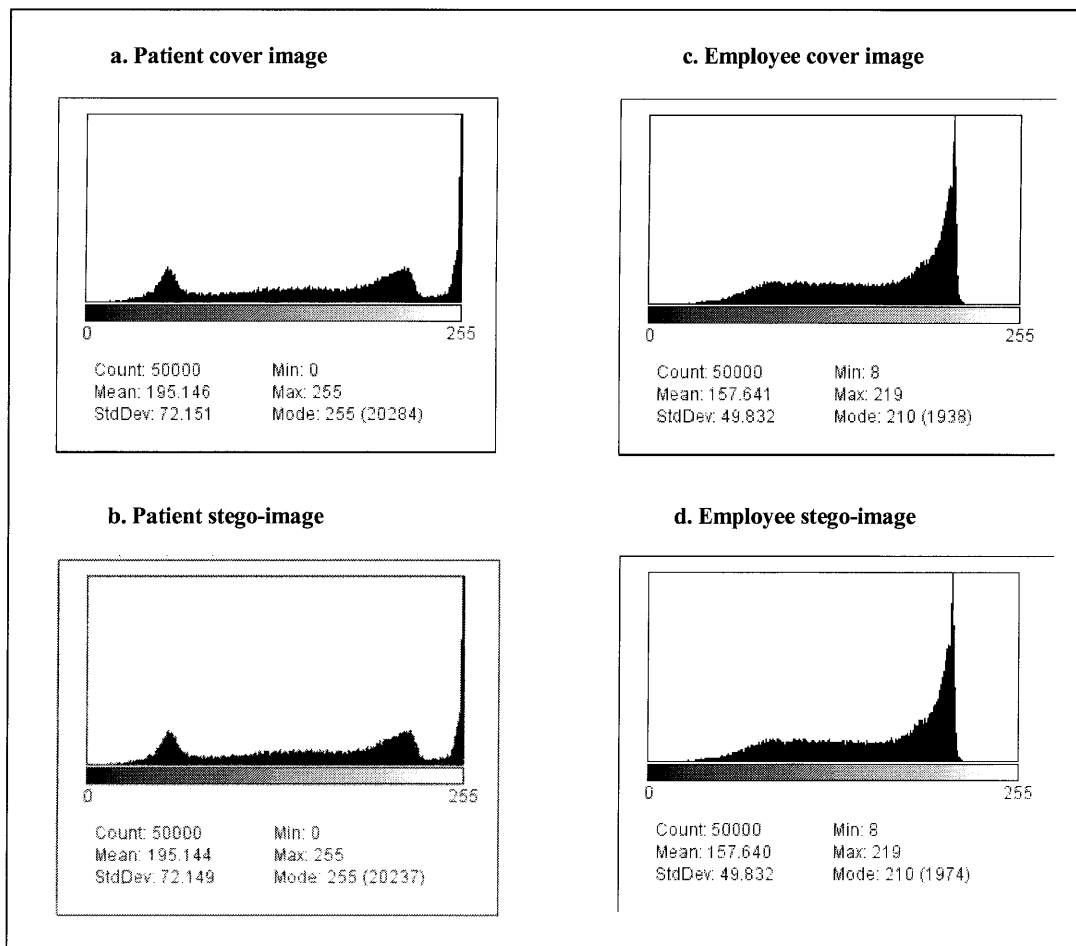


Figure (4.8)
Cover and Stego-Images Histograms

Bearing in mind the encoding and decoding periods of both experiment sets, we believe that the processing time for the proposed

system is acceptable and manages to meet the requirements of the concerned institute.

C. Storage Utilization

Storage space is a major concern for information systems especially those associated with multimedia content. Broadly speaking, embedding secret data within certain carriers may introduce large overhead and unacceptable redundancy. As a result, it is curtail to assess stego-objects in terms of file size.

The implemented steganographic process excels in terms of resource utilization. It stores both the confidential data and the cover media within a single file (i.e. stego-file) that is equivalent in size to the original cover media. As a result, steganography yields less overall storage space as compared to Alpha's current system.

D. Usability

In information systems, increased security may translate to decreased usability. Enforcing security may place heavy demands on system users. However, in accordance with Alpha's current system, the proposed security system requires the same user input (i.e. no additional user actions were needed to enforce steganographic controls). To exemplify, both systems require user IDs, passwords, and biometrics to access. Further, usability factors (i.e. ease of learning, efficiency of use, memorability, error frequency, and user satisfaction) were strongly considered while designing the user interface.

4.5 Summary

In the context of this chapter, we utilized the multimedia security engineering process introduced in the previous chapter to develop a security system for a healthcare information system.

Based on the security assessment of the current healthcare information system, we developed a security architecture to address the security needs of the system.

We believe that implementing the proposed architecture will improve the overall security of the information system by decreasing the vulnerability level associated with major risks, which in turn will reduce the level of risks associated with the current system.

Further, the security evaluation results have proven the effectiveness of the proposed security system. For the given datasets, the obtained results were promising in terms of accuracy, processing time, storage utilization, and usability.

Chapter Five: Conclusion and Future Work

5.1 Conclusion

5.2 Future Work

Chapter Five: Conclusion and Future Work

This chapter represents the conclusion of this study. In the context of this chapter, an overview of the study findings is presented first, followed by recommendations for future research directions.

5.1 Conclusion

This study was conducted to investigate the means by which information hiding may improve MMISs security. The broad theoretical literature on information hiding primarily emphasizes the security of multimedia content. Hence, the study sought to propose a systematic approach for the development of secure MMISs using information hiding.

The main empirical findings of the study are synthesized to answer the research questions and draw further conclusions as follows:

As indicated by the literature, there exist various security techniques to address the different security requirements of MMISs. However, apart from information hiding, there is no other security technique to exploit the unique features of multimedia content to achieve further security. The voluminous amount of heterogonous data stored in MMISs render the use of traditional security techniques rather inefficient. Thus, we recommend the use of information hiding in conjunction with other security techniques to achieve elevated MMISs security.

Given that the proposed security system yields a lower risk level as compared with the current system, the case study findings support the contention that information hiding can improve the security of MMISs.

The results of the risk assessment confirmed that information hiding utilization has largely contributed to minimizing high-level risks; nonetheless, a systematic approach must be followed through each phase of SDLC to ensure optimal utilization of information hiding. Therefore,

we have introduced and implemented an MMIS security engineering framework.

Cryptography and steganography are two major contributors to MMISs security. They share the common purpose of protecting the confidentiality of information. Despite the resemblance in their goals and services, both mechanisms have different qualities to offer:

- Whereas cryptography is the art of hiding the meaning of a message, steganography is concerned with hiding the very existence of a secret message. Thus, the principal advantage of steganography as opposed to cryptography is that the secret message does not stand out as worthy of examination. Perceptible enciphered messages, on the other hand, raise suspicion and may require further efforts to ensure unbreakable security.
- In order to conceal secret data, steganography requires a carrier medium. Consequently, if a particular steganography technique was able to hide the secret data within the carrier medium while maintaining the original carrier size (e.g. partial DCT decoding), then such technique is declared storage efficient.
- Given that steganography utilizes redundancy in cover media to conceal secret data, steganographic capacity is proportional to the size of the cover medium. Thus, to obtain favorable results, it is advised to conceal relatively small amounts of data using steganography (i.e. as compared to cryptography).
- Steganography and cryptography are evaluated in different manners. Cryptographic systems are considered broken when the attacker is able to comprehend the meaning of the secret message. On the contrary, steganographic systems fail when the attacker is able to detect the presence of the secret message.

- Several nations place strong restrictions on the use of cryptography (Saper, 2013); Hence comes the need for alternatives. When cryptography is outlawed, steganography can evade such regulations to communicate messages secretly.

From what precedes, it is evident that cryptography and steganography are complementary mechanisms, whereas choosing the most fitting mechanism is an application specific problem (i.e. the application requirements will direct the developer preferences).

However, to conquer the shortcomings of both mechanisms and add further layers of security, it is a good practice to combine cryptography and steganography into a single framework. The combination of such mechanisms will enhance the overall security of embedded data. To illustrate further, if an attacker were to defeat the steganographic system by detecting the existence of the secret message, he would still need to decipher the message to be able to access its content.

Information hiding provides multiple security services that are targeted to meet the security requirements of a system. The queries arising are whether the provided security introduces considerable performance overhead that overshadows the benefits for the system, and how to optimize performance once information hiding has been considered.

Prior to estimating the impact of information hiding on system performance, one must identify the non-functional requirements of the system (i.e. system quality characteristics). Upon their identification, the quality characteristics must be prioritized in accordance with their relevance to key business objectives.

The impact of information hiding on the quality characteristics of MMISs is dependent upon the utilized algorithm. As per the literature, there is no information hiding algorithm to satisfy all the quality

characteristics of MMISs. Thus, we propose the process of impact and trade-off analysis to assist in selecting the most appropriate algorithm for a given set of quality characteristics. To validate the results suggested by the impact and trade-off analysis process, performance testing must be conducted with particular emphasis on the required quality characteristics.

In the course of the case study we declared partial DCT steganography most suitable with respect to the required quality characteristics. To confirm our choice, we evaluated the steganographic sub-system against the quality characteristics to flow: Accuracy, performance, and usability. Evaluation results have proven the superior performance of the proposed steganographic sub-system.

5.2 Future Work

Several directions for future research arise in light of what precedes. Investigating the following as future research areas shall contribute to MMISs security:

- The proposed security system should be further deployed and evaluated in real life environment. Experiments conducted in this study involved a system prototype. Despite the positive experimental results, additional aspects might be revealed in real environment. Hence, we recommend accommodating the security system to real environments as an area for future research.
- Identifying the key features of steganographic techniques lacks standardization. The performance of a particular technique is estimated by comparing the values of its key features with those of other techniques. Nonetheless, steganographic techniques may excel in some features and fail in others. Thus, as a future research direction, we recommend the utilization of decision making

algorithms to elect the best fitting technique for a given situation (i.e. based on each steganography feature).

- The current state of research indicates a lack of standardization in terms of measuring the impact of steganography against information systems quality attributes. Hence, we recommend developing metrics to calculate the effect of steganography on the quality attributes post to implementation.

References

- AbdulLatef, A. (2011). Color image steganography based on discrete wavelet and discrete cosine transforms. *Ibn Al-Haitham journal for pure and applied science*, 24(3), 296-302.
- Amirtharajan, R., Akila, R., & Deepikachowdavarapu, P. (2010). A comparative analysis of image steganography. *International journal of computer applications*, 2(3), 41-47.
- Bailey, K., & Curran, K. (2006). An evaluation of image based steganography methods. *Multimedia tools and applications*, 30(1), 55-88. doi: 10.1007/s11042-006-0047-x
- Barry, C., & Lang, M. (2001). A survey of multimedia and web development techniques and methodology usage. *IEEE multimedia*, 8(2), 52-60. doi: 10.1109/93.917971
- Barry, C., & Lang, M. (2003). A comparison of 'traditional' and multimedia information systems development practices. *Information and Software Technology*, 45(4), 217-227. doi: 10.1016/S0950-5849(02)00207-0
- Bertoa, M. F., Troya, J. M., & Vallecillo, A. (July). *A survey on the quality information provided by software component vendors*. Paper presented at the 7th ECOOP workshop on quantitative approaches in object-oriented software engineering, Darmstadt, Germany. Retrieved from <http://www.lcc.uma.es/~av/Publicaciones/03/QAOOSE2003.pdf>
- Beznosov, K. (2003). *Extreme security engineering: On employing XP practices to achieve 'good enough security' without defining it*.

- Paper presented at the First ACM workshop on business driven security engineering, Fairfax, VA. Retrieved from <http://137.82.84.194/record/43/files/43.pdf>
- Blackledge, J., Al-Rawi, A., & Tobin, P. (2013). *Stegacryption of DICOM metadata*. Paper presented at the Irish signals & systems conference 2014 and 2014 china-ireland international conference on information and communications technologies, Limerick, Ireland. doi: 10.1049/cp.2014.0703
- Cabot, J., & Zannone, N. (2008). *Towards an integrated framework for model-driven security engineering*. Paper presented at the Workshop on modeling security, Toalose, France. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.142.8468&rep=rep1&type=pdf>
- Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, 90(3), 727-752. doi:10.1016/j.sigpro.2009.08.010
- Dagar, E., & Dagar, S. (2014). Comparative study of various steganography techniques. *International journal of emerging engineering research and technology*, 2(2), 30-36.
- Dalvi, I., & Patil, N. (2014). Color image steganography based on DWT and SWT. *International journal of research in electronics and communication technology*, 1(3), 78-80.
- Davenport, H. (2013). *Implementation and evaluation of security protocols in e-commerce applications* (Master's thesis, Victoria University of Wellington, Wellington, New Zealand). Retrieved

from

<http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/2631/thesis.pdf>

De Win, B., Scandariato, R., Buyens, K., Grégoire, J., & Joosen, W. (2009). On the secure software development process: CLASP, SDL and Touchpoints compared. *Information and software technology*, 51(7), 1152-1171. doi: 10.1016/j.infsof.2008.01.010

Desai, J., Hemalatha, S., & Shishira, S. R. (2014). Comparison between DCT and DWT steganography algorithms. *International journal of advanced information science and technology*, 24(24), 51-55.

Flechais, I., Mascolo, C., & Sasse, M. A. (2007). Integrating security and usability into the requirements and design process. *International journal of electronic security and digital forensics*, 1(1), 12-26. doi: 10.1504/IJESDF.2007.013589

Futcher, L., & von Solms, R. (2007). SecSDM: a model for integrating security into the software development life cycle. In L. Futcher, & R. Dodge (Eds.), *Fifth world conference on information security education*, 41-48. Boston: Springer US.

Futcher, L., & von Solms, R. (2013). A risk-based approach to formalise information security requirements for software development. In R. Dodge, & L. Futcher (Eds.), *Information assurance and security education and training*, 257-264. Berlin, Germany: Springer Berlin Heidelberg.

Garg, M., & Jangra, A. G. (2014). An overview of different type of data hiding scheme in image using steganographic

- techniques. *International journal of advanced research in computer science and software engineering*, 4(1), 746-751.
- Ghasemi, E., Shanbehzadeh, J., & Fassihi, N. (2011). *High capacity image steganography using wavelet transform and genetic algorithm*. Paper presented at the International multiconference of engineers and computer scientists, Hong Kong, China. Retrieved from http://www.iaeng.org/publication/IMECS2011/IMECS2011_pp495-498.pdf
- Global data privacy [directory]. (2014). Retrieved from <http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf>
- Goel, S., Kumar, P., & Saraswat, R. (2014). High capacity image steganography method using LZW, IWT and modified pixel indicator. *International journal of computer science and information technologies*, 5(3), 3759-3763.
- Goel, S., Rana, A., & Kaur, M. (2013). Comparison of image steganography techniques. *International journal of computers and distributed systems*, 3(1), 20-30.
- Govinda, K., Abburu, P. K., & Reddy, G. P. (2013). On-demand secure streaming of multimedia data over cloud. *International journal of engineering & technology*, 5(3), 2101-2107.
- Gupta, H., Kumar, R., & Changlani, S. (2013). Enhanced data hiding capacity using LSB-based image steganography method. *International journal of emerging technology and advanced engineering*, 3(6), 212-214.

- Hansen, E. T. (2007). *Analysis of the singular value decomposition in data hiding* (Doctoral dissertation, Iowa State University). Retrieved from <http://orion.math.iastate.edu/dept/thesisarchive/MSCC/HansenEMSSS07.pdf>
- Hansson, J., Feiler, P. H., & Morley, J. (2008). Building secure systems using model-based engineering and architectural models. *CrossTalk: The journal of defense software engineering*, 21(9), 1-14.
- Hatebur, D., Heisel, M., & Schmidt, H. (2006). Security engineering using problem frames. In G. Müller (Ed.), *Emerging trends in information and communication security*, 238-253. Freiburg, Germany: Springer Berlin Heidelberg.
- Hong, W., Chen, T. S., & Shiu, C. W. (2008). Lossless steganography for AMBTC-compressed images. In D. Li, & G. Deng (Eds.), *Image and signal processing*, 13-17. Los Alamitos, CA: IEEE.
- Howard, M., & Lipner, S. (2006). *The security development lifecycle*. Redmond, WA: Microsoft Press.
- Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. *International Journal of advanced science & technology*, 54, 113-124.
- Image Compressor (Version 6.8.0.5) [Computer software]. (2008). Retrieved from <http://www.image-compressor.com>
- INTOSAI EDP Audit Committee. (1995). *Information system security review methodology: a guide for reviewing information system*

- security in government organizations*. Retrieved from http://www.issai.org/media/13024/issai_5310_e.pdf
- Kaur, A., & Sardana, N. (2013). A novel image steganography (NIS) technique. *International journal of engineering and computer science*, 2(8), 2533-2535.
- Kim, Y. G., & Cha, S. (2012). Security engineering methodology for developing secure enterprise information systems: An overview. In J. J. J. H. Park, Y. S. Jeong, S. O. Park, & H. C. Chen (Eds.), *Embedded and multimedia computing technology and service*, 393-400. Dordrecht, Netherlands: Springer Netherlands.
- Kouns, J., & Minoli, D. (2011). *Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams*. Hoboken, NJ: John Wiley & Sons.
- Kumar, L. (2012). Novel security scheme for image steganography using cryptography technique. *International journal of advanced research in computer science and software engineering*, 2(4), 143-146.
- Krutsch, R., & Tenorio, D. (2011). *Histogram equalization*. Retrieved from: http://cache.freescale.com/files/dsp/doc/app_note/AN4318.pdf
- Lian, S., Kanellopoulos, D., & Ruffo, G. (2009). Recent advances in multimedia information system security. *Informatica*, 33(1), 3-24.
- Lin, W. S., Zhao, H. V., & Liu, K. R. (2006). *Scalable multimedia fingerprinting forensics with side information*. Paper presented at

IEEE international conference on image processing, Atlanta, GA.
doi: 10.1109/ICIP.2006.312833

Markotten, D. G. (2002). *User-centered security engineering*. Paper presented at the 4th EurOpen/USENIX conference, Helsinki, Finland. Retrieved from <http://isy1.isy.vcu.edu/~mthomas/info750/UserCenteredSecurityEngineering.pdf>

Mazumder, J. A., & Hemachandran, K. (2013). Study of Image steganography using LSB, DFT and DWT. *International journal of computers & technology*, 11(5), 2618-2627.

Memon, A. G., Khawaja, S., & Shah, A. (2008). Steganography: A new horizon for safe communication through XML. *Journal of theoretical and applied information technology*, 4(3), 187-202.

Moradian, E. (2012). *Integrating security in software engineering process: The CSEP methodology* (Doctoral thesis, KTH Royal Institute of Technology, Stockholm, Sweden). Retrieved from <http://www.diva-portal.org/smash/get/diva2:528069/FULLTEXT01.pdf>

Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). *An overview of image steganography*. Paper presented at the Fifth annual information security South Africa conference, Sandton, South Africa. Retrieved from <http://mo.co.za/open/stegoverview.pdf>

Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2014). A novel image steganographic approach for hiding text in color images using HSI color model. *Middle-East journal of scientific research*, 22(5), 647-654.

- Muttoo, S. K., & Kumar, S. (2009). Data hiding in JPEG images. *International journal of information technology*, 1(1), 13-16.
- O'docherty, M. H., & Daskalakis, C. N. (1991). Multimedia information systems—the management and semantic retrieval of all electronic data types. *The computer journal*, 34(3), 225-238.
- Ojha, V., Sharma, N., Sharma, A., & Jain, S. (2011). Information processing for multimedia e-learning systems. *International journal of science and advanced technology*, 1(2), 98-102.
- Phad Vitthal, S., Bhosale Rajkumar, S., & Panhalkar Archana, R. (2012). A novel security scheme for secret data using cryptography and steganography. *IJ computer network and information security*, 4(2), 36-42.
- Provos, N., & Honeyman, P. (2002). *Detecting steganographic content on the internet*. Paper presented at the Network and distributed system security symposium, San Diego, CA. Retrieved from <http://www.w.honeyman.org/u/provos/papers/detecting.pdf>
- Reddy, V. L., Subramanyam, A., & Reddy, P. C. (2011). *Steganpeg steganography+ jpeg*. Paper presented at the Ubiquitous computing and multimedia applications international conference, Daejeon, South Korea. doi: 10.1109/UCMA.2011.17
- Rednic, E., & Toma, A. (2009). Security management in a multimedia system. *Journal of applied quantitative methods*, 4(2), 37-47.
- Rowley, J. (2002). Using case studies in research. *Management research news*, 25(1), 16-27. doi: 10.1108/01409170210782990

- Saab, F., Elhajj, I. H., Chehab, A., & Kayssi, A. (2012). *Energy efficient JPEG using stochastic processing*. Paper presented at the Energy aware computing international conference, Guzelyurt, Cyprus. doi: 10.1109/ICEAC.2012.6471025
- Saejung, S., Boondee, A., Preechasuk, J., & Chantrapornchai, C. (2013). *On the comparison of digital image steganography algorithm based on DCT and wavelet*. Paper presented at the Computer science and engineering conference, Nakorn Pathom, Thailand. doi:10.1109/ICSEC.2013.6694803
- Saper, N. (2013). International cryptography regulation and the global information economy. *Northwestern journal of technology and intellectual property*, 11(7), 673-688.
- Sapino, M. L., & Candan, K. S. (2008). Multimedia information systems. In B. Furht (Ed.), *Encyclopedia of multimedia*, 554-562. New York: Springer US.
- Sarker, M. Z. H., & Parvez, M. S. (2005). *A Cost effective symmetric key cryptographic algorithm for small amount of data*. Paper presented at IEEE 9th International Multitopic Conference, Karachi, Pakistan. doi:10.1109/INMIC.2005.334435
- Schell, C. (1992). *The value of the case study as a research strategy*. Retrieved from <http://www.finance-mba.com/Case%20Method.pdf>
- Sharma, A. (2013). *Comparative study of image steganography in image and transform domain*. Paper presented at the 2nd International conference on role of technology in nation building, Meerut, India. Retrieved from <http://sitesubharti.org/mobile/icrtnb/pdf/ICRTNB-44.pdf>

- Sheisi, H., Mesgarian, J., & Rahmani, M. (2012). Steganography: DCT coefficient replacement method and compare with JSteg algorithm. *International journal of computer and electrical engineering*, 4(4), 458-462. doi: 10.7763/IJCEE.2012.V4.533
- Singh, I., Khullar, S., & Laroia, D. S. (2013). DFT based image enhancement and steganography. *International journal of computer science and communication engineering*, 2(1), 5-7.
- Sodiya, A. S., Onashoga, S. A., & Ajayi, O. B. (2006). Towards building secure software systems. *Issues in informing science and information technology*, 3, 635-646.
- Stoica, A., Vertan, C., & Fernandez-Maloigne, C. (2003). *Objective and subjective color image quality evaluation for JPEG 2000 compressed images*. Paper presented at the Signals, circuits and systems international symposium, Iasi, Romania. doi:10.1109/SCS.2003.1226967
- Sun, S. W., Lu, C. S., & Chang, P. C. (2007). *Joint multimedia fingerprinting and encryption: Security issues and some solutions*. Paper presented at IEEE international conference on multimedia and expo, Beijing, China. doi:10.1109/ICME.2007.4284954
- Sundaram, A. (1996). An introduction to intrusion detection. *ACM crossroads*, 2(4), 3-7. doi: 10.1145/332159.332161
- Susanto, H., & Muhaya, F. B. (2010). *Multimedia information security architecture framework*. Paper presented at the Future information technology 5th international conference, Busan, South Korea. doi: 10.1109/FUTURETECH.2010.5482696

- Thorn, A., Christen, T., Gruber, B., Portman, R., & Ruf, L. (2008). What is a security architecture. *Information security society switzerland*, 6, 1-6.
- Thuraisingham, B. (2007). Security and privacy for multimedia database management systems. *Multimedia tools and applications*, 33(1), 13-29. doi: 10.1007/s11042-006-0096-1
- Tiwari, A., Yadav, S. R., & Mittal, N. K. (2014). A Review on different image steganography techniques. *International journal of engineering and innovative technology*, 3(7), 121-124.
- Uludag, U., & Jain, A. K. (2003). *Multimedia content protection via biometrics-based encryption*. Paper presented at ICME'03 international conference on multimedia and expo, Baltimore, MD. doi:10.1109/ICME.2003.1221292
- Vazan, R. (2009). *Source AFIS| fingerprint recognition library for .NET and experimentally for Java*. Retrieved from: <http://sourceforge.net/projects/sourceafis>
- Venkateswaran Radhakrishnan, D., & Venkatachalam, S. (2011). Novel information security model using proposed e-cipher method with combining the features of cryptic-steganography. *International journal of computer science issues*, 8(5), 443-449.
- Younis, R. M. (2011). *Modern advances in software and solution algorithms for reservoir simulation* (Doctoral dissertation, Stanford University). Retrieved from https://stacks.stanford.edu/file/druid:fb287kz3299/RMY_PHD_THESIS-augmented.pdf

Zhao, N., Chen, M., Chen, S. C., & Shyu, M. L. (2008). *MRBAC: Hierarchical role management and security access control for distributed multimedia systems*. Paper presented at IEEE international symposium on object oriented real-time distributed computing, Orlando, FL. doi:10.1109/ISORC.2008.41

Appendix 1: Interviews – Alpha Case Study

This appendix will describe the process of data collection through interviews. The aim of such interviews is to investigate the information requirements and infrastructure of Alpha healthcare institute in order to develop a security system that will achieve its security objectives. The interviews were semi-structured, whereas an interview guide was followed to direct the topics of discussion. The interviews were held between April and May 2015.

A. Semi-structured Interview Questions (Interview Guide)

Section1: Functional Requirements

- What types of functions are introduced by the information system?

Section2: Non-Functional Requirements

Quality issues

- What are the most important quality attributes that must be offered by the system?

Usability

- What type of users will be using the system?
- What sort of training will be required for users?

Performance

- Are there any speed, or response time constraints on the system?
- Are there size or capacity constraints on the data to be processed by the system?

Security Issues

- Must access to any data or the system itself be controlled?

- Is physical security an issue?
- What are the main requirements of confidentiality, integrity, and availability?

Section3: Multimedia Requirements

- What types of media are utilized by the system?
- Are there any restrictions on the media files (e.g. size, format, etc)?
- What types of hardware and software resources are used to manage media, and what are their characteristics?

Section4: Information Architecture

- What type of network architecture is used to manage information?

Note: Further follow-up questions were asked, as appropriate.

B. Interviews Findings

Based on information collected through interviews, this section will describe Alpha's information system in terms of requirements, infrastructure, and data models.

B.1 System Requirements

This section aims to fully describe the high-level requirements of Alpha. It highlights Alpha's functional and non-functional requirements obtained through data collection.

B.1.1 Functional Requirements

Functional requirements represent the core behavior intended by the system. Figure 1 and figure 2 demonstrate the functional requirements of the system.

User Registration

SRS001 Add users

The system shall allow administrators to add new users to the system.

SRS002 Assign permission

The system shall allow administrators to assign permissions to each user based upon his/her job role.

Users Termination

SRS003 Delete users

The system shall allow administrators to delete users from the system when they no longer work for Alpha.

Patient Registration

SRS004 Add patient

The system shall allow patient records staff to add new patients to the system.

Patient Search

SRS005 Search for patient

The system shall allow patient records staff and doctors to search for patients using patient ID.

Modifying Patient Information

SRS006 Edit contact information

The system shall allow patient records staff to edit patient contact information when necessary.

SRS007 Add patient to doctor's list

The system shall allow patient records staff to add patients to doctor's list.

SRS008 Add diagnosis

The system shall allow physicians to add patient diagnosis to the system.

SRS009 Add test results

The system shall allow lab technicians to add test results to the system.

SRS010 Add payment information

The system shall allow patient records staff to add patients payment information.

Figure (1)

Functional Requirements Specification

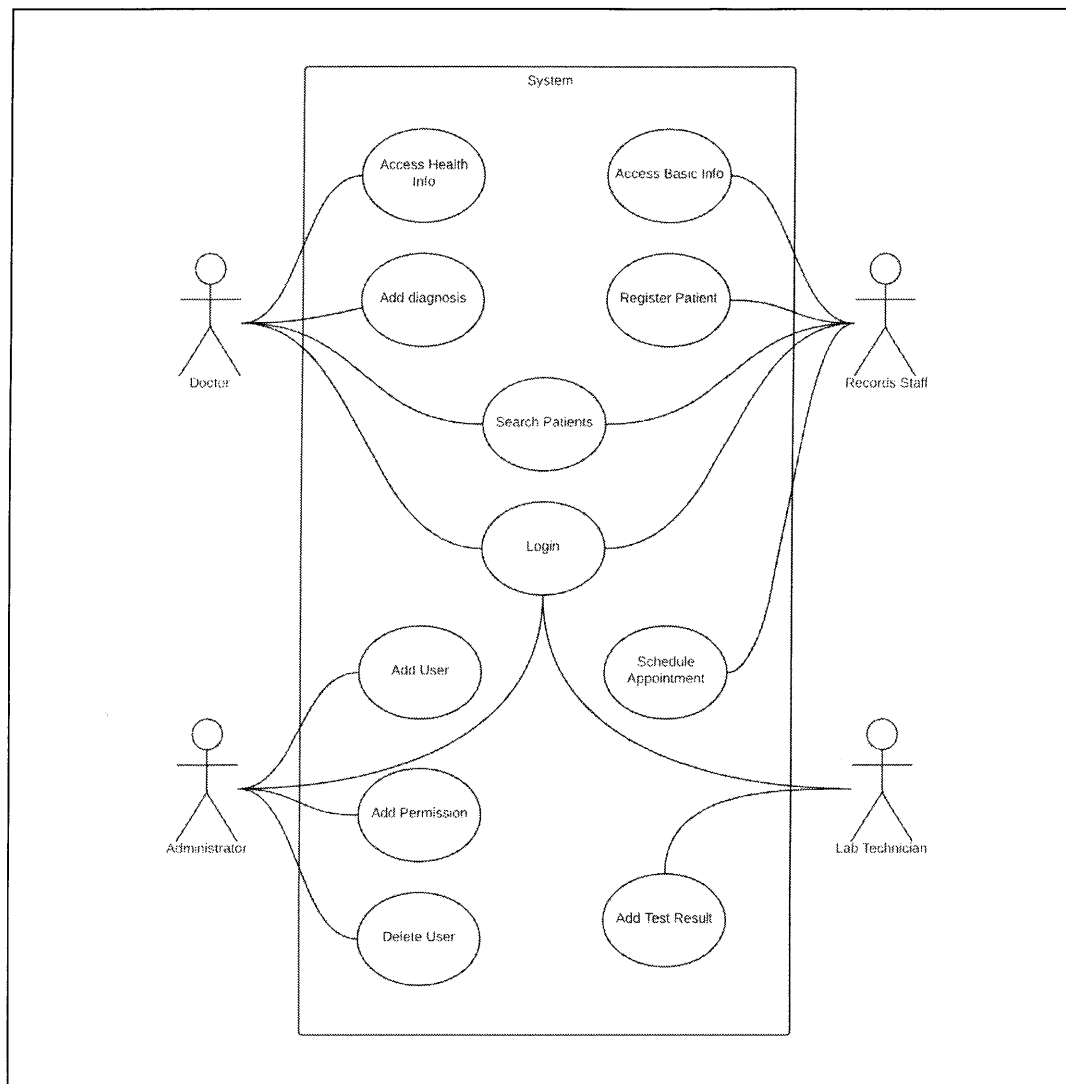


Figure (2)
System Use-Case Diagram

B.1.2 Non-Functional Requirements

Non-functional requirements represent the quality attributes of the system. In the course of the interviews, five major non-functional requirements were stressed as follows:

- **Security:** Given that patient records are confidential, only authorized personnel can gain access to the system. System authorization is role-based where administrators are responsible for granting and modifying user permissions.

- Data accuracy: Accurate data support the delivery of quality services. Thus, data accuracy was emphasized as inaccurate records will translate to poor service.
- Time behavior: Alpha policies grant physicians a limited time period for patient examination and diagnosis. Therefore, minimizing the user-system interaction time will facilitate better service delivery.
- Storage utilization: Alpha stores thousands of patient records that include full medical history in different media forms. Hence, Alpha considers utilizing storage space an essential concern.
- Usability: Usability means making automated tasks simpler, faster, and more convenient. Usability is an important quality as Alpha requires system users to learn basic system operations within one day of use.

B.2 Information Infrastructure

Figure 3 demonstrates the current IT infrastructure of the target system. It is represented by a client/server architecture interconnected through a private network. A database server connection is established to obtain information.

B.3 Data Model

Figure 4 presents the main entities and relations of the healthcare information system.

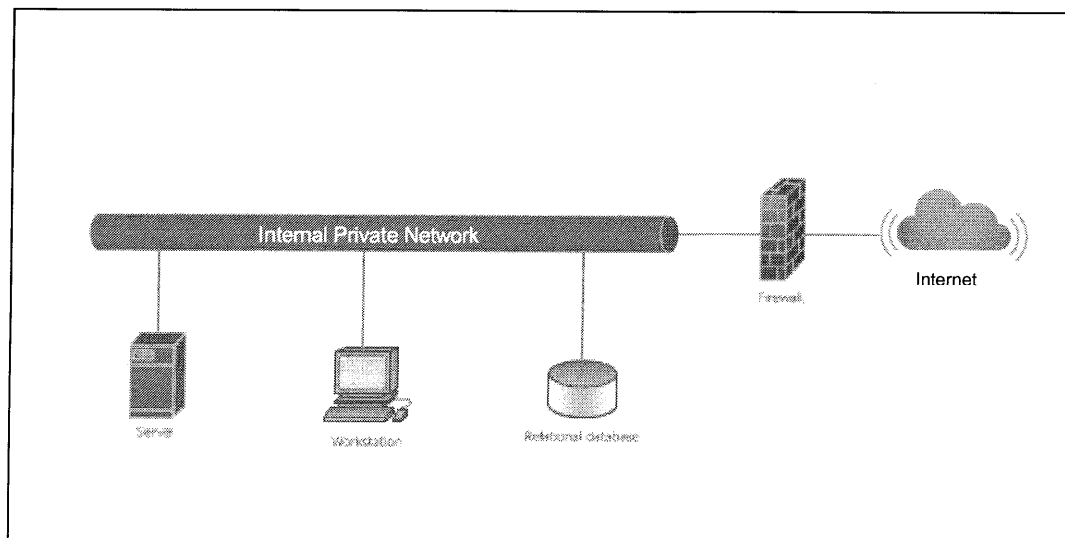


Figure (3)
System Information Infrastructure

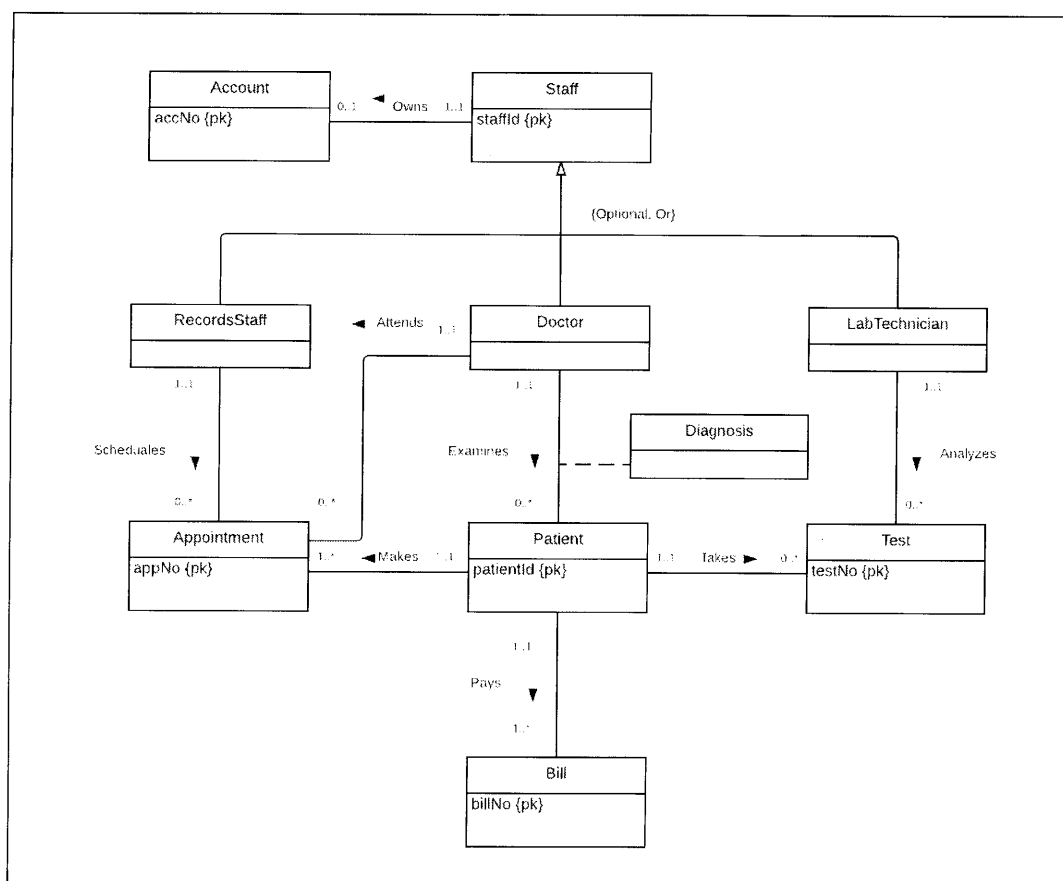


Figure (4)
System Entity-Relation Diagram

ملخص الأطروحة

أصبحت الحاجة إلى حماية أنظمة الوسائط المتعددة في وقتنا الحاضر أشد منها في أي وقت مضى، حيث أن تطبيقات الوسائط المتعددة صارت تمثل جزءاً لا يتجزأ من حياتنا اليومية. ولهذا تهدف هذه الأطروحة إلى دراسة استخدام تقنية إخفاء المعلومات لحماية أنظمة الوسائط المتعددة.

تبدأ الدراسة باستعراض تقنيات أمن المعلومات الحالية المستخدمة لحماية أنظمة الوسائط المتعددة، ثم تطرح إطاراً للهندسة الأمنية يهدف إلى دمج أنشطة أمن المعلومات مع أنظمة الوسائط المتعددة بشكل كلي.

كذلك تقوم الدراسة بتفعيل الإطار المقترح لتصميم وتنفيذ نظام أمني لحماية أنظمة الوسائط المتعددة باستخدام تقنية إخفاء المعلومات. هذا وقد أجريت دراسة حالة لتقييم أمن أحد أنظمة المعلومات الصحية ومن ثم إيضاح استخدام الإطار الهندسي المقترح لخفض مستوى الخطر المعلوماتي. ثم تقوم الدراسة بتقييم أداء النظام الأمني المقترح وذلك من حيث تأثيره على الخصائص النوعية لنظام المعلومات الصحية.

لقد توصلت نتائج الدراسة إلى إمكانية خفض مستوى الخطر المعلوماتي بتطبيق النظام الأمني المقترح. لذا فإن الدراسة تدعم الفرضية القائلة بأن تقنية إخفاء المعلومات يمكن أن تساهم بشكل كبير في تحسين أمن أنظمة الوسائط المتعددة. كما تبين نتائج تقييم الأداء تفوق للنظام الأمني المقترح من حيث الدقة والسرعة واستغلال وحدات التخزين وسهولة الاستخدام. ومع ذلك، تؤكد الدراسة أهمية إتباع أسلوب منهجي خلال كل مرحلة من مراحل تطوير نظام الوسائط المتعددة لضمان الاستخدام الأمثل لتقنية إخفاء المعلومات.

جامعة البحرين

كلية تقنية المعلومات



تطوير نظام أمني لأنظمة الوسائط المتعددة باستخدام إخفاء المعلومات

أطروحة مقدمة كجزء من متطلبات الحصول على درجة الماجستير

في تقنية المعلومات

إعداد

أمل حسن الصقر

الرقم الجامعي: 20114862

إشراف

د. وسن شاكر عواد

(أستاذ مشارك)

جامعة البحرين

مملكة البحرين

ديسمبر 2015