



# **Secure Digital Documents Using Steganography and QR Code**

**A thesis submitted for the degree of Doctor of Philosophy**

**By**

**Mohamed Sameh Hassanein**

**Department of Computer Science,**

**Brunel University**

**November 2014**

## **ABSTRACT**

With the increasing use of the Internet several problems have arisen regarding the processing of electronic documents. These include content filtering, content retrieval/search. Moreover, document security has taken a centre stage including copyright protection, broadcast monitoring etc. There is an acute need of an effective tool which can find the identity, location and the time when the document was created so that it can be determined whether or not the contents of the document were tampered with after creation. Owing the sensitivity of the large amounts of data which is processed on a daily basis, verifying the authenticity and integrity of a document is more important now than it ever was. Unsurprisingly document authenticity verification has become the centre of attention in the world of research.

Consequently, this research is concerned with creating a tool which deals with the above problem. This research proposes the use of a Quick Response Code as a message carrier for Text Key-print. The Text Key-print is a novel method which employs the basic element of the language (i.e. Characters of the alphabet) in order to achieve authenticity of electronic documents through the transformation of its physical structure into a logical structured relationship. The resultant dimensional matrix is then converted into a binary stream and encapsulated with a serial number or URL inside a Quick response Code (QR code) to form a digital fingerprint mark. For hiding a QR code, two image steganography techniques were developed based upon the spatial and the transform domains. In the spatial domain, three methods were proposed and implemented based on the least significant bit insertion technique and the use of pseudorandom number generator to scatter the message into a set of arbitrary pixels. These methods utilise the three colour channels in the images based on the RGB model based in order to embed one, two or three bits per the eight bit channel which results in three different hiding capacities. The second technique is an adaptive approach in transforming domain where a threshold value is calculated under a predefined location for embedding in order to identify the embedding strength of the embedding technique.

The quality of the generated stego images was evaluated using both objective (PSNR) and Subjective (DSCQS) methods to ensure the reliability of our proposed methods. The experimental results revealed that PSNR is not a strong indicator of the perceived stego image quality, but not a bad interpreter also of the actual quality of stego images. Since the visual difference between the cover and the stego image must be absolutely imperceptible to the human visual system, it was logically convenient to ask human observers with different qualifications and experience in the field of image processing to evaluate the perceived quality of the cover and the stego image. Thus, the subjective responses were analysed using statistical measurements to describe the distribution of the scores given by the assessors. Thus, the proposed scheme presents an alternative approach to protect digital documents rather than the traditional techniques of digital signature and watermarking.

## **ACKNOWLEDGEMENTS**

I would like to take this opportunity extend my hearty gratitude to the aid and support of the kind people around me to accomplish this thesis in time. First and foremost, I am grateful to my supervisor, Dr George Ghinea, who has offered me invaluable support and guidance throughout my Ph.D. with his knowledge and patience.

This thesis would not have been possible without the support of my family. I owe my sincerest gratitude to my family for their endless support, for which my mere expression of thanks does not suffice.

Last, by no means least, I wish to offer my heartfelt thanks and gratitude to all my fellow colleagues, the academic and support staff in the Department of Computer Science at Brunel University. I am grateful to all of those with whom I have had the pleasure to work during the course of my PH.D.

## **DECLARATION**

The following papers have been published (or submitted for publication) as a direct result of the research discussed in this thesis:

Hassanein, M. S., & Ghinea, G., 2012. Text fingerprint key generation. In *Internet Technology And Secured Transactions, IEEE 2012 International Conference*, pp. 603-609.

## ABBREVIATIONS

<b>1D</b>	One Dimensional
<b>2D</b>	Bi-dimensional
<b>AC</b>	Alternate Current
<b>ANOVA</b>	Analysis of Variance
<b>BMP</b>	Bitmap Format
<b>DC</b>	Direct Current
<b>DCT</b>	Discrete Cosine Transforms
<b>DFT</b>	Discrete Fourier Transforms
<b>DSCQS</b>	Double Stimulus Continuous Quality Scale
<b>DSIS</b>	Double Stimulus Impairment Scale
<b>DSR</b>	Design Science Research
<b>DWT</b>	Discrete Wavelet Transforms
<b>EAN</b>	International Article Number
<b>ENMPP</b>	Expected Number of Modifications per Pixel
<b>FH</b>	High Frequency
<b>FL</b>	Low Frequency
<b>FM</b>	Middle Frequency
<b>GIF</b>	Graphics Interchange Format
<b>HVS</b>	Human Visual System
<b>JPEG</b>	Joint Photographic Experts Group
<b>L.C.A</b>	Letter Count After
<b>L.C.B</b>	Letter Count Before
<b>LSB</b>	Least Significant Bits
<b>MOS</b>	Mean Opinion Scores
<b>MPD</b>	Multi-Pixel Differencing
<b>MSE</b>	Mean Squared Error
<b>NLP</b>	Natural Language Processing
<b>OCR</b>	Optical Character Recognition

<b>OPAP</b>	Optimal Pixel Adjustment Process
<b>PNG</b>	Portable Network Graphics
<b>PRNG</b>	Pseudorandom Number Generator
<b>PSNR</b>	Peak Signal-to-Noise Ratio
<b>PVD</b>	Pixel Value Differencing
<b>QR Code</b>	Quick Response Code
<b>QT</b>	Quantisation Table
<b>RGB</b>	Red, Green and Blue
<b>SSCQE</b>	Single Stimulus Continuous Quality Evaluation
<b>T.L.I</b>	Total letter Index
<b>UID</b>	Unique Identification
<b>UPC</b>	Universal Product Code

# TABLE OF CONTENTS

ABSTRACT .....	i
ACKNOWLEDGEMENTS.....	iii
DECLARATION .....	iv
ABBREVIATIONS .....	v
TABLE OF CONTENTS .....	vii
LIST OF TABLES.....	xiii
LIST OF FIGURES .....	xv
<b>Chapter 1: Information Hiding and Steganography .....</b>	<b>1</b>
1.1    OVERVIEW .....	1
1.2    RESEARCH BACKGROUND .....	2
1.2.1 <i>Steganography and Cryptography</i> .....	3
1.2.2 <i>Steganography and Watermarking</i> .....	4
1.2.3 <i>Steganography and Fingerprinting</i> .....	4
1.3    RESEARCH MOTIVATIONS .....	6
1.4    RESEARCH AIM AND OBJECTIVES .....	8
1.5    RESEARCH APPROACH .....	9
1.6    THESIS STRUCTURE .....	10
<b>Chapter 2: Nuts and Bolts of Steganography .....</b>	<b>11</b>
2.1    OVERVIEW .....	11
2.2    STEGANOGRAPHY DEFINED.....	13
2.3    TAXONOMY OF INFORMATION HIDING TECHNIQUES .....	15
2.3.1 <i>Hiding Method-Based Classification</i> .....	15
2.3.1.1 Insertion-Based Method: .....	15
2.3.1.2 Substitution-Based Method: .....	15



2.3.1.3	Generation-Based Method.....	16
2.3.1.4	Transform Domain Technique.....	16
2.3.1.5	Spread Spectrum Technique.....	16
2.3.1.6	Statistical Technique.....	17
2.3.1.7	Distortion Technique.....	17
2.3.2	<i>Cover-Type Based Classification</i> .....	18
2.4	TEXT WATERMARKING.....	19
2.4.1	<i>Format Based Methods</i> .....	20
2.4.1.1	Line-shift encoding.....	20
2.4.1.2	Word-shift encoding.....	20
2.4.1.3	Feature encoding.....	21
2.4.1.4	White-space encoding.....	24
2.4.2	<i>Linguistic Methods</i> .....	24
2.4.2.1	Syntactic Method.....	24
2.4.2.2	Semantic Method.....	25
2.5	IMAGE STEGANOGRAPHY.....	27
2.5.1	<i>Background on Digital Image</i> .....	27
2.5.2	<i>Spatial Domain</i> .....	29
2.5.3	<i>Transform Domain</i> .....	32
2.5.4	<i>Adaptive Steganography</i> .....	36
2.6	IMAGE QUALITY EVALUATION.....	38
2.6.1	<i>Objective Quality Evaluation</i> .....	39
2.6.2	<i>Subjective Evaluation Method Key Concepts</i> .....	40
2.6.3	<i>Subjective Evaluation Related Work</i> .....	43
2.7	STEGANOGRAPHIC SYSTEMS EVALUATION.....	45

2.7.1	<i>Security or Imperceptibility</i> .....	45
2.7.2	<i>Payload Capacity</i> .....	46
2.7.3	<i>Robustness</i> .....	46
2.8	STEGANALYSIS.....	47
2.8.1	<i>Passive Warden</i> .....	48
2.8.2	<i>Active Warden</i> .....	48
2.8.3	<i>Malicious Warden</i> .....	49
2.9	BARCODE.....	49
2.9.1	<i>Two dimensional (2D) barcodes</i> .....	50
2.9.2	<i>QR Code</i> .....	52
2.9.3	<i>Related Work For Using QR code in Information Hiding</i> .....	54
2.10	SUMMARY.....	55
<b>Chapter 3: Research Design and Proposed Framework .....</b>		<b>56</b>
3.1	OVERVIEW .....	56
3.2	DESIGN SCIENCE RESEARCH .....	57
3.3	DESIGN SCIENCE RESEARCH METHODOLOGY .....	59
3.3.1	<i>Awareness of Problem</i> .....	60
3.3.2	<i>Suggestion</i> .....	61
3.3.3	<i>Development</i> .....	63
3.3.4	<i>Evaluation</i> .....	66
3.4	CONCLUSION.....	76

<b>Chapter 4: Document Key-Print and QR-Code Generation .....</b>	<b>77</b>
4.1 INTRODUCTION.....	77
4.2 ARCHITECTURE OF TEXT-BASED DOCUMENTS .....	78
4.3 DOCUMENT KEY-PRINT ALGORITHM.....	79
4.4 PROPOSE SYSTEM VERIFICATION AGAINST “CUT AND PASTE” ATTACKS	83
4.4.1 Scenario (1): Bob lends Alice money.....	85
4.4.2 Scenario (2): Alice lends Alex money. ....	91
4.5 FINGERPRINT GENERATION.....	96
4.6 CONCLUSION.....	98
<b>Chapter 5: Robust QR-Code Image Steganography .....</b>	<b>99</b>
5.1 OVERVIEW .....	99
5.2 IMAGE STEGANOGRAPHY .....	99
5.3 SPATIAL DOMAIN METHOD.....	102
5.3.1 Data Embedding Procedure.....	103
5.3.2 Data Extraction Procedure.....	105
5.4 ADAPTIVE TRANSFORM DOMAIN METHOD .....	106
5.4.1 Phase One: Choose the Locations .....	107
5.4.2 Phase Two: Identify the Embedding Strength.....	108
5.4.3 Phase three: Embedding and Extracting .....	110
5.5 METHODS EVALUATION RESULTS.....	113
5.5.1 Payload Capacity.....	114

5.5.2	<i>Imperceptibility</i> .....	118
5.5.3	<i>Robustness</i> .....	122
5.6	CONCLUSION.....	124
<b>Chapter 6: Subjective Performance Evaluation.....</b>		<b>126</b>
6.1	OBJECTIVE EVALUATION METRICS .....	126
6.2	OVERVIEW .....	127
6.3	EXPERIMENT RESULTS .....	128
6.3.1	<i>Spatial Method (3bit)</i> .....	128
6.3.2	<i>Spatial Method (6bit)</i> .....	132
6.3.3	<i>Spatial Method (9bit)</i> .....	135
6.3.4	<i>Transform Domain Method CH(1)</i> .....	138
6.3.5	<i>Transform Domain Method CH(2)</i> .....	142
6.4	SUMMARY OF EXPERIMENT RESULTS.....	145
6.5	CONCLUSION.....	147
<b>Chapter 7: Conclusions .....</b>		<b>149</b>
7.1	OVERVIEW .....	149
7.2	THESIS OVERVIEW .....	150
7.3	RESEARCH FINDINGS.....	153
7.4	RESEARCH CONTRIBUTION.....	158
7.4.1	<i>Proposed Text Key-print Fingerprinting Method</i> .....	158
7.4.2	<i>Increasing Payload Capacity While Maintaining Imperceptibility..</i>	159

7.4.3 <i>Proved PSNR Unreliability for Stego Images</i> .....	159
7.5 RESEARCH LIMITATIONS AND FUTURE WORK.....	161
<b>References</b> .....	<b>162</b>

## LIST OF TABLES

Table 1-1: Summary of the Difference between Watermarking, Fingerprinting, and Steganography .....	6
Table 2-1: Steganography Technique Categories .....	17
Table 2-2: Arabic and Persian Letters Dots .....	21
Table 2-3: List of words with different spelling in UK and US (M. Shirali-Shahreza, 2008).....	25
Table 2-4: Grade Quality and Impairment Scale .....	40
Table 2-5: Four Widely Known 2D Barcodes .....	50
Table 2-6: Main QR Code Specification.....	53
Table 3-1: Five-Grade Quality .....	73
Table 4-1: TEXT KEY-PRINT MATRIX .....	81
Table 4-2: THE ASSOCIATED TEXT INDEX.....	84
Table 4-3: CHARACTERS FIRST OCCURRENCE AND THEIR POSITIONS IN THE ASSOCIATED TEXT .....	84
Table 4-4: ORIGINAL KEY-PRINT MATRIX.....	84
Table 4-5: THE ASSOCIATED TEXT INDEX.....	86
Table 4-6: CHARACTERS FIRST OCCURRENCE AND THEIR POSITIONS IN THE ASSOCIATED TEXT .....	86
Table 4-7: Generated Key-print Matrix .....	86
Table 4-8: THE ASSOCIATED TEXT INDEX .....	91

Table 4-9: CHARACTERS FIRST OCCURRENCE AND THEIR POSITIONS IN THE ASSOCIATED TEXT .....	92
Table 4-10: GENERATED KEY-PRINT MATRIX .....	92
Table 5-1: A sample of the extracted QR codes .....	123
Table 6-1: Results of Three Bits per pixel method .....	129
Table 6-2: Paired-sample t-test for Three Bits per pixel.....	131
Table 6-3: ANOVA test for Three Bits per pixel.....	132
Table 6-4: Results of Six Bits per pixel method .....	132
Table 6-5: Paired-sample T-test for Six Bits per pixel .....	134
Table 6-6: ANOVA test for Six Bits per pixel.....	135
Table 6-7: Results of Nine Bits per pixel method.....	136
Table 6-8: Paired-sample T-test for Nine Bits per pixel .....	137
Table 6-9: ANOVA test for Nine Bits per pixel .....	138
Table 6-10: Results of CH (1) method.....	139
Table 6-11: Paired-sample T-test for CH (1) method .....	141
Table 6-12: ANOVA test for CH (1) method .....	141
Table 6-13: Results of CH (2) method.....	142
Table 6-14: Paired-sample T-test for CH (2) method .....	144
Table 6-15: ANOVA test for CH (1) method .....	145
Table 6-16: MOS Results for Stego Images .....	145

Table 6-17: Groups of Users Unable to Distinguish between Stego Images Containing QR (1) and QR (2).....	146
--	-----

## LIST OF FIGURES

Figure 2-1: General Model of Steganography .....	14
Figure 2-2: Types of Text Watermarking .....	19
Figure 2-3: Reverse Fatha (Memon et al, 2005) .....	22
Figure 2-4: Diacritic Steganographic Usage (Bensaad and Yagoubi, 2011) .....	22
Figure 2-5: Dot vertical displacement (M. Shirali-Shahreza and S. Shirali-Shahreza, 2006).....	23
Figure 2-6: watermarking using Kashida in Arabic (Gutub and Fattani, 2007) ...	23
Figure 2-7: The Steps of JPEG Image Compression based on DCT .....	34
Figure 2-8: Structure of a QR Code Symbol Specification (Japanese Industrial Standards, 2004)) .....	52
Figure 3-1: A General Model for Generating and Accumulating Knowledge (Owen, 1997).....	56
Figure 3-2: The General Methodology of DSR (Vaishnavi and Kuechler, 2009)	58
Figure 3-3: Proposed Framework .....	62
Figure 3-4: A Snapshot of Our Developed Tool.....	65
Figure 3-5: Five 24 bit RGB Colour Images.....	66
Figure 3-6: The Categorisation of Participants .....	70
Figure 3-7: Five Methods Used to Generate the Test Sample .....	71



Figure 3-8: The GUI for DSCQS Method.....	72
Figure 4-1: Document Logical and Physical Structure .....	78
Figure 4-2: Text Key-Print Generation Algorithm .....	82
Figure 4-3: Text Key-Print Detecting Alteration Algorithm .....	83
Figure 4-4: KEY-PRINT ALTERATION DETECTION ALGORITHM .....	88
Figure 4-5: KEY-PRINT ALTERATION DETECTION ALGORITHM .....	93
Figure 5-1: The Steganography Process .....	101
Figure 5-2: Three Different Hiding Capacities based on RGB images .....	102
Figure 5-3: Embedding Procedure.....	104
Figure 5-4: Extraction Procedure .....	105
Figure 5-5: (HC)-1 and (HC)-2 technique in embedding 64 DCT coefficient per Block .....	108
Figure 5-6: Embedding Procedure.....	111
Figure 5-7: Extraction Procedure .....	112
Figure 5-8: An example for the data embedding in (HC)-1 and (HC)-2 .....	113
<u>Figure 5-9: QR code (<a href="http://www.brunel.ac.uk/">http://www.brunel.ac.uk/</a>).....</u>	<u>114</u>
Figure 5-10: Hiding capacity for the three spatial domain methods.....	115
Figure 5-11: The Capacity (bits) of Proposed Method for Five Cover Images ..	116
Figure 5-12: Pixel Affected by Embedding One and Two QR code .....	117
Figure 5-13: Blocks (8x8) Affected by Embedding One and Two QR code.....	118
Figure 5-14: PSNR values for five cover images using 3bit method.....	119

Figure 5-15: PSNR values for five cover images using 6bit method.....	120
Figure 5-16: PSNR values for five cover images using 9bit method.....	121
Figure 5-17: PSNR (dB) of Stego Images .....	122
Figure 6-1: Weighted Assessors Opinion for Quality Grade for each Stego Image .....	129
Figure 6-2: Weighted Assessors Opinion for Quality Grade for each Stego Image .....	133
Figure 6-3: Weighted Assessors Opinion for Quality Grade for each Stego Image .....	136
Figure 6-4: Weighted Assessors Opinion for Quality Grade for each Stego Image .....	139
Figure 6-5: Weighted Assessors Opinion for Quality Grade for each Stego Image .....	142

# **Chapter 1: Information Hiding and Steganography**

## **1.1 Overview**

The evolution of networked multimedia systems, digital cameras and wireless technology was promoted by content digitalisation that has greatly increased the possibilities of reproducing and distributing information. Digital media offer distinctive advantages over analogue media: the quality of digital media is higher than that of their analogue counterparts. Copying digital content is simple and identical to the original without any loss of fidelity. Editing digital content can be done by accessing the exact discrete locations which are required to be changed (Moulin 2003). These advantages have initiated many new opportunities; in particular, it is possible to hide information within a digital content file in such a way that it is perceptually and statistically undetectable. With many schemes, the hidden information can still be recovered if the host signal is compressed, edited or converted from digital to analogue format and back (Swanson, 1998). Information hiding is thus, an emerging research area which incorporates applications for digital media copyright protection and data embedding such as watermarking, fingerprinting, and steganography.

Steganography is the art and science of covert communication by embedding a message into an innocuous looking cover media such as text, image, and video. In steganography, covert writing is established for two main reasons: protection against detection (data hiding) and protection against removal, which is in turn divided into watermarking and fingerprinting. In these applications, information is hidden within a host data set and is to be unfailingly communicated to a receiver.

This chapter provides general information about this research and begins by explaining the research background. Secondly, the research motivation of this study is discussed. Thirdly, the proposed solution is presented by setting the aim and objectives of this research. Fourthly, the method adopted to conduct this research is introduced. This chapter ends by presenting the structure of the rest of the thesis.

## **1.2 Research Background**

Steganography is the art and science of hiding communication by embedding a message into an innocuous-looking cover media. Traditional techniques of steganography varied from tattooing a trusted messenger shaved head during the 5<sup>th</sup> Century to writing secret messages during the two World Wars by invisible ink (Silman, 2001). Today, steganography uses digital media content as camouflage to hide a secret message with the help of computers computational power and signal processing techniques, thus enabling two parties to communicate covertly. The art of steganography rests in the selection of features and characteristics of a cover for hiding a secret message, while the science helps in the design and implementation of information hiding techniques. Modern steganography exploits the advantages of the present day digital media, such as text, image, audio and video in order to carry a secret message and networks of high speed delivery channels. Moreover, the message supplies additional information, such as authors' signatures, authentication information, etc. Formerly, information-hiding techniques have received more attention compared to cryptography from the research community and the industry, as the first academic conference on the subject was organised in 1996 (Anderson, 1996). According to the first international workshop, the general principle of hiding information within other data object can be described as follows:

The embedded data - the message that one wishes to communicate covertly - is normally hidden in an innocuous message, known as a cover object in which the stego-object is produced. A stego-key is used to manage the hiding process and

retrieval of the embedded data between communicating covert parties. Digital media are increasingly equipped with distinguishable marks, which may encompass a hidden copyright notification or serial number to counteract copyright violation.

Cryptography aims to keep the contents of a message secret, while steganography aims to keep the existence of a message undetectable (Wang and Wang, 2004). Encryption ciphers secret information in a way that it becomes unreadable except for the intended recipient who can decode it. The encrypted message might grab eavesdropper's attention, since its protection means something valuable is kept confidential. Therefore, this security vulnerability can be significantly reduced by using steganography techniques so that it draws no special attention.

### **1.2.1 Steganography and Cryptography**

Cryptography and Steganography are members of the spy craft family, both aiming at providing secret communication. Cryptography secretes only the meaning or contents of a message from an eavesdropper, but the encrypted message still exists and can be seen. Steganography, on the other hand, offers more secrecy than cryptography, since it hides the mere existence of secret message rather than only protecting the message contents (Lou and Liu, 2002).

A Cryptography system is jeopardized if a malicious attacker can read the contents of a secret message, while a steganographic system is jeopardized if the existence of the message is detected by an attacker. In other words, a steganographic system is considered exposed even without decoding the message, if an attacker suspects the file carrying the secret message or the steganography method used for encoding the secret message. Hence, steganography can complement cryptography to avoid raising the suspicion of system attackers and not to substitute cryptography.

Steganography is a branch of information hiding technology which encompasses applications for protection against detection and protection against removal such

as copyright protection for digital media, watermarking, fingerprinting and data embedding. In these applications, information is hidden within a host data set, which is intentionally corrupted in a covert way, so that it could be sent secretly to an intended receiver.

### **1.2.2 Steganography and Watermarking**

Steganography and watermarking are methods of data hiding and share common features. The goal of watermarking is to embed a unique signature to signify the origin or ownership of a digital media for the purpose of copyright protection, while the goal of steganography is to cover the existence of the communication taking place within a digital media. Watermarking is a mechanism used to prove that illegal copying or any minor modification of the watermarked file is done. One of the main features of watermarking is known as “robustness”, if someone knows that a digital mark exists (i.e. visible watermarking) and tries to remove the watermark from the watermarked media, he/she should consequently cause distortions or destroys the original watermarked media.

In order to take our discussion further, in the next section another technology, closely related to watermarking, called fingerprinting is discussed.

### **1.2.3 Steganography and Fingerprinting**

Watermarking and fingerprinting are closely related to steganography and fall in same domain of information hiding. Both approaches share techniques that are used to imperceptibly convey information by embedding it into the cover file, yet the kind of embedding information is of a different algorithmic form. In watermarking, all copies of the carrier object are marked in the same way, while in fingerprinting different unique marks are embedded in distinctive copies that are supplied to different clients. These unique embedded marks should identify the redistribution of illegal copies providing a traitor-tracing functionality. A steganographic system is jeopardized, if an attacker suspects a specific file or

steganography method even without decoding the message, while a successful attack on a watermarking or fingerprinting system would be the removal of the mark.

The fundamental difference between the three technologies is the underlying philosophies of the cover file. In watermarking and fingerprinting, the information hidden inside the cover file may also be public knowledge and even visible sometimes, while in steganography the imperceptibility of the hidden information is critical. A successful attack on a steganographic system consists of an adversary detecting the existence of hidden information inside a file (Artz, 2001), while a successful attack on a watermarking or fingerprinting system would be removing the mark, and not its detection. Technically, steganographic methods are considered robust against modifications that may occur during transmission and storage, but not against modification of data. Watermarking and fingerprinting, on the other hand, have the additional notion of resilience against attempts to remove hidden data. In these applications, the embedded information should be robust against possible attempts to remove it, since they provide proof of ownership of digital data (Katzenbeisser and Petitcolas, 2000). Thus, steganography's underlying philosophy is protection against detection, while watermarking and fingerprinting's underlying philosophy is protection against removal. The differences between these three technologies are summarised in Table 1-1.

**Table 1-1: Summary of the Difference between Watermarking, Fingerprinting, and Steganography**

	<b>Watermarking</b>	<b>Fingerprinting</b>	<b>Steganography</b>
Purpose	Protect intellectual property rights	Protect intellectual property rights by identifying who broke licensing agreements	Transmission of secret message without raising suspicion
Perceptual invisibility	Desirable, but not a must		Vital requirement of a steganographic system
Robustness against removal	Crucial not to be able to remove the mark		Desirable, but not a must
Large hiding capacity	Not vital since the mark is usually small		Vital requirement of a steganographic system

### 1.3 Research Motivations

With increasing use of the Internet, copyright protection of digital content has become a significant concern in an environment where intellectual property is constantly threatened. The ability of anyone to make perfect copies of digital content and the ease through which its copies can be distributed facilitate its alteration, plagiarism, piracy and illegal distribution. These features represent a threat to the owners and producers of intellectual property and digital content. Thus, many problems of modern multimedia management (content filtering, content retrieval / search, and content tagging) and multimedia security (copyright protection, broadcast monitoring, etc.) require efficient content identification tools.



Despite the textual nature of most of the information available on the Internet, digital signature and digital watermarking solutions for plain text are quite inadequate. Digital signature based solutions rely on encryption techniques. This requires a system to manage key exchange and in most cases the need for a third party in order to manage certificates and public/private key generation. Moreover, if a public key availability is disturbed or a private key is lost/ stolen then the digital signature is no longer secure and signature authentication is no longer assured. In watermarking solutions, most of the techniques and methods used to protect text depend on the text's format and structure, both of which can be easily defeated by a simple rewriting attack. Carrying out a rewriting attack does not need a professional since editing the font or spacing within a document is quite a trivial task. Although there are many novel ideas that depend on the language properties, they are not sufficient to ensure a text document's security.

Consequently, the evolution of barcode technology can be utilised to provide a unique identification (UID) number for multimedia authentication and integrity. The concept of barcodes appeared decades ago because of their reading speed, accuracy, and functional characteristics. Barcodes represent data by varying the widths and spacing of parallel lines and they are known as linear or one-dimensional (1D). Later they evolved into rectangles, dots, hexagons and other geometric patterns which are referred to as matrix or bi-dimensional (2D) codes that can store large amounts of data in a small area to support information distribution and detection (Palmer, 2004).

## 1.4 Research Aim and Objectives

Considering the limitations of cryptography, cryptographic techniques cannot only be used to protect digital documents against alteration and tampering. Therefore, QR Code and steganography are proposed to provide a higher level of security by converting document signature into QR Code which in turn will be embedded in any of the document image formats using an efficient steganography technique. This proposed solution is considered a reversible steganographic scheme which utilise the capabilities of both two dimensional barcodes and a high payload capacity in a cover document while maintaining the stego document quality (imperceptibility) to provide a robust protection for digital documents against alteration and tampering

In fulfilling this aim, the following objectives need to be achieved:

**Objective 1:** Design and implementation of a digital fingerprint that can detect any form of alteration of the original content of the text based document.

**Objective 2:** Investigation of the impact of using QR code in providing a high payload capacity and its effect on quality using different steganographic techniques.

**Objective 3:** Evaluation of the reliability of the proposed work through both objective and subjective Quality Evaluation methods.

The key contribution of the proposed work is to protect text against alteration and tampering by generating a text digital fingerprint called Text key-print. A Quick Response Code (QR code) – a two dimensional (2D) barcode – is used as a message in a carrier object to provide a mechanism facilitating a descriptive or reference function in a given digital media, namely digital text documents. The QR code – the carrier for Text key-print, – is hidden into the graphical representation component of the digital text document using image steganography techniques. These two fundamental aspects, i.e. payload capacity and imperceptibility, are at odds with each other, since it is quite challenging to

increase the payload capacity while maintaining the stego image quality (imperceptibility). A QR code scheme is thus proposed to enhance these two fundamental aspects.

## 1.5 Research Approach

The methodology followed in this research is the Design-Science Research (DSR) methodology. According to Van Aken (2005), the main goal of design science research is to develop knowledge in order to describe, explain and predict the application of knowledge which can be used by the professionals of the discipline in question to design solutions for their field problems. This research aims at producing an artefact in the form of a framework to provide a unique identification for digital documents, thereby authenticating them against copyright violations. The main aim of the research, which is to change the current situation related to organisational or social systems with regards to digital document authentication against copyright violations into a more desirable one through the development of novel artefacts, is highly consistent with the general aim of DSR.

Design artefacts are classified by March and Smith (1995) into *constructs* of vocabulary of a domain, *models* representing solution statements with appropriate levels of abstraction, *methods* in the form of algorithms and practices, and *instantiations*, which are the demonstration of the model's feasibility. The developed framework in this thesis represents a model artefact which includes *constructs*. Its application is in digital document protection and the steganographic embedding/extracting algorithms represents the *method* artefacts. Developing the proposed framework in a form of software application and validating it according to the established standards in literature illustrate the *instantiations*. March and Smith (1995) also added two main processes in constructing the design artefact: build and evaluate. The building process is to demonstrate the feasibility of the designed artefact so that its value to a community of intended users can be evaluated ensuring utility, quality, and efficacy (Hevner et al., 2004). Thus, these two main processes of design artefacts represent the outcome of this research.

## **1.6 Thesis Structure**

The rest of this thesis is structured as follows:

**Chapter 2** presents a literature review on relevant steganographic systems. It explains and critiques related work studying and choosing the appropriate practices used to enhance digital steganography. It also discusses the fundamental properties through which steganographic systems are evaluated and asserted. The discussion identifies the research gaps which this thesis is addressing.

**Chapter 3** details the research methodology conducted in this thesis. A theoretical grounding of Design Science Research (DSR) is presented in this chapter to justify the adoption of this approach. Thereafter, the research is explained in line with the DSR research cycle.

**Chapter 4** introduces a novel algorithm to protect the textual component of a digital document.

**Chapter 5** develops two image steganographic methods based in the spatial and the transform domains. The two methods are evaluated based on the main aspects of steganographic systems.

**Chapter 6** checks the reliability of objective image quality methods with a subjective image quality method.

**Chapter 7** summarises the research findings and thereby concludes the research. It also presents the main contributions which this research makes in the literature.

## **Chapter 2: Nuts and Bolts of Steganography**

### **2.1 Overview**

This chapter discusses the basic principles of digital steganography as a method of covert communication in Section 2.2. The main components and the different approaches of classifying steganographic systems are identified. Within these classifications, the main methods and key techniques of steganography are presented in Section 2.3. Writing has always been the primary mean of documenting formal communication. In the current era, we rely heavily on digital writing. A document is a material reproduction of the author's thoughts with a prime objective to transmit, communicate and store these thoughts as accurately as possible (Arno et al, 1985). A document is usually composed of text or/and graphics. Based on the textual component of a document, watermarking methods encode the digital mark directly in the text or in the text format. Many ways have been proposed to embed the digital mark such as an irregular typing style or spelling errors could be introduced, commas omitted, and words replaced by synonyms. These techniques will be discussed in Section 2.4. Section 2.5 provides a fair amount of background information regarding the presentation and properties of digital images. The concepts covered in this chapter are chosen for their relevance, in order to construct an understanding of how information is embedded in the graphical representation. An in-depth discussion on image definition, colour representation, image compression and the most common steganographic techniques in digital images will be presented.

According to Neil Johnson and Sushil Jajodia (1998) the steganographic methods proposed in the literature can be broadly classified into three categories: image domain (spatial domain), algorithmic transformations (transform domain) and masking and filtering (Adaptive Steganography). Imaging systems may introduce

some amount of distortion or artefacts in the signal during their acquisition, processing, storage, transmission and reproduction, and, therefore, assessing the perceived quality of digital image is an important aspect. There are two primary ways to measure image quality: objective and subjective quality methods (Stoica et al., 2003). The objective method is an automated measurement of the physical aspects of images. The subjective method, on the other hand, uses human observers to evaluate the quality of images. These two methods are discussed in Section 2.6 under image quality evaluation. Furthermore, the evaluation criteria and fundamental properties of the steganography method are discussed in Section 2.7 to enable us to measure the efficiency of a steganography technique.

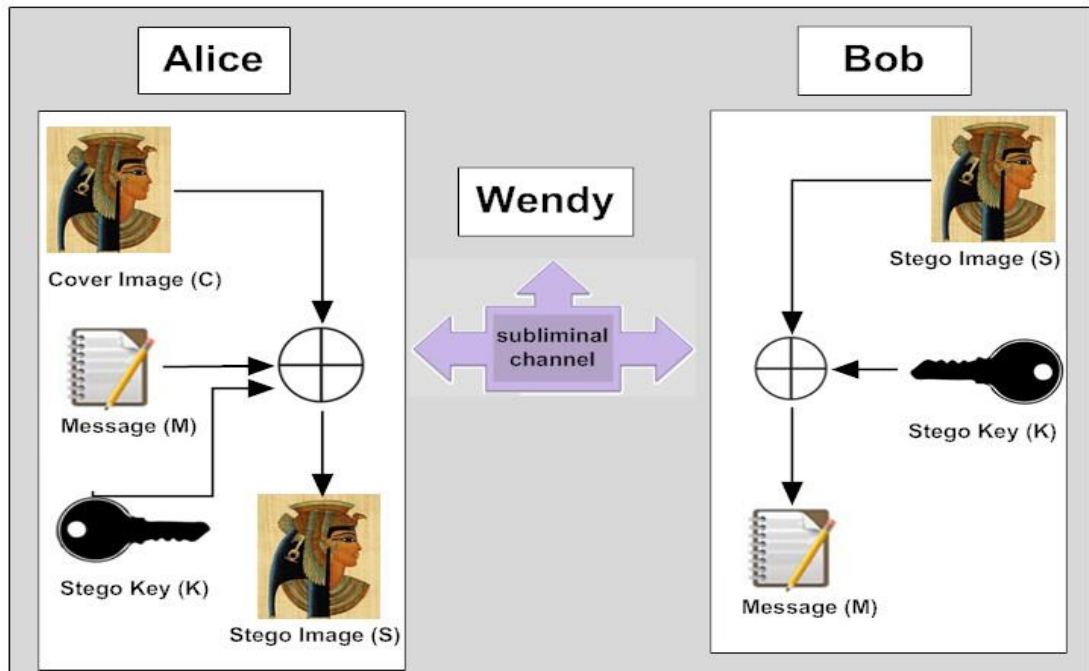
Section 2.8 presents the counter technology of steganography which can be used to defeat steganography namely steganalysis, and different types of attacks that digital steganography can be subjected to. Moreover, Quick Response Codes are covered in Section 2.9, since QR codes are vital part of the proposed scheme for enhancing steganography in digital documents. The concept of barcodes appeared decades ago because of their reading speed, accuracy, and functional characteristics. As barcodes became popular and their convenience gained universal recognition, the market began to call for codes capable of storing more information and more character types which could be printed in smaller space. Thus, research work focussing on data storage in barcodes led to the development of 2D barcodes that can store large amounts of data in a small area to support information distribution and detection (Pavlidis, 2000). Lastly, Section 2.10 provides a summary of the chapter, highlighting the key points related to the above mentioned concepts. These concepts provide a good foundation for our research framework and methodology, which will subsequently be discussed in Chapter 3.

## 2.2 Steganography Defined

“*Steganography*” is originally derived from of two Greek words *steganos* (secret) and *grafia* (writing). Gradually, it evolved into the art and science of hiding secret data in an innocent looking dummy container, thus hiding the existence of the communicated information (Bailey et al., 2004; Cachin, 1998; Kahn, 1996). The reason behind steganography being defined as an art and science is its encapsulation of multidisciplinary fields which are employed to satisfy the needs of information security. These fields include such theories and applications as: digital signal and data compression methods, information theory, signal coding theory, digital communication theory, and the theory of human visual perception (Cole, 2003; Rabah, 2004).

Although steganography is an ancient subject, its modern formulation is often cited to have given in terms originated from the prisoners’ problem proposed by Simmons (1983). The prisoners’ problem involves two inmates, Alice and Bob, who communicate through a warden, called Wendy. If Wendy suspects them to set up a plan to escape, she would send them to one of the high security jails. If Alice and Bob use cryptography to communicate securely, Wendy would notice it and may force them to reveal their secret key. Their only way to communicate securely is to send an innocuous message and embed the secret message in it. The subliminal transmission channel will no more be visible by Wendy (Katzenbeisser and Petitcolas, 2000).

The general model of steganography can be illustrated in Figure 2-1 which shows sender (Alice) who would like to send a secret message ( $m$ ) to the recipient (Bob). Alice embeds the secret message ( $m$ ) into an innocent looking dummy cover file ( $c$ ), which is an image using a stego key ( $k$ ). Consequently, Alice develops a stego file ( $s$ ) which is to be sent to the recipient (Bob) without alerting the arbitrator’s (Wendy) suspicion. Upon delivery, Bob extracts the embedded message ( $m$ ) given that he knows the stego key ( $k$ ) and the embedding method used.



**Figure 2-1: General Model of Steganography**

Some ground rules should be considered when transmitting through a subliminal channel. A cover should never be used twice, since an attacker (like Wendy) who has access to the two "versions" of one cover can easily detect and possibly rebuild the message. Therefore, both sender and receiver should destroy all covers they have already used for information transfer (Katzenbeisser and Petitcolas, 2000).

Moreover, the security of steganographic systems must be founded on the hypothesis that an attacker has full knowledge of the steganographic system embedding and extracting algorithmic procedures. Yet, he/she has no access to the stego key which must be as strong as possible in order to prevent attackers from extracting the secret information out of the cover (Cox et al., 2008).

This section has briefly discussed the basic principles of steganography. There is, however, much more to this technology than what meets the eye and an in-depth study of the available literature on different types of information hiding techniques are discussed in next section.



## **2.3 Taxonomy Of Information Hiding Techniques**

There are mainly two approaches of classification of information hiding techniques: (1) by identifying the different techniques used in the hiding process and (2) classifying according to carrier types, i.e. the type of file used as a cover object (Cole, 2003; Katzenbeisser and Petitcolas, 2000). These two general classification approaches of information hiding techniques are explained in the next subsections.

### **2.3.1 Hiding Method-Based Classification**

There are three techniques used for hiding information in a cover object (Weiss, 2009): insertion-based, substitution-based, and generation-based methods.

#### **2.3.1.1 Insertion-Based Method:**

This method depends on finding some regions in the cover object that are ignored by the processing application and then adds the secret data in these regions. The disadvantage of this method is that the size of the stego file will be larger than the size of the original cover file, but the contents of the cover file will not be altered.

#### **2.3.1.2 Substitution-Based Method:**

This method depends on finding some insignificant information in cover files and swapping this information with the secret data. It is vital to find out some regions that can be intentionally modified without having any substantial effects on this cover file (Cole, 2003). The most common substitution technique is ‘least significant bits (LSB) replacing’ technique used at the spatial domain, where the bits of the secret message substitute the LSB of the cover file. Unlike the insertion-based method, the size of both the stego file and the cover file are similar because some of the cover data are just replaced. However, depending on the cover file and hiding algorithm used, substitution may result in degrading the quality of the cover file (Fridrich, 2010).

### **2.3.1.3 Generation-Based Method**

Unlike both previous methods, this method does not need a cover file since it creates a cover file specifically for the purpose of hiding the secret message. The properties of the generated cover file are usually dependent on the secret message structure (Fridrich, 2010). While insertion and substitution methods can be discovered by comparing the stego file with the original cover file, generation-based methods prevent such types of detection since the result of a generation method is the original file.

In addition to these methods of information hiding presented above, Kipper identifies a further six categories of information hiding techniques namely: substitution, transform domain, spread spectrum, statistical method, distortion, and cover generation techniques (Kipper, 2003). Two of these six techniques (Substitution and Cover Generation) have already been discussed earlier, so the remaining four are explained below.

### **2.3.1.4 Transform Domain Technique**

This technique depends on transforming a signal from the spatial domain into a frequency representation. The embedding process is applied to the transformed coefficients. There are many transform methods such as discrete cosine transforms (DCT), discrete wavelet transforms (DWT), and discrete Fourier transforms (DFT). Transform (frequency) domain techniques spread the secret data across the entire cover and are not concentrated in one certain area or region like spatial domain techniques (e.g. LSB technique). Therefore, frequency domain techniques are considered to be more robust against attacks than spatial domain techniques.

### **2.3.1.5 Spread Spectrum Technique**

Marvel et al. (1999) defines spread spectrum communication as “the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies”. In spread spectrum, the secret message is considered as a signal

which is transmitted through the communication channel of the cover file in the frequency domain.

### 2.3.1.6 Statistical Technique

This technique only embeds one bit of secret data in a cover file resulting in a statistical change. The change of the cover statistical features (e.g. probability distribution) indicates the existence of a message; therefore, this technique depends on the capability of the recipient to configure the statistical behaviour of the cover file (Kipper, 2003).

### 2.3.1.7 Distortion Technique

Most of information-hiding techniques are blind, which means that a recipient can extract the hidden message from the stego without having the original cover file. In distortion technique, the recipient cannot extract the hidden message without the original cover, since the embedded message is the difference between the stego file and the original cover file (Katzenbeisser and Petitcolas, 2000). Kipper's six techniques can be merged with the original three categories, resulting in Table 2-1.

**Table 2-1: Steganography Technique Categories**

<b>Technique</b>	<b>General categorisation</b>
Substitution Techniques	Substitution
Transform Domain Techniques	Substitution
Spread Spectrum Techniques	Substitution
Statistical Techniques	Substitution
Distortion Technique	Insertion
Cover Generation Technique	Generation

As illustrated in the above table, substitution is the most popular technique. Such a technique does not add information to the cover file and thus does not increase the size of the stego file. However, the disadvantage of substitution is that the

amount of data of the original file to be replaced needs to be carefully selected. Otherwise the change might become perceivable and detectable.

Categorising information hiding based on the hiding techniques used is one approach. An alternative approach is considering the type of the cover file that is used to carry the embedded information. This approach is presented in next subsection.

### **2.3.2 Cover-Type Based Classification**

Almost all digital file formats can be used as a cover file to contain a hidden data or secret messages. However, the ability of such files to embed secret data depends on the availability of redundant or insignificant areas within these files. The redundant bits of a cover file are those bits that can be altered without the alteration being detected easily (Anderson and Petitcolas, 1998). Redundancy is defined as the bits of a cover object that provide accuracy far greater than necessary for the object's use and display (Currie and Irvine, 1996). For example, image files can display 16 million different colours, while the human eye is only able to perceive about 10 million different colours (Owens, 2002). The file formats with a high degree of redundancy is preferable, since redundant bits can be substituted with secret information in an imperceptible and undetectable manner. Thus, in the case of interception by an unauthorised recipient, the appearance of cover files should not indicate the existence of hidden data. Many kinds of digital media such as text, image, audio, and video files can be used as cover files. The properties of cover files vary from one type to another depending on the redundancy created in the digital representation and the unique characteristics of the file format. These properties control how the secret data can be hidden in the digital representation of the cover files. Thus, most information hiding techniques are classified according to the cover file used (Cole, 2003; Katzenbeisser and Petitcolas, 2000). Two main cover files present the focus of the work in this thesis, namely text and image.

## 2.4 Text Watermarking

Text Watermarking is the process of embedding unique information that carries the creator of the document copyright statement (i.e. watermark into a text document). Text is a common used medium for information exchange; thus, many text watermarking methods have been proposed to deal with the illicit redistribution, reproduction of information content and copyright violations. This section presents a literature survey on methods proposed for text watermarking.

Text watermarking is thought to be the tricky because of the deficiency of redundant data in a text file as compared to an image file, an audio file or a video file. M. Shirali-Shahreza and S. Shirali-Shahreza (2006) state, “The structure of text documents is identical with what we observe, while in other types of documents such as in picture, the structure of document is different from what we observe”. Therefore, information hiding in text documents should be carried out by introducing changes to the structure of the document without making any notable change to the output. Text watermarking can be broadly classified into two categories: Linguistic, which is further divided into semantic and syntactic methods; and Format based, which is further divided into the following categories: Line-shift encoding, Word-shift encoding, Feature encoding and White-space encoding as illustrated in Figure 2-2

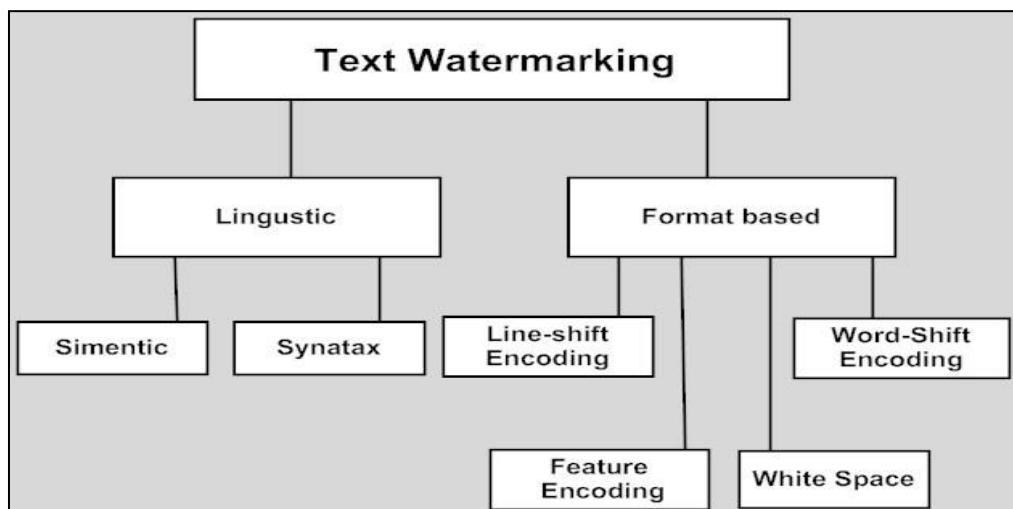


Figure 2-2: Types of Text Watermarking

## **2.4.1 Format Based Methods**

Format based methods involve changing the physical format of the text to conceal information. Generally, these methods modify existing text as a space to hide the watermark object. Insertion of spaces, non-displayed characters, resizing of fonts, and deliberate misspelling are some of the many format-based methods used in text watermarking that will be discussed in details.

### **2.4.1.1 Line-shift encoding**

Brassil et al (1995) introduced this method to text documents which moves a line upwards or downwards depending on the binary signal (watermark) to be inserted. For example, to hide a 0 bit, a line is shifted up, while to hide a 1 bit, the line is shifted down. The encoder has to shift the lines up or down, depending on the mark at which to be embedded in the file. On the other hand, the decoder measures the distance between each pair of two neighbouring lines. Two different techniques can be applied: either the decoder measures the distance between the baselines (a logical line on which the characters of a line sit) of two neighbouring lines or between the centroids (a centroid is the centre of the mass of certain text lines) of two neighbouring lines.

### **2.4.1.2 Word-shift encoding**

Brassil et al (1995) introduced another method to text based documents which slightly shifts the words within the text lines horizontally, i.e. left or right, to represent bits 0 or 1 in order to embed the unique mark. Due to variable word spacing, the decoder needs the original document in order to extract the digital mark. Thus, Huang and Yan (2001) proposed a method that slightly modifies inter-word spaces so that different lines across a text document act as sampling points of a sine wave where the wave constitutes a mark.

### 2.4.1.3 Feature encoding

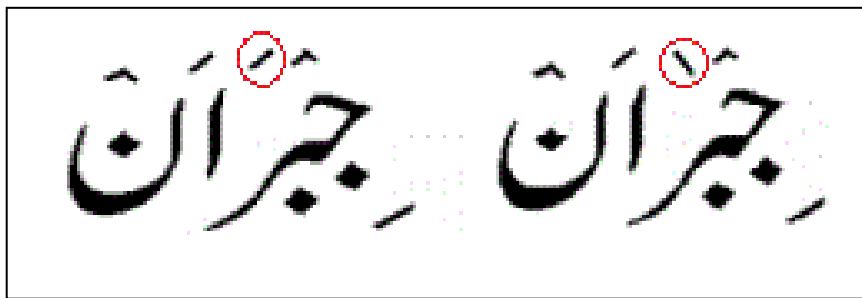
Another method proposed by Brassil et al (1999) is one where a secret message is encoded by altering one or more features of the text. These features could be the vertical lines of the letters (b, d, h, and k) or the length of the strike in letters f and t, which are changed. The length of those lines may be modified in a way that is imperceptible to the ordinary readers. Our survey revealed that feature encoding in English language is limited in comparison with Arabic, Persian and Urdu due to the richness of these languages. This will be illustrated by examples of the proposed methods for these languages in this section.

In English, the letters are written in a left-to-right format, while in Arabic and Persian the letters are written in a right-to-left format. The Arabic alphabet has 28 letters and Persian has all the letters of Arabic plus four more letters (گ، ژ، چ، پ). In these two languages, a letter can have four different shapes determined by the position of that letter in a word. For example the letter «ع» is written as «عـ» at the beginning of a word, as «ـع» in the middle, as «ع» at the end, and as «ع» in an isolated form. In the Arabic and Persian languages, the dot is very important and 17 of 32 Persian letters and 14 of 28 Arabic letters have one or more dots. Among these 17 letters, 5 letters have 3 dots, 2 letters have 2 dots, and the remaining 10 letters have one single dot illustrated in Table 2-2, while in English only two small letters have dots, "i" and "j".

**Table 2-2: Arabic and Persian Letters Dots**

Without	ا ح د ر س ص ط ع ك گ ل م و ه
One	ب ج خ ذ ز ض ظ غ ف ن
Two	ت ق ی (پ)
Three	پ ث چ ژ ش

One of the characteristics of the Arabic language is the use of diacritics i.e. (Fatha, Kasra, and Damma). Fatha is a dash-like symbol ‘َ’ placed over a character, whereas Kasra is also a dash-like symbol ‘ِ’ placed below a character; Damma is a number nine-like symbol ‘ُ’ placed over the character. These diacritics are applicable on each alphabet character in the Arabic language to give a different pronunciation only. Memon et al (2005) proposed the use of Fatha in reversed order to hide a secret character in the text for the intended receiver. A highlighted example is presented in Figure 2-3 to explain the implementation.



**Figure 2-3: Reverse Fatha (Memon et al, 2005)**

Another implementation utilising the Arabic language’s characteristics is proposed by Bensaad and Yagoubi (2011), where the secret bit is 1 when the diacritic is present and 0 if the diacritic is removed. Figure 2-4 shows an example of this method.

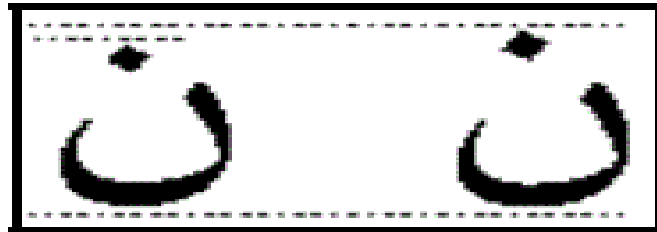
Cover text:	مُسْتَفْعِلٌ
Secret bits:	0 1 1 0 0 1
Stego-text:	مُسْتَفْعِل

**Figure 2-4: Diacritic Steganographic Usage (Bensaad and Yagoubi, 2011)**

M. Shirali-Shahreza and S. Shirali-Shahreza (2006) proposed a method which takes advantage of the existence of too many dots in Persian and Arabic characters. With this method, they encode the information in text documents by



adjusting the vertical displacement of the dots (see Figure 2-5), to encode information in text documents.



**Figure 2-5: Dot vertical displacement (M. Shirali-Shahreza and S. Shirali-Shahreza, 2006)**

Gutub and Fattani (2007) proposed a method using the pointed letters with extension (Kashida in Arabic or elongation) to hold the secret bit ‘one’ and the un-pointed letters with extension to hold the secret bit ‘zero’. Note that letter extension does not have any effect to the writing content. It has a standard character hexadecimal code of 0640 in the Unicode system. Figure 2-6 shows an example of this method.

Watermarking bits	110010
Cover-text	من حسن اسلام المرء تركه مالا يعنيه
Output text	<p>من حسن اسلام المرء تركه مالا يعنيه</p> <p>↑↑ ↑↑↑ ↑</p> <p>1 1 0 0 1 0</p>

**Figure 2-6: watermarking using Kashida in Arabic (Gutub and Fattani, 2007)**

#### **2.4.1.4 White-space encoding**

This technique uses white spaces for hiding a secret message. There are three methods of hiding data using white spaces. In inter sentence spacing; a single space is inserted to hide a bit 0 and two spaces to hide a bit 1 at the end of each terminating character. At end of line spaces, a fixed number of spaces is inserted at the end of each line. For example, two spaces to encode one bit per line, four spaces to encode two bits and so on. Using the inter word spacing technique, one space after a word represents bit 0 and two spaces after a word represents bit 1 (Bender et al, 1996).

### **2.4.2 Linguistic Methods**

Linguistic methods consider the use of a language linguistic properties as the space in which messages are hidden. This section describes existing linguistic methods, which themselves are divided further into syntactic and semantic methods.

#### **2.4.2.1 Syntactic Method**

Text is composed of sentences which themselves are constituted of words, and words can be nouns, verbs, articles, prepositions, adjectives, adverbs etc. Sentences have various syntactic structures, depending on a language and its principles. One of the common approaches towards text watermarking is applying syntactic transformations on text structures to embed watermarks. A simple implementation to conceal information in a text file could be done, by inserting some punctuation signs such as comma (,) and full stop (.) in specific places. Thus this method commands identifying the appropriate place for positioning punctuation signs within text (Bennett, 2004). For instance: the phrases “bread, butter, and jam” and “bread, butter and jam”, both are correct phrases considering the use of commas to list. The alteration between phrases can provide a binary message, as the first phrase can denote ‘1’ while the second phrase can denote ‘0’. Another syntactic approach includes changing the diction and structure

of a sentence without modifying the meaning of text. Another example, the sentence “before the weekend is over, I will clean my car.” Could also be stated “I will clean my car, before the weekend is over.”

Atallah, et al., (2000) introduced the natural language (NLP) watermarking scheme which depends on the syntactic and the semantic structures of text to construct a syntactic tree and apply certain transformations on this tree to embed the watermark, while preserving the inherent properties of the text. Hassan et al. (2009) proposed another natural language watermarking method by transforming text into a syntactic tree diagram and performing morpho-syntactic alterations to the text, so that the watermark is embedded.

#### 2.4.2.2 Semantic Method

Atallah, et al., (2000) also introduced synonym-substitution to watermark text by assigning primary or secondary values for two synonyms. Based on this concept, M. Shirali-Shahreza and S. Shirali-Shahreza (2008) proposed a method relying on the different diction of words in English language between the UK and the US. For instance, the word “check” is spelled in the UK English as (cheque) and the in US English as (check). Table 2-3 shows a list of words with different spelling in the US and UK the (M. Shirali-Shahreza, 2008)

**Table 2-3: List of words with different spelling in UK and US (M. Shirali-Shahreza, 2008)**

<b>British Spelling</b>	<b>American Spelling</b>
Favourite	Favorite
Criticise	Criticize
Fulfil	Fulfill
Centre	Center
Dialogue	Dialog
Mediaeval	Medieval
Cheque	Check
Defence	Defense
Tyre	Tire

M. Shirali-Shahreza and S. Shirali-Shahreza (2008) also proposed a method relying on substituting the words with different terms in the UK and the US English language. For instance, the word (Candy) is the term used in the US and the term (Sweets) in the UK. Table 2-4 shows a list of words with different terms in the US and the UK.

**Table 2.4: List of Words with Different Terms in US and UK (M. Shirali-Shahreza and S. Shirali-Shahreza, 2008)**

British English	American English
Bill	Account
Sweets	Candy
Cupboard	Closet
Autumn	Fall
Petrol	Gas
Post	Mail
Film	Movie
Parcel	Package
Football	Soccer

All of the above mentioned algorithms are critically analysed as follows. Format based methods might trick a user who ignores irregular space-insertion, but are not immune to text reproduction attacks. These methods can be easily detected by using Optical Character Recognition (OCR), and destroyed by editing the document margins and paragraph spacing. A computer, as well might not recognise feature encoding in text format as a problem, however, a watermark can be simply damaged by a “copy paste to notepad” attack. In this way, all the changes made in the text to embed the watermark are lost. In Linguistic Methods, the synonym based techniques may change the exact meaning of the substituted word; hereafter they destroy the semantic connotation of text documents, especially those of a sensitive nature such as legal documents, poetry, and quotes. Moreover, research into semantic techniques is still at an immature stage.

In conclusion, encoding data in text is a challenging task due to the small amount of redundant data in text files that can be replaced with a secret message (Katzenbeisser and Petitcolas, 2000). Furthermore, the embedding task requires

the interaction of the user and cannot be automated. Therefore, text watermarking methods proposed so far lack robustness, practicality and has limited applicability to protect text against illicit redistribution, reproduction of information content and copyright violations.

## **2.5 Image Steganography**

Due to the large amount of redundancy created in the manner in which digital images are represented, images are the most appropriate carrier type for steganography. Coding data in digital images is the most widely exercised of all information hiding methods. Wayner (2002) stated that: “There are millions of images floating about the Net used as window dressing for Web sites and who knows what. Anyone could hijack the bits to carry their own messages”. Technically, any digital media that can be converted into a bit stream and concealed in a digital image and take advantage of the human visual system (HVS) limitation power (Johnson and Jajodia, 1998). With the growing popularity of graphical media and capabilities of modern computers along with the research conducted on image based steganography, this field is growing rapidly as images are considered the ideal carrier objects

### **2.5.1 Background on Digital Image**

An image is understood by a computer as an array of numbers that exemplify light intensities at a number of points (Johnson, and Jajodia, 1998). These points are known as pixels, which compose the image’s raster data. In a colour scheme, the number of bits assigned per pixel is known as the bit depth (Owens, 2002). In most image colour scheme, the least bit depth is 8 bits are used to correspond to a colour per pixel. Images with 8 bits per pixel are capable of displaying up to 256 different shades of grey. Digital coloured images utilising the RGB colour model are saved in 24-bit files as the three basic colours: red, green, and blue responsible to display all the colour variations per pixels are represented in 8-bits for each colour. Hence, in any given pixel, the number of different colour variations can

reaches 256 per colour channel adding up to more than 16 million combinations of colours. The most common image formats on the Internet, are joint photographic experts group (JPEG), graphics interchange format (GIF), portable network graphics (PNG) and bitmap format (BMP) (Cheddad et al, 2010).

Digital images files with 8-bit and 24-bit per pixel image have their advantages and disadvantages when used for a steganographic method. The 8-bit images are commonly used due to their relatively small size, but only 256 possible colours can be utilised which can be a potential limitation in the process of encoding. On the other hand, 24-bit images offer over 16 million colours available to pick from which goes beyond the human visual system (HVS) that can only perceive about 10 million different colours (Owens, 2002). Thus, 24-bit digital image can encode much larger amount of hidden data and be difficult to detect in comparison with an 8-bit digital image. However, 24-bit digital image major drawback is their large size when sent over a standard network connection (The Internet) can make them draw attention of possible attacks more than the 8-bit digital images.

When dealing with images of greater bit depth, the image file size turn out too large to be sent over the Internet. Thus, some methods were introduced to reduce an image's file size so that it can be displayed in reasonable time and use less space during storage. These methods employs mathematical formulas to compress image data, leading to a smaller file sizes also known as image compression (Scheider and Gersting, 2004). Image compression is a good solution for the susceptibility of digital images which have greater bit depth such as 24-bit images. Two types of compression are applied in digital images, lossy and lossless. Lossy compression significantly condenses the image size and saves storage space by removing excess image data which human eyes find hard to spot. The resultant image is not exactly the same as the original, just a close approximation of the original. One of the major drawbacks of lossy compression methods is that they increase the risk of the loss of some parts of the uncompressed secret message because lossy compression strip off what it consider as surplus image data. Lossless compression method preserves the original digital

image in its entirety with the possibility to reconstruct an identical copy of the original data. Therefore, this compression technique is a preferred choice for steganographic uses.

## **2.5.2 Spatial Domain**

Spatial domain techniques modify the parameters of the cover-image, i.e. the payload or disturbance between the cover-image and the stego-image in order to make it imperceptible to human eyes. These techniques take into account the characteristics of the human vision system (HVS) and make use of its limitation in order to embed data in cover images. Cover image resolution and its depth of colour are two factors which can be used to manipulate the cover in order to make it less noticeable. Basically these techniques attempt to hide secret information by replacing insignificant segments of the cover with secret message bits. The extraction of the secret information is not possible unless the receiver knows its position. The sender assumes that a passive attacker cannot notice the existence of the secret message since few modifications were made in the embedding process.

Various steganographic techniques proposed in the literature include: LSB substitution, LSB matching, Adaptive LSB, Pixel Value Differencing (PVD), Edge detection filter, Pixel Indicator techniques, Component based LSB, and many other techniques (Mamta and Parvinder, 2013). These embedding techniques utilise image cover to enhance the trade-off between the three main criteria of steganographic system: imperceptibility, robustness and payload capacity.

Chang et al., (2002) and Thien et al., (2003) state that **LSB substitution** is the technique commonly used to generate the stego-image by replacing the least significant bits (LSBs) of pixels of a cover image with the secret bits. The LSBs of an image pixel is replaced with the encrypted message. Thus, authenticated receivers can only extract the message from the cover image using a pre-shared key, since altering the LSB of a cover image is visually imperceptible by a human.

The algorithm hiding capacity is 1 bit per pixel. In order to improve the perceived quality of the stego-image, (Wang et al., 2000) had developed a genetic algorithm to produce a substitution table for embedding the secret data into a number of the image pixels by editing the pixel value to another value closer to the original image value. Without the use of genetic algorithm, Chan and Cheng (2001) proposed a simple LSB substitution method using an Optimal Pixel Adjustment Process (OPAP) to improve the visual quality of the stego-image and enhance image embedding effectiveness.

Ker (2004) introduced the **LSB matching** scheme, which modifies the LSBs of the pixels by randomly incrementing or decrementing one bit in the cover pixel value, if the secret bit is not similar to the LSB of the cover image. Mielikainen (2006) add another method which significantly improves LSB matching scheme by reducing the expected number of modifications per pixel from 0.5 to 0.375. One of the bit falls of these techniques is the visual quality of the stego-image is badly damage due to the artificial noises caused in image smooth regions.

The research carried out in simple image LSB substitution found that the histogram of stego image demonstrates a “pair-wise” block, which is referred to as Pairs of Values (PoV). Chi-square Test can identify stego images because of that PoV (Westfled and Pfitzmann, 2000). To overcome this issue, **Adaptive LSB** employs the Human Visual System (HVS) characteristics to create a mapping function, which will determine the adaptive number of LSBs for data hiding depending on the HVS contrast sensitivity. Lee and Chen (2000) proposed a mapping function for data hiding that exploits the properties of contrast and luminance in an image pixel to embed the secret data into a variable size using LSB insertion technique. Liu et al., (2004) proposed a method that groups pixels of the cover image depending on their intensity. Then the different frequency within each group is counted, so that the secret message to be embedded according to a priority for pixels with high frequencies.



**Pixel value differencing (PVD)** method was proposed to enhance the quality of the stego-image by selecting a range where the difference between the values of two neighbour pixels is tiny. This range takes advantage of the HVS sensitivity to intensity variations from smoothness to high contrast (Wu and Tsai, 2003). Wu et al (2005) proposed a method that hides the secret data into the smooth areas using LSB substitution and PVD methods in the edge areas, if the difference between two consecutive pixels falls into a certain level. Furthermore, Yang et al. (2008), proposed an adaptive method using LSB substitution and PVD. The method embeds the secret message in pixels located in edged areas more than smooth areas, where the hiding capacity is determined by the difference value of two neighbourhood pixels. However, these methods belonging to PVD assumes that edge area can handle changes better than smooth areas, but these methods cannot differentiate between texture and edge features.

To overcome this problem, **Edge detection filtering** approach was introduced by Alwan et al. (2005). They used Sobel mask filter and a fuzzy approach for embedding data in images edge area. Hussain and Hussain (2011) worked on varying the threshold value of filter to hide the data around the edge area of an image. Their experimental results show a limited hiding capacity but high PSNR values. Chen et al (2010) proposed a scheme based on utilising a hybrid edge detector which is made of the fuzzy edge detector and the canny edge detector, and LSB substitution to construct a better stego image quality with 2.88bpp embedding rate.

All previous discussed techniques focused on greyscale images until image technology advanced and paved the way to steganography application for colour images based on the RGB model. To this end, **Pixel Indicator Techniques** was introduced by Gutub et al. (2008, 2009). They proposed a steganographic technique which use the least two significant bits of one of the colour channels at RGB based image to indicate existence of data in the other two channels combined with a random function to form the stego Key.

By doing so, they take advantage of the 8-bits binary representations of each colour channel to provide high hiding capacity in the RGB image base steganography. These methods encourage researchers to understand the contribution of each of the colour channels (red, green, and blue) components on the visual perception, which lead to the introduction of **component based approaches**.

Chou et al (2008) proposed a large payload data embedding method that modifies the pixel LSBs of the blue channel in order to indicate where the secret data is hidden. They choice the blue channel because human eyes are an insensitive towards changes in blue values. In a related work, Mandal and Das (2012) proposed a method based on PVD and embedding the secret data in a variable number of bits at each colour components of a pixel in a colour image. Hamid et al. (2009) proposed a steganographic method which splits the texture areas into two sets, simple and complex texture areas. In the simple texture area, they embed in three LSBs from the red and green colour components and in two LSBs from the blue components, while in the complex texture area, data embedding is increase to four LSBs from the three colour components. This approach increases the data hidden in the image but if any filter is applied in the stego-image, the message gets lost.

### 2.5.3 Transform Domain

The transform based technique utilises the characteristics of different algorithmic transformations applied to images in order to embed data by transforming images from the spatial domain to the transform domain such as discrete fourier transform (DFT), discrete cosine transform (DCT) and discrete wavelet transform (DWT). In these techniques, the image must be transformed before embedding, and then the coefficients of the transformed image are slightly modified to accommodate data of the payload before the image is retransformed to spatial domain. The data of the payload is replaced with the smaller insignificant coefficients of the transformed image.

Under the DCT, hiding secret information in a cover image can be performed into Global or Block-based. In the global, DCT computation is performed on the whole image. In the block-based, the image is partitioned into non overlapping block of size 8×8 and DCT computation is performed on each block separately using forward DCT. The two-dimensional transformation of DCT and IDCT (inverse DCT) are defined as follows:

Forward DCT:

$$F(u, v) = c(u) \cdot c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cdot \cos\left(\frac{(2x+1)u\pi}{2N}\right) \cdot \cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (2.1)$$

If  $u = v = 0, C(u) = c(v) = \sqrt{1/N}$ ; otherwise  $c(u) = c(v) = \sqrt{1/2N}$ ,

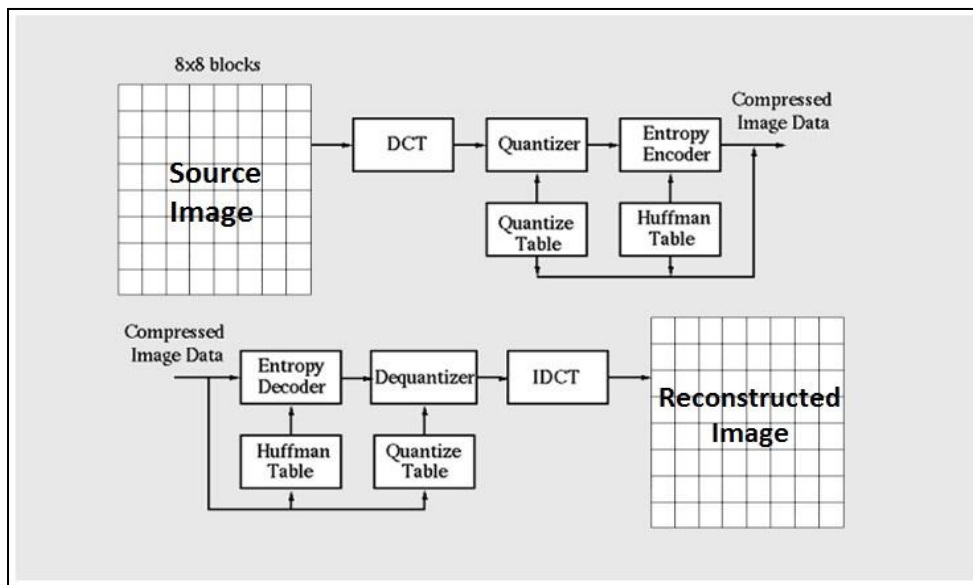
Inverse DCT:

$$f(x, y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u) \cdot c(v) \cdot f(u, v) \cdot \cos\left(\frac{(2x+1)u\pi}{2N}\right) \cdot \cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (2.2)$$

Note that, the input image is DCT matrix of size NxN, where x, y, u, v = 0,1,2,...N-1. Equation symbols refer to: (x and u) row, (y and v) column, c (x, y) the intensity of the pixel, and C (u,v) the DCT coefficient. Every 8x8 block is composed of 64 coefficients: the direct current (DC) which is the coefficient at the top left of a block and the remaining 63 coefficients are called the alternate current (AC). The DC coefficients provides a good estimate about the details in each block and if DC coefficients value is changed many of the AC coefficients values will change as well. The consequences of changing the DC coefficients value will appear when the image is transformed back to the spatial domain in form of visual discrepancy.

This transforms 8x8 pixel blocks into 64 DCT coefficients with three different frequency bands: low frequency (FL), middle frequency (FM) and high frequency (FH) (Wallace, 1991). The literature survey shows that information hiding methods prefer the middle frequency bands because embedding in the low frequencies will affect important parts of the image while high frequency components are overexposed to removal through compression and noise attacks (Bohme and Westfeld, 2005).

DCT is widely used with video and image compression e.g. JPEG lossy compression which aims at providing large compression ratio while maintaining high image quality. The general compression process can be broken up into two main procedures: encoding and decoding as show in Figure 2-7.



**Figure 2-7: The Steps of JPEG Image Compression based on DCT**

The JPEG encoding process consists of three main steps: forward DCT (FDCT), quantisation, and entropy encoding, as shown in Figure 2-7 (ISO-DIS, 1992). The input image is divided into non overlapping blocks of size 8×8 pixels. Then, each block is transformed by the FDCT into a set of 64 DCT coefficients. In the quantisation step, all DCT coefficients of each block are divided by predefined quantisation values obtained from the quantisation table (QT). These values can be any integer from 1 to 255. Note that some camera manufacturers have their own built in QT to balance the trade-off between image compression and quality factor. Then, each quantised DCT coefficient is rounded to the nearest integer. Hence, it is a lossy process due to the rounding error. Finally, these quantised DCT coefficients are encoded using an entropy encoder (Huffman coding or arithmetic coding), which is a lossless process. The second process is the reverse engineering of the first process. The JPEG decoding process also consists of three main steps: entropy decoding, de-quantisation, and inverse DCT (IDCT) (ISO-

DIS, 1992). The compressed image code is entropy decoded and the quantised DCT coefficients are obtained. In the de-quantisation step, each block of quantised DCT coefficients is multiplied with the quantisation table to convert these coefficients to their approximate value. Afterwards, the IDCT is used to convert the de-quantised DCT coefficients to their spatial values.

Koch and Zhao (1995) introduced the first efficient watermarking scheme. With this method, the image is first divided into square blocks of size 8x8 for DCT computation. Then a pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. Bors and Pitas( 1996) developed a method that modifies DCT coefficients satisfying a block site selection constraint. After dividing the image into blocks of size 8x8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. Swanson et al, (1996) introduced a DCT domain watermarking technique based on the frequency masking of DCT blocks. Cox et al, (1997) developed the first frequency-domain watermarking scheme. After that, a lot of watermarking algorithms in the frequency domain have been proposed. However, the JSteg algorithm was among the first steganographic algorithms to build upon the standard JPEG compression (Provos and Honeyman, 2003). It was proposed by Derek Upham. His approach was to sequentially replace the LSB of the quantised DCT coefficients with secret bits and skip all coefficients whose magnitudes are 0 or 1. Even though manipulating the LSB of quantised DCT coefficients (frequency domain) can harm the stego image quality, JSteg is resistant against visual attacks. Although the algorithm stood strongly against visual attacks, it was found that examining the statistical distribution of the DCT coefficients shows that it leaves the significant statistical signature of the hidden data (Provos and Honeyman, 2003). The JSteg method can however be easily detected by simple statistical attacks (e.g. chi-square attack - $\chi^2$  test-) (Westfeld and Pfitzmann, 1999).

Outguess is a steganography software written by Niels Provos (Provos, 2001). Outguess and JSteg are almost similar techniques. However, Outguess scatters the locations of embedding by using a pseudo random number generation (PRNG) to shuffle the ordering of the coefficients. Moreover, it carefully uses the LSB technique to avoid causing statistical distortions which may attract the attention of the attackers to steganography.  $X^2$ -test does not detect data that is randomly distributed but Provos and Honeyman (2003) suggested an extended version of the  $X^2$ -test to detect Pseudo randomly embedded messages in JPEG images.

The F5 algorithm was proposed and created by Andreas Westfeld (Westfeld, 2001). It is based on subtraction and matrix encoding, also known as syndrome coding. The F5 algorithm skips the DC and the AC coefficients whose magnitudes are zero, so it does not use them for embedding. Moreover, it decrements the absolute value of a quantised DCT coefficient by one to embed a secret bit and it uses a matrix encoding technique which spreads the secret information out among more bits. Therefore, if a given secret bit does not match the LSB of a predefined coefficient, the algorithm decrements the absolute value of this coefficient. Otherwise, the value of this coefficient will not be changed (Cox et al., 2008). Neither the  $X^2$ test nor its extended version can break this solid algorithm. However, Fridrich et al. (2003) proposed a steganalysis method which exploits the natural distribution of DCT coefficients and detects F5 contents.

## 2.5.4 Adaptive Steganography

Adaptive steganography is a special case of the two former discussed methods. It is also known as “Statistics-aware embedding” (Provos and Honeyman, 2003), “Masking and Filtering” (Johnson and Jajodia, 1998) or “Model-Based” (Sallee, 2004). This method takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. It is characterised by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD, standard deviation. Adaptive steganography seeks images with existing or deliberately added noise and images that demonstrate

colour complexity, avoiding areas of uniform colour. However, in order to maintain the image's quality, it is necessary to take the human visual system (HVS) into consideration and ensure that the distortion introduced by embedding is imperceptible to the human eye.

One of the embedding strategies in the spatial and frequency domain relies on image thresholding. Thresholding is one of the methods used in image segmentation where a binary image is created from a grayscale image. One of its main functions is to separate objects from the background such as printed characters, graphical content and map processing where lines, legends and characters are to be detected. In Sezgin and Sankur (2004), thresholding methods are categorised according to the information they obtain from the data into:

1. Histogram-shaped-based: these analyse the form and shape of image histogram such as the peaks, valleys and curvatures.
2. Clustering-based: these rely on generating two cluster objects (background and foreground) from grey-level information.
3. Entropy-based: these use the entropy of the distribution of grey levels in the picture.
4. Object attribute-based: these are methods that extract a threshold value based on similarities between the original image and the binarized one using some attribute quality or similarity measure.
5. Spatial approaches: these use higher-order probability distribution and/or correlation between pixels.
6. Locally adaptive methods: these calculate a threshold value for each pixel, depending on some local parameters like range, variance or surface-fitting in the neighbourhood.

Among the first adaptive thresholding techniques was the algorithm developed by Nakagawa and Rosenfeld (1979), who proposed a variation on the original

method of variable thresholding by Chow and Kaneko (1972). In their method, the image is divided into several windows of the original image with the locality property. Those windows with bimodal histograms are selected and a threshold is calculated. Then the threshold from different windows is incorporated to calculate a final threshold for the whole image. Their results were successfully applied to the TV images of machine components with substantially better results than those that applied a fixed threshold to the whole image.

Niblack (1986) developed an algorithm that adapts threshold selection from a local window by calculating a local mean and standard deviation. This method was later enhanced by Sauvola and Pietikaine (2000) to recognise letters in stained documents or documents with bad illumination by adjusting the impact of the standard deviation in the algorithm. Such techniques are known as **local variance methods**.

**Local contrast methods** are also the techniques which belong to the same thresholding class. White and Rohrer (1983) suggested comparing the grey level of a pixel with the average of the grey levels of their neighbouring pixels. In their experiments, they used a window which is approximately the size of a printed character. If a pixel is significantly darker than the average, it can be classified as a character pixel; otherwise, it is a background pixel. Huang and Wang's (1995) method first smoothens the image by averaging the grey level of a pixel with their local neighbours provided that the range (difference between maximum and minimum grey levels within the window) is below a given threshold. Afterwards, an adaptive threshold is applied, which sets a pixel to the maximum value if it is greater than the local average or to a minimum value if the local range is below a second threshold.

## 2.6 Image Quality Evaluation

Imaging systems may introduce some amounts of distortion or artefacts in the signal during its acquisition, processing, storage, transmission and reproduction,



so assessing the perceived quality of digital image is an important problem. There are two primary ways to measure image quality: objective and subjective quality methods (Stoica et al., 2003). The objective method is an automated measurement of the physical aspects of images. The subjective method, on the other hand, uses human observers to evaluate the quality of images.

## 2.6.1 Objective Quality Evaluation

Objective image quality evaluation metrics are classified into three categories according to the availability of the original (distortion-free) image: (1) full-reference means that the original and test images are available, (2) reduced-reference means that the test image and some information about the original image are available, and (3) no-reference means that only the test image is available. The most widely used full reference quality metric is the mean squared error (MSE), computed by averaging the squared intensity differences of distorted and reference image pixels, along with the related quantity of peak signal-to-noise ratio (PSNR) (Sheikh et al., 2006). Furthermore, PSNR is considered as a reference model to evaluate the efficiency of stego image quality and used in many image processing applications (Wang et al., 2004).

The Peak Signal-to-Noise Ratio (PSNR) is a statistical analysis measurement used for digital image or video quality assessment by calculating the mean squared error (MSE) where one of the images is considered a noisy approximation of the other. The MSE and PSNR equations are given below, where  $i$  and  $j$  are the image coordinates,  $m$  and  $n$  are the dimensions of the image,  $S_{ij}$  is the generated stego-image,  $C_{ij}$  is the cover image and  $C_{max}^2$  is the maximum value in the image. PSNR is expressed on a logarithmic scale in decibels (dB).

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [S_{ij} - C_{ij}]^2 \quad (2.3)$$

$$PSNR = 10 \log_{10} \left( \frac{C_{max}^2}{MSE} \right) \quad (2.4)$$

The best image quality can be found when the MSE value is very small or going to be zero since the difference between the original and reconstructed image is insignificant. A fall in the PSNR values below 30 dB due to distortions caused by embedding a secret image indicates a fairly low image quality. In contrast a high quality stego-image should strive for PSNR values of 40 dB or above. Moreover, it is difficult for the human visual system to recognise any difference between a greyscale cover image and its stego image if the PSNR value exceeds 36 dB (Wu and Hwang, 2007).

## 2.6.2 Subjective Evaluation Method Key Concepts

The method is a structured experimental design and depends on human subjects to assess the quality of images. In practice, humans are asked to observe some images usually with a full reference to other images, and then evaluate their visual quality either to a quality scale or an impairment scale. Thus, subjective measures are the most reliable method to assess image quality since human beings are the intended receivers in most applications (Stoica et al., 2003). However subjective evaluations are difficult to repeat, very expensive, and time consuming. Table 2-4 summarises the scales used in evaluating image quality (ITU-R-BT.500-11, 2002).

**Table 2-4:** Grade Quality and Impairment Scale

<b>Five-Grade Quality and Impairment Scale</b>			
<b>Quality Scale</b>		<b>Impairment Scale</b>	
5	Excellent	5	Imperceptible
4	Good	4	Perceptible, but not annoying
3	Fair	3	Slightly annoying
2	Poor	2	Annoying
1	Bad	1	Very annoying

The subjective quality measurement Mean Opinion Scores (MOS) is the average score for the subjects' scores to these rated images (Simone et al., 2009). The

MOS is calculated for each test condition  $k$  (i.e. steganography method) where  $m_{nK}$  is the score of subject  $n$  for the test condition  $k$  and  $N$  is the number of subjects as follows:

$$MOS_k = \frac{\sum_{n=1}^N m_{nK}}{N} \quad (2.5)$$

The first standard of subjective image quality evaluation was published in 1974, i.e. ITU-R BT.500-7 "Methodology for the subjective assessment of the quality of television pictures". This standard establishes a certain reference image against which the impairment factors that affect the overall appearance of the image are measured, as well as some of the earlier approaches to subjective television picture assessment (Allnatt, and Lewis, 1965).

- **Assessor:** An assessor is defined as a person taking part in a quality evaluation test. Other synonyms for assessor include participant, evaluator, and pane list user. The assessors can be categorised based on their sensorial sensitivity, experience in evaluation and domain specific knowledge into 1) naive assessors (untrained, defined as the assessors who do not meet any particular selection criterion for assessment tests, neither do they have experience in the research domain or in evaluation tasks), 2) experienced assessors (trained for accurate, detailed, and domain-specific evaluation tasks e.g. visual artefacts) and 3) experts (who are involved with audio and/or video quality or technology as part of their normal work (ITU-T P.920, 2002)).
- **Evaluation tasks:** An evaluation task is either overall quality evaluation or an attribute-specific evaluation. An overall quality evaluation task is called affective measurement and it can be used to evaluate heterogeneous stimuli material to build up the global or holistic judgment of quality. it assumes that both stimuli-driven sensorial processing and high-level cognitive processing – including knowledge, expectations, emotions and attitudes – are integrated into the final quality perception of stimuli, for

naive participants in user or consumer-oriented studies (Bech and Zacharov, 2006; Lawless and Heyman, 1999). An attribute-specific evaluation task is called a perceptual measurement. It is an objective quantification of the sensorial strength of the individual attributes of perceived stimuli (Bech and Zacharov, 2006). It defines the dimensions (e.g. brightness) for the participants and it requires the use of highly trained and experienced assessors (Bech and Zacharov, 2006).

- **Stimulus:** is a test material presented to the participant during the study and it is characterised by content, treatment and duration. Content is a sequence of video clips where treatment is generated. Treatment represents the independent variables in the experiments. The duration of the stimulus content varies depending on the phenomenon under study (e.g. transmission) and the target of the study. A short stimulus material, such as 10s, is conventionally used to go beyond the limitations of human working memory (Aldridge et al., 1995).
- **Scaling and comparisons:** Scaling refers to the application of numbers to quantify the sensory experience (Lawless and Heyman, 1999). In quality evaluation research, the scales used vary from nominal to continuous and are labelled or non-labelled. Furthermore, the chosen scaling also determines the statistical method of analysis. Comparisons refer to the way the stimuli are presented and rated. In single stimulus studies, each stimulus is rated independent of other stimuli. The double stimulus studies are used for pair-wise comparisons between two stimuli and multiple comparisons are used for comparisons between more than two stimuli.

Moreover, Recommendation ITU-R Rec.500-11 describes the subjective evaluation of visual quality and suggests criteria for: selection of observers, test materials, viewing conditions, evaluation procedures, and analysis methods. This international standard contains various methods of subjective evaluation for image quality, such as, double stimulus continuous quality scale (DSCQS), double stimulus impairment scale (DSIS), single stimulus continuous quality evaluation

(SSCQE) and many other methods. The double stimulus continuous quality scale (DSCQS) is one of the most adopted methods for subjective image quality evaluation in both research community and the industry (Baroncini, 2006). Moreover, (DSCQS) is widely accepted and used as an accurate test method (Pinson and Wolf, 2003).

### **2.6.3 Subjective Evaluation Related Work**

Stoica et al. (2003) implemented both objective and subjective tests on two JPEG 2000 algorithms. The objective quality of 24 bpp RGB colour images was evaluated by three methods (PSNR, normalised MSE, and normalised colour difference methods). Moreover, they performed the subjective tests with a panel of ten assessors where three images were presented at once; the reference image was placed in the middle, while both compressed images were randomly positioned on the left or the right of the reference image. According to their results, the subjective evaluation was in contradiction with the objective measures (Stoica et al., 2003).

Grgic et al. (2004) investigated the reliability of nine objective picture quality measures for application in still image compression systems. Furthermore, they evaluated the correlation of these measures with subjective image quality measures. They used the double stimulus impairment scale (DSIS) as a testing method and 20 naive assessors in their experiment. They examined the correlation between the MOS and each objective measure for different image compression algorithms, compression ratios, and image contents.

Bailey and Curran (2006) evaluated the strengths and weaknesses of seven steganography methods using visual inspection. The chosen methods used the least significant bit (LSB) technique in image colours to hide the secret information in Graphics Interchange Format (GIF) images. Basically, 13 assessors were provided with 18 folders and each folder contained 6 images (one was stego

image while the other 5 were original images) and asked to identify the stego image within each folder.

In respect of watermarked images, Marini et al. (2007) claim that there is not a sufficient attention devoted for assessing their quality of watermarked images. Furthermore, the PSNR and MSE are neither suitable nor reliable to assess the visual impairment present in an image, since these statistical differences do not represent visual impairment. They used subjective experiments to evaluate the invisibility of many watermarking algorithms and suggested the use of double stimulus impairment scale (DSIS) method since there is no standard method for watermarking.

Since the quality evaluation of still images is different from the quality evaluation of moving images described in the ITU standard (ITU-R-BT.500-11, 2002), Simone et al. (2009) developed a subjective evaluation method for still images. The proposed method is a modified version of the double stimulus continuous quality scale (DSCQS) method. In this method, images are shown simultaneously in each presentation and the assessor has no time limit to evaluate the quality of each image. Moreover, the assessor is asked to detect the impaired image in each pair and assess its quality only instead of assessing the quality of both images.

Almohammad et al (2010) investigated the reliability of four steganography methods with five different grayscale images (4 methods x 5 images) with both subjective and objective image quality measurements. They adapted the double stimulus continuous quality scale (DSCQS) method and 20 naive assessors in their experiment. Therefore, they examined the correlation between the MOS and the objective measure for the different stego images. They concluded that subjective evaluation is the most reliable method to measure the image quality, especially in digital image steganography.

## **2.7 Steganographic Systems Evaluation**

The amount of hidden information and the difficulty of detection of stego files are the most important aspects of any steganographic system. Thus, measuring these two aspects will determine the superiority of a steganographic technique over another. Since the product of the proposed solution depends on image steganographic techniques, image steganography evaluation criteria should be defined. To this end, Wang and Wang (2004) identified security (the hidden contents must be invisible both perceptually and statistically), payload capacity, and robustness against image manipulation attacks as the three key requirements of an image steganography algorithm.

### **2.7.1 Security or Imperceptibility**

The imperceptibility of the embedded information is the first and foremost requirement, since the strength of image steganography lies in the ability to be unnoticed by the human eye. Thus, imperceptibility in steganographic system means that the hidden information cannot be perceived by the human visual system or other statistical means. An attacker can make use of statistical anomalies to prove that a secret communication is taking place (Cox et al., 2008). Therefore, the hidden message must not disturb the visual perception or the statistical property of a cover file to avoid any suspicions of the attacker . In other words, a steganographic system is considered secure if the statistics of the cover the stego files are identical. Despite this fact, hiding secret information in a cover may introduce some noise or cause statistical anomalies (Venkatraman et al., 2004). However, it is essential that the introduced noise must not degrade the perceived quality of the stego object in order to get a secure steganographic system.

## **2.7.2 Payload Capacity**

Payload capacity is the maximum number of bits that can be embedded in a digital image without visible image distortion or detection by an adversary. The amount of hidden information relative to the size of the cover image is defined as embedding rate or hiding capacity (Venkatraman et al., 2004). However, developing a steganography technique should take into consideration the amount of data that can be hidden in a given cover file without affecting the properties of stego files.

## **2.7.3 Robustness**

Robustness is a key requirement in a fingerprint system especially if a deliberate manipulation or modification is done to the marked file. Therefore, fingerprint systems that can stand and survive against all kinds of attacks are called robust systems. The design of most steganographic systems, however, does not consider robustness as a fundamental requirement, since the majority of these systems assume the passive warden scenario (Cox et al., 2008). Hence, steganographic systems are either not robust against modifications or have limited robustness against technical modifications such as compression, format conversion, or digital-to-analogue conversion. Fingerprint systems, on the other hand must be robust and resist any kind of transformations or manipulations that may attempt to remove the fingerprint mark.

In image steganography, two fundamental aspects: payload capacity and imperceptibility are at odds with each other, since it is quite challenging to increase the payload capacity while maintaining the stego image quality (imperceptibility). This is due to the amount of artefacts introduced to the cover file from the embedding process. Therefore, a trade-off between these two fundamental aspects is needed to achieve a secure system (Venkatraman et al., 2004). Since the strength of image steganography lies in its ability to remain unnoticed by the human eye, the visual difference between the cover and the stego



image must be perfectly imperceptible for the human visual system. Therefore, evaluating the quality of stego images is a significant measure to evaluate the performance of image steganography techniques (Wu and Hwang, 2007).

After this discussion on different information hiding evaluation requirements, it is time to discuss the biggest concern in the field of steganography called steganalysis which is the counter technology of steganography (Wang and Wang, 2004). In the information hiding field, watermarking has received more attention from researchers and multimedia product vendors due to the increased interest in copyright protection. However, more recently, computer specialists and security researchers have recognised that steganography might become a threat to the security of the worldwide information infrastructure if it was misused (Kovacich and Jones, 2002). For instance, steganography could enable terrorists to communicate secretly without law enforcement agencies having any knowledge of their communication. Due to this threat, researchers have actively tried and succeeded in finding flaws in the existing steganographic systems. Thus, the next section will discuss the major techniques of steganalysis.

## **2.8 Steganalysis**

Steganalysis is the practice of detecting the presence of messages that have been hidden using steganography. The increasing numbers of steganography techniques have motivated steganalysis research. Basically, most steganographic techniques leave behind (in the stego file) some detectable traces, even though these traces are imperceptible by humans. Technically, modifying some parts of a cover file changes the properties or degrades the quality of this file. Thus, this could indicate that there is a hidden message within this stego file (Provos and Honeyman, 2003). Steganalysis involves two major techniques: visual analysis and statistical analysis. Visual analysis tries to reveal the presence of hidden data through inspection either with the naked eye or with the assistance of a computer. Statistical analysis, on the other hand, attempts to reveal tiny alterations in a stego

file's statistical characteristics caused by steganographic embedding (Wang and Wang, 2004).

In the Prisoner's Problem, steganalysis is the job of the Warden. Wendy classifies covers as they are passed on via the insecure channel (herself). If she suspects any hidden communication, her reaction towards the cover can be associated with a variety of categories such as: active, passive and malicious.

### **2.8.1 Passive Warden**

A passive warden inspects the cover file, attempting to determine by observation alone, whether or not a hidden message is present. Passive wardens will often use statistical analysis in an effort to ascertain the presence of a message. The only action a passive warden can perform is to prevent or permit the message delivery. Most steganography techniques consider the passive warden scenario in which the warden does not interfere with the stego file in any way. Therefore, most steganography research is concerned with such scenarios (Cox et al., 2008).

### **2.8.2 Active Warden**

An active warden will not only attempt to determine the presence of a message, but also perform slight modifications of any intercepted messages. In the case of Linguistic steganography, an active warden will rephrase passages and exploit synonyms in intercepted communication. Thus the active warden can alter the stego files and introduce distortion in order to destroy any secret message that might be present (Cox et al., 2008). On the other hand, many steganography applications such as watermarking and fingerprinting publicly reveal the existence of hidden information in some files (Cachin, 1998). Thus, watermarking and fingerprinting techniques consider the active warden scenario in which the warden interferes with the stego file in one way or another.

### **2.8.3 Malicious Warden**

A malicious warden will attempt to catch the prisoners communicating, often by modifying large portions of the container or even by fabricating entire messages by impersonating one of the prisoners. In such attacks, the warden can pass his own message to a specific communication partner as if it is sent by the other partner hoping for a reply to gain more information. However, this attack is the most difficult and rare among all three main attacks discussed, since the attacker here needs to know the stego key shared between the communicating parties (Cox et al., 2008).



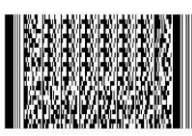

## **2.9 Barcode**

A barcode (binary image) is an optical machine readable representation of data, which shows data about the object to which it is attached. Barcodes have become very common for unique identification (UID) of almost everything from groceries to expensive goods. A Barcode represents data by varying the widths and spacing of parallel lines, and initially were linear or one-dimensional (1D). Later, they evolved into rectangles, dots, hexagons and other geometric patterns, which are referred to as matrix or bi-dimensional (2D) codes. Although 2D systems use a variety of symbols, they are generally referred to as barcodes as well. The mapping between messages and barcodes is called a symbology. The specification of a symbology includes the encoding of the single digits/characters of the message, the start and stop markers into bars and space, the size of the quiet zone required before and after the barcode, as well as the computation of a checksum. Barcodes were originally scanned by special optical scanners called barcode readers; later, scanners and interpretive software became available on devices including desktop computers and Smartphones (Pavlidis, 2000).

### 2.9.1 Two dimensional (2D) barcodes

Many different 2D symbols have been developed and they are competing to gain a dominant relevance in different applications. The barcode symbology refers to the protocol that defines the standard for arranging the bars and spaces that comprise a particular type of barcode, such as Universal Product Code (UPC) and European Article Number (EAN) renamed to International Article Number even though the abbreviation is still EAN. There are four widely known 2D barcodes, which also form the focus of ISO standards displayed in Table 2-5.

**Table 2-5: Four Widely Known 2D Barcodes**

			
Maxi Code	Data Matrix	PDF417	QR Code

Though each 2D symbol has its own morphological structure, different symbols may be grouped in three main classes (Ouaviani et al, 1999).

1. Multi-row (or stack) code, in which a set of linear barcodes are stacked together in a single, multi-row symbols. A typical example is the PDF417
2. 2D codes with a locating target, in which a special pattern is used to locate the symbols against a complex or unknown background. Two typical examples are the Maxi Code and the QR Code.
3. 2D codes without a locating target, in which the locating must exploit the internal structure of the code itself. A typical example is the Data Matrix.

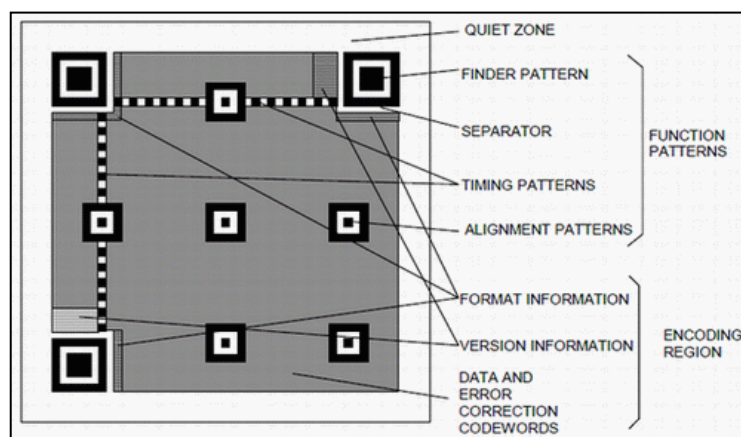
The QR code, Maxi code, Data matrix code, and PDF417 are widely implemented in daily life and they are described below:-

- 1) **Maxi Code:** is a fixed length matrix-type code developed in 1989 to enhance the internal logistics management such as automated package sorting and efficient customer services by the US courier company, United Parcel Service (UPS). Maxi Code is an open system; as such, it is available to the general public for use and/or modification from its original design. It can carry any of the 256 ASCII characters and holds up to a maximum 93 characters or 135 numeric characters per symbol. The symbol is composed of a central bulls-eye locator and offset rows of hexagonal elements. The dimensions of the symbol are approximately 1.11 x 1.054 inches (ISO/IEC 16023, 2000).
- 2) **Data Matrix:** is a 2D barcode which uses a dot matrix printer to print black and white elements representing 1 and 0, respectively, thus forming data patterns. The symbol is a square object that can range from 0.001 inch per side up to 14 inches per side. Data Matrix can carry any of the 256 ASCII characters. Its density storage depends on the symbol size. For example, 500 numeric characters can be encoded in a 1-inch square or 500 ASCII characters can be encoded in a 1.4-inch square (ISO/IEC 16022, 2006).
- 3) **PDF417:** is a 2D barcode composed of a combination of four bars. The rectangular shape symbol can be adjusted by setting the width and allowing the height to grow with the data. PDF417 can store up to 1,800 ASCII characters or 1,100 binary characters per symbol; it can encode large amounts of data into several PDF-417 symbols which are logically linked (ISO/IEC 15438, 2006).
- 4) **QR Code (Quick Response Code):** is a 2D barcode composed of a black square pattern on a white background; it has three main squares in the bottom left, top left, and top right corners that are locator

patterns. QR Codes were developed in Japan by the Nippondenso Company. The data density storage is determined by the QR code's version number (from 1 to 40). This indicates the number of rows and columns that the QR Code can use. It can grow in increments of 4 cells per side from 21x21 cells in version 1 to 177x177 cells in version 40. The symbol can encode up to 7,089 numeric characters, 4,296 alphanumeric characters, or 2,953 bytes (ISO/IEC, 2000).

## 2.9.2 QR Code

A QR code has six features: high capacity encoding of data, small printout size, Chinese/Japanese (kanji and kana) capability, dirt and damage resistance, readable from any direction in 360° and a structure append feature. Moreover, its capacity can encode 7089 numeric characters. Each QR code symbol is constructed by nominal square modules set out in a regular square array and must consist of an encoding region and functional patterns called finder, separator, timing patterns, and alignment patterns. Function patterns should not be used for the encoding of data. The symbol has to be surrounded on all four sides by a quiet zone border. Figure 2-8 illustrates the structure of a QR code symbol specification (Japanese Industrial Standards, 2004).



**Figure 2-8: Structure of a QR Code Symbol Specification (Japanese Industrial Standards, 2004))**

Table 2-6 shows the main specification of the QR code. There are four modes available, (1) number mode, (2) alphanumeric mode, (3) 8-bit byte mode, and (4) kanji and kana characters mode, combinations of these modes are also possible. The RS (Reed Solomon) error correction code is used for recovering from dirty or transmission error. There are four levels of error correction capability, L: about 7 percent error recovery, M: about 15 percent error recovery, Q: about 20 percent error recovery and H: about 30 percent recovery (Soo, 2008).

**Table 2-6: Main QR Code Specification**

Item	Specifications	
Error correcting code	RS code	Data
	BCH code	Formation information Version information
Characters	Number	10 bits coding per 3 number digits
	Alphanumeric	11 bits coding per 2 characters
	8 bit byte	8 bits coding
	kanji	13 bits coding per 2 characters
Version	1	21 X 21 modules
	2	25 X 25 modules
	40	177 X 177 modules
Error correcting level	L	About 7%
	M	About 15%
	Q	About 25%
	H	About 30%
Finder Pattern	1:1:3:1:1	3 concentric squares
		7X7.5X5. 3X3 modules
Alignment Pattern	1:1:1:1:1	3 concentric squares
		Higher version 2
		5X5. 3X3.1X1 modules

### 2.9.3 Related Work For Using QR code in Information Hiding

Naderahmadian and Khayat (2010) proposed a watermark for images in the DWT transform domain, which employs QR decomposition and uses the R matrix to embed a watermark in the LL frequency sub-band coefficients. Their experimental results demonstrated that their scheme can achieve low computational complexity and good robustness against some image processing operations such as cropping and noise pollution attacks.

In related work, Vongpradhip and Rungrangsilp (2011) proposed the embedding of QR code (carrying secret information) using discrete cosine transform into the middle frequency band using a pseudo random number sequence (PNRSR) technique which acts as an invisible watermark.

Hsu et al (2012) proposed a reversible watermarking method, which embeds QR code into grey-scale image to create a visible watermarking by embedding black and white binary images into the target image. The embedding method changes the pixel values by adding positive random values so that the resultant visible QR marked image could be scanned by a mobile phone. Afterwards, the QR code information is hidden into grey images by a reversible steganographic method that can successfully recover the original image when extracted.

Chen and Zhu (2012) utilise QR factorization and discrete cosine transform (DCT) techniques through which a meaningful watermark image is embedded into another image by modifying its stable features with a quantization index modulation (QIM) method. The combination of QR factorization, DCT, and QIM techniques guarantees the robustness of the algorithm against common signal processing operations and lossy compressions, such as filtering, noise addition, scaling, sharpening, rotation, cropping, and JPEG/JPEG2000 compression.

Later, Lin et al (2013) designed a secret hiding scheme utilising QR code error correction capability. The proposed scheme can provide the secret hiding



mechanism to embed the secret message into the QR code directly. Moreover, the secret payload is adjustable according to the QR version (1 to 40) and error correction level (L, M, Q, H), preserving the readability of the QR content.

## **2.10 Summary**

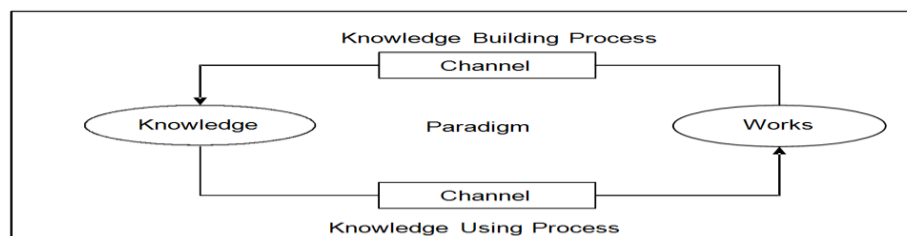
This chapter presented an overview of the main principles concerning digital steganography. The key steganography techniques and methods have been explained to establish a clear background about the proposed methods in the literature, such as spatial and transform domain methods. An in depth discussion and critical analyses on text watermarking and image steganography has been provided. This chapter has also introduced the different technologies in the information hiding discipline which are closely related to steganography, such as watermarking and fingerprinting. It covered issues related to attacks against steganography and steganalysis. Furthermore, the main aspects of evaluating a steganographic system in order to measure its efficiency have been identified. Image quality evaluation methods were presented, which includes the objective and the subjective methods. The chapter ends by discussing barcode, which is a vital component in the proposed framework.

The upcoming chapter – the research methodology – explains the formal research approach adopted for the primary research based on the ideas learned in Chapter 2.

## Chapter 3: Research Design and Proposed Framework

### 3.1 Overview

Research, according to Kuhn (1996), is defined as an activity that contributes to the understanding of a phenomenon. A phenomenon is a set of behaviours of some entities that are found interesting by a researcher or a group of researchers. Understanding means validating the knowledge that allows prediction of the behaviour of some aspects of the phenomenon. Thus, research must lead to contribution of knowledge which is validated by a research community through publications. In other words, research methods or techniques are a set of activities which a research community considers appropriate to the production of understanding (knowledge). “Knowledge is generated and accumulated through action. Doing something and judging the results is the general model” (Owen, 1997). Owen presented a general model for generating and accumulating knowledge (Figure 3-1). The process is illustrated as a cycle where knowledge is used to create works, and works are appraised to build knowledge. The channels in Figure 3-1 represent the guidelines – “ways of knowing” – under which the discipline operates and are products of its evolution.



**Figure 3-1: A General Model for Generating and Accumulating Knowledge (Owen, 1997)**

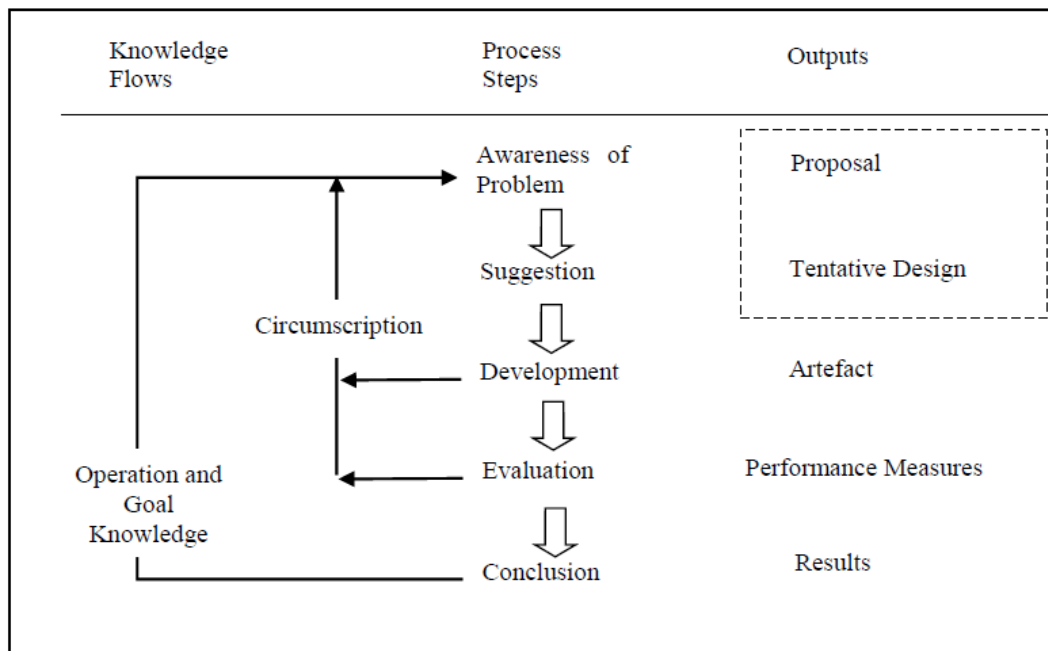
At an intellectual level, one should be able to distinguish between “natural science” and “science of artificial”. The natural science is the understanding of reality, producing general theoretical knowledge derived from nature, and includes theorising and justifying classes of things or phenomena by explaining how they behave and interact with each other. The science of artificial, on the other hand, deals with solving problems and production. It applies knowledge to create effective artefacts derived from engineering. It includes development and evaluation to meet certain desired goals. It could be defined as the creation of missing knowledge for a problem solving paradigm.

### **3.2 Design Science Research**

Design Science research (DSR) is primarily a problem solving paradigm where a set of analytical techniques and perspectives assist in performing research in the area of information systems and computing (Hevner et al., 2004). It could also be defined as “learning through building- artefact construction”. Design Science Research involves the design of artefacts characterised as novel, innovative, and purposeful and the analysis of the performance of such creation, in order to understand and enhance the behaviour of certain aspects in information systems (Vaishnavi and Kuechler, 2009). In principle, when artefacts are portrayed as purposeful, this implies that these artefacts would potentially provide organisations and humans with recognisable utility since they should address unsolved problems (Hevner et al., 2004), or provide a better solution that enhances existing practices (Vaishnavi and Kuechler, 2009). Hence, the introduction of these novel artefacts could enhance the human lifestyle and change the ways that organisations do business as a result of the opportunities emerging from these artefacts.

Vaishnavi and Kuechler (2009) have formulated a model through which work with Design Science can commence. The model describes a process starting with an *Awareness of a Problem*. Then *Suggestions* for the solutions to the problem are drawn from existing knowledge, followed by an attempt to implement an artefact

based on the suggested solution (called the *Development* phase). Afterwards, an *Evaluation* of the implementations is made, and finally, a *Conclusion* indicates that the design project is finished by deciding that the results are “good enough”, and by summarising the contributions of the artefact. The phases: development, evaluation, and further suggestions are iteratively performed until the results are “good enough”. The Design Science Model is illustrated in Figure 3-2, followed by a description of each of the five phases of the Design Science Research.



**Figure 3-2: The General Methodology of DSR (Vaishnavi and Kuechler, 2009)**

**Awareness of Problem:** The knowledge building of an interesting problem could be constructed from multiple sources. These sources could be read in an allied discipline, new developments in industry or in a reference discipline. Consequently, this provides the opportunity for the application of new findings to the researcher’s field. The outcome of this phase is a proposal, formal or informal, for a new research effort.

**Suggestion:** This phase comes immediately after the proposal. The outcome of this phase is a tentative design that is intimately connected with the proposal.

**Development:** The tentative design is implemented in this phase to construct an artefact, where the novelty is mainly in the design, not the construction of the artefact.

**Evaluation:** Once constructed, the artefact is evaluated according to the criteria that are always implicit and frequently made explicit in the proposal (in the Awareness of Problem phase).

**Conclusion:** This is the final phase of the research cycle or a specific research effort. The research effort's resultant artefact is considered satisfactory "good enough", even if there are still deviations in the behaviour of the artefact from the hypothetical predictions. The results of the effort are consolidated and written up at this phase, and the knowledge gained in the effort is frequently classified as "firm facts" that have been learned and can be constantly applied, or behaviour that can be constantly invoked. Otherwise, the knowledge gained in the effort is categorised as "loose ends" or anomalous behaviour that requires explanation which might provide the subject for further research.

### **3.3 Design Science Research Methodology**

Copyright protection and authentication of information has become necessary with the dawn of the internet communication technologies such as, digital libraries and smart phones etc. The ease of dissemination and reproduction of digital contents has made it difficult to protect their copyright. Threats to electronic publishing, such as illegal copying and redistribution of copyrighted material, plagiarism, digital counterfeiting and other forms of violations of copyrights had to be dealt with. Our research aims at producing an artefact in the form of a framework to provide copyright protection and authentication of digital documents against copyright violations. The aim of this research is highly consistent with the general aim of DSR, since the main aim is to change a current situation related to organisational or social systems into a more desirable one through the development of novel artefacts (Hevner et al., 2004). Hence, we argue

that DSR is highly fitting in the context of this research. By referring to Vaishnavi and Kuechler's (2009) model, each of the first four phases of the design science research related to this research is discussed in the next four subsections.

### **3.3.1 Awareness of Problem**

We followed a library research in which a comprehensive literature review was constructed in Chapter 2. The reason behind this research is to comprehend an evaluation criteria and an existing solution that are relevant for the domain of digital multimedia protection. The two main evaluation criteria identified for digital multimedia protection were authenticity and integrity. Furthermore, our comprehensive literature review revealed that copyright protection for images, audio, and video has been duly taken into account by researchers; while the amount of work to protect the text – the most common medium presenting human comprehension – is inadequate. To elaborate, most of the proposed mechanisms to protect digital documents containing textual contents rely on digital signature and digital watermarking solutions. Digital signature solutions are based on encryption techniques. This requires a system to manage key exchange and in most cases a third party is needed to manage certificates and public/private key generations. Moreover, if public key availability is disturbed or the private key is lost/stolen, the digital signature is no longer secured and signature authentication is no longer assured. In watermark solutions, most of the techniques and methods used to protect text are dependent on the format and structure of text which can be easily defeated by a simple rewriting attack. The rewriting attack does not need a professional to do it because it is trivial to edit the font or spacing within a document, as mentioned earlier in Chapter 2.

The reason behind the inadequacy of the amount of work required to protect the text is that encoding secret messages in text can be a very challenging task because text files have a very small amount of redundant data to be replaced with a secret message (Katzenbeisser and Petitcolas, 2000). Additionally, the embedding task requires user interaction and cannot be automated. Moreover,

many problems of modern multimedia management (content filtering, content retrieval/ search, and content tagging) and multimedia security (copyright protection, broadcast monitoring, etc.) require efficient tools providing content identification. Thus, an alternative automated mechanism is required to provide an efficient content identification and guarantee the authenticity and integrity of a digital document.

### **3.3.2 Suggestion**

We propose a method called Text key-print which aims to protect digital documents' authenticity and integrity against alteration and tampering by generating a text digital fingerprint. The Text Key-print is a novel method which protects the textual component of digital documents by operating on the basic element of the language (i.e. alphabets). By using the Text Key-Print the physical structure of a document is transformed into a logical structured relationship which asserts the position of the alphabets in order to discover any alteration in the original document, discussed in detail in Chapter 4. The outcome of this method is a dimensional matrix which is then converted into a binary stream and encapsulated with a serial number or URL (Unified Resource Locator) inside a Quick response Code (QR code) to form a digital fingerprint mark. Fingerprinting is similar to watermarking, except a different secret message is embedded in every distributed cover message. This may allow us to not only detect when theft has occurred, but also to trace the copyright violator. A typical fingerprint includes a vendor, product, or customer identification numbers.

The Awareness of Problem section has highlighted that many problems of modern multimedia management and multimedia security require efficient tools providing content identification. These days, barcodes have become very common for unique identification of almost everything from groceries to expensive goods. Consequently, the evolution of barcode technology can be utilised, namely the use of a QR code to provide a unique identification (UID) for multimedia authentication and integrity. A QR code is a binary image and most digital

documents are usually composed of textual as well as graphical representations such as logos, figures, diagrams or any digitally drawn artefacts stored into an image format. Therefore, we suggest the use of image steganography techniques to embed the digital fingerprint mark (i.e. Text Key-print and serial number or URL) in the graphical presentation of text documents as illustrated in Figure 3-3, which depicts the proposed framework.

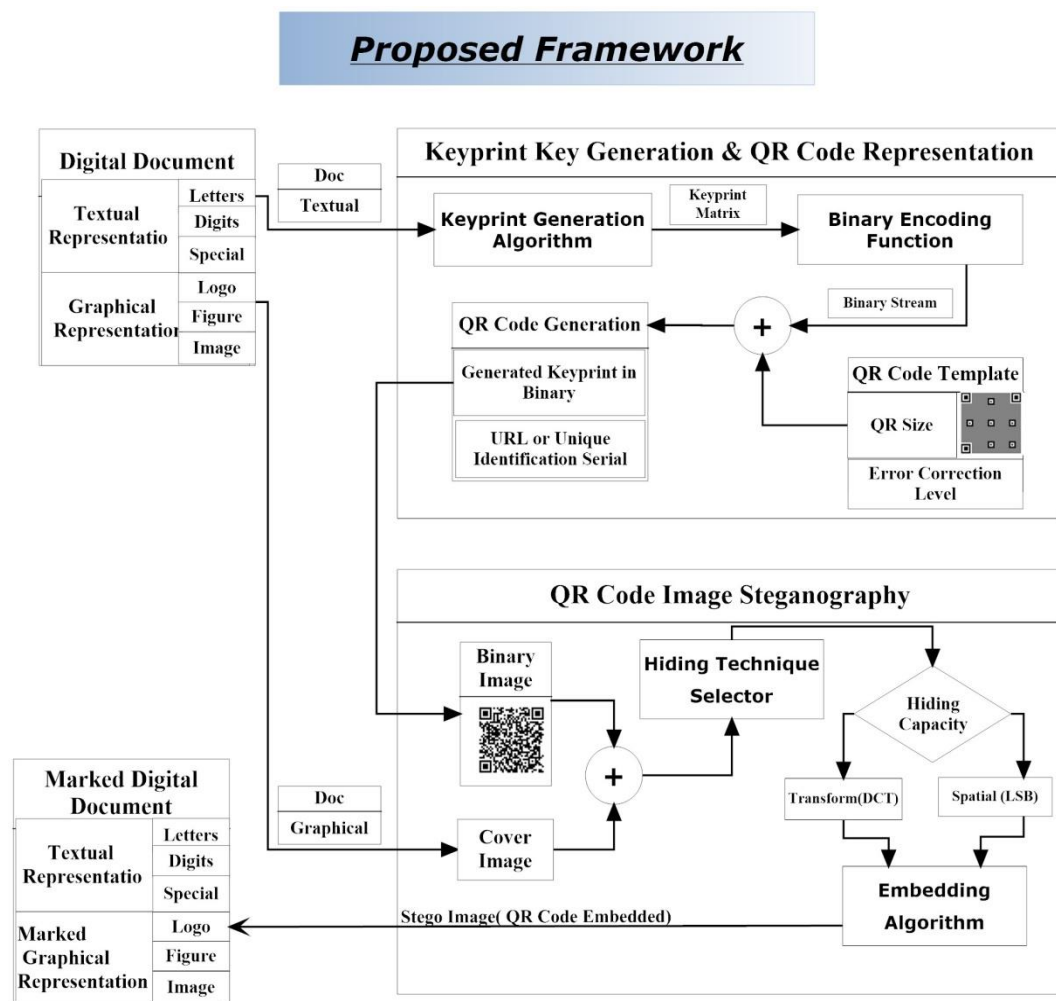


Figure 3-3: Proposed Framework



### 3.3.3 Development

The tentative design is implemented in Chapter 4. However, this implementation has raised a new problem, i.e. where to hide the QR code which is the carrier of Text key-print. The literature review revealed that steganography is an emerging field in information hiding, especially in digital images. Since digital documents contain graphical representations and some documents are stored in image format, a further literature review about image steganography was conducted to find the evaluation criteria and different hiding techniques. The three main evaluation criteria identified for steganographic systems were payload capacity, robustness and imperceptibility. Therefore, the proposed artefact was implemented to include the step of hiding the QR code – the carrier for Text key-print, into the graphical representation component of a digital document using image steganography techniques.

The two image steganography techniques were developed based upon the spatial and the transform domains as shown in Figure 3-3. In the spatial domain, three methods were proposed and implemented based on least significant bit (LSB) insertion technique and the use of a pseudorandom number generator (PRNG) to scatter the message into a set of arbitrary pixels. These methods utilise the three colour channels in RGB model based images to embed one or two or three bits per the eight bit channel, resulting in three different hiding capacities. The second technique is an adaptive approach in the transform domain where a threshold value is calculated to identify the embedding strength under a predefined location for embedding. Depending on the embedding location, the algorithm has two different hiding capacities (HC)-1 and (HC)-2. The threshold is calculated to determine which DCT coefficients to embed in.

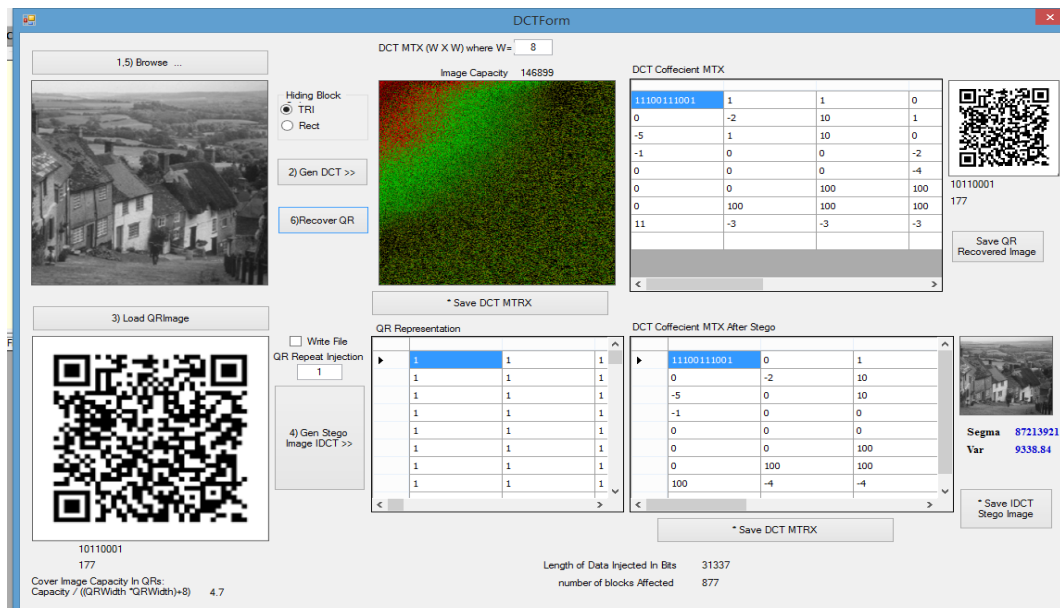
Specialised software was used to acquire the threshold value called IGOR Pro. IGOR Pro is a scientific data analysis software, numerical computing environment and programming language that run on the Windows or Mac operating system. It was originally aimed at time series analysis but it evolved to cover other applications such as curve fitting and image processing. One of its main features

is an external operations (XOP) toolkit which allows C or C++ programmers to extend its built-in-functions in order for it to perform any programming tasks. Moreover, IGOR Pro contains a full set of operations and functions for scientific image analysis applications such as image transformations and colour conversions, image filtering, threshold operation, morphological filtering, and particle analysis. Of these, the threshold operation is an important member of the level mapping class. It converts a greyscale image into a binary image. A binary image in Igor is usually stored as a wave of type unsigned byte. The threshold operation can also provide a correlation value, which is a measure of the threshold quality either by providing a specific threshold value or by allowing the operation to determine the threshold value for you. There are five methods for automatic threshold determination:

- **Iterated:** Iteration over threshold levels to maximise correlation with the original image.
- **Bimodal:** Attempts to fit a bimodal distribution to the image histogram. The threshold level is chosen between the two modal peaks.
- **Adaptive:** Calculates a threshold for every pixel based on the last 8 pixels on the same scan line. It usually gives rise to drag lines in the direction of the scan lines.
- **Fuzzy Entropy:** Considers the image as a fuzzy set of background and object pixels where every pixel may belong to a set with some probability. The algorithm obtains a threshold value by minimising the fuzziness which is calculated using Shannon's Entropy function.
- **Fuzzy Means:** Minimises a fuzziness measure that is based on the product of the probability that the pixel belongs to the object against the probability that the pixel belongs to the background.

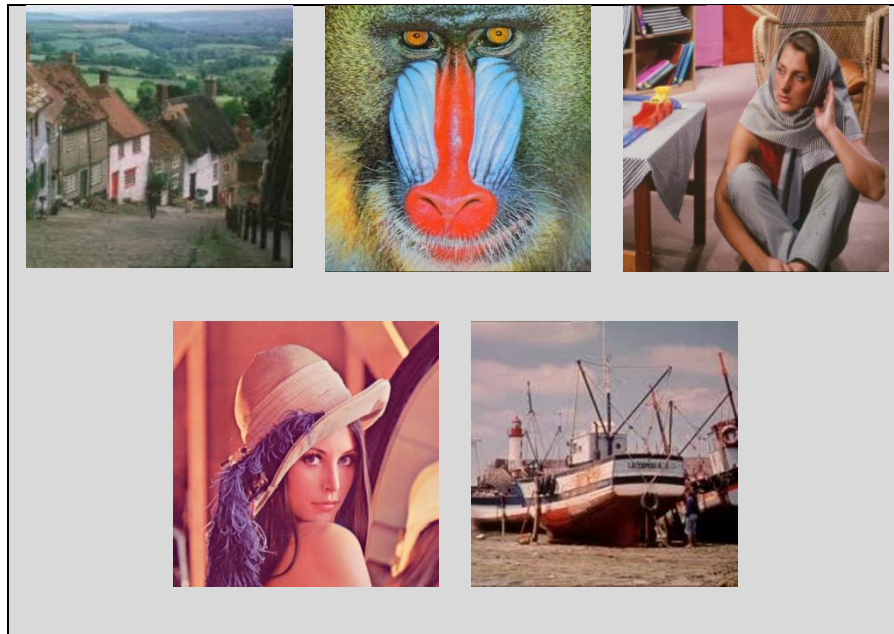
The implementation of the proposed methods was coded using Microsoft visual studio 2008. All experiments were run on a PC Pentium 4 with a processor speed

2.13 GHz and 2 GB of RAM under the Windows seven operating system. Figure 3-4 is a snapshot of our developed tool with a GUI displaying a scenario: a QR code size (a 177x177 pixels binary image) is embedded and then extracted from the Gold hill image using the proposed discrete cosine transform (DCT) technique and the 64 DCT coefficients of 8x8 pixel of a greyscale image before and after embedding.



**Figure 3-4: A Snapshot of Our Developed Tool**

Five 24 bit RGB colour image and their greyscale equivalent – Gold hills, Baboon, Barbara, Lena and Boat (Figure 3-5) – were downloaded from the internet and used as cover images for the proposed method. These images are well known and commonly used in the fields of digital image processing and image steganography (see, for instance, Chang et al., 2007; Lee and Chen, 2003; Li and Wang, 2007; Wang et al., 2002; Yu et al., 2005).



**Figure 3-5: Five 24 bit RGB Colour Images**

### 3.3.4 Evaluation

A design experiment was set to evaluate the second objective “*Investigating the impact of using QR in increasing payload capacity and its effect on quality using different steganographic techniques.*” based on the three fundamental aspects of a steganography system which are payload capacity, robustness and imperceptibility.

Payload capacity refers to the amount of secret information that can be hidden into a cover image. The payload capacity is measured for each method of hiding capacities with two different cover image pixel dimensions, namely (512x512 pixels and 256x256 pixels). Thus, 512x512 pixel dimension image was downloaded for each of the five images, and then downsampled to 256x 256 pixel dimension using Microsoft paint application. Each technique was implemented offering a different hiding capacity and producing different levels of distortion. In other words, each hiding capacity could be considered a method in its own right. These methods will be evaluated by hiding the largest QR code into testing images using objective and subjective image quality matrices to ensure the

reliability of our proposal. In meeting our objective, the largest QR code (a binary image with 177x177 pixels) was used for embedding not only once but sometimes twice to establish an understanding of the significant of the distortion when utilising the majority of the embedding capacity.

Robustness is a key requirement in a fingerprint system, especially if a deliberate manipulation or modification is done to the marked file. Fingerprint systems must be robust and able to resist any kind of transformations or manipulations that may attempt to remove the fingerprint mark. The robustness of framework is measured for each method through the successfulness of the extracting process. This aims to recover the hidden data from the stego image by reverse engineering the embedding process. The hidden data is the content displayed after scanning the extracted QR code from the stego image, using a barcode reader application installed on a Smartphone. In other words, the robustness of each method is evaluated according to the extracted QR code from the stego image. Moreover, it is a main requirement of our proposed scheme, as stated in the aim of the research: *to develop reversible steganographic scheme*.

Imperceptibility, on the other hand, means that the hidden information cannot be perceived by the human visual system or other statistical means. Evaluating the quality of the stego images used within our security scheme is a key requirement in a steganography system to ensure that it does not arouse suspicion by an attacker and thus, its success. In the literature, both objective and subjective image quality evaluation methods have been investigated and utilised for various purposes (Simone et al., 2009s). Basically, the objective methods and particularly the PSNR metric, has been tested and validated to be used with many image processing applications. Technically, PSNR measures the efficiency of a particular stego method over another in terms of imperceptibility or stego image quality. The effect of embedding on the quality of the cover image is measured using MSE and PSNR image quality metrics. The most common objective quality metric (PSNR) in the literature is used in Chapter 5 to evaluate the performance of the implemented methods. However, a visual attack is defined as the process of

detecting hidden messages in stego files through inspection by naked eye or through the assistance of a computer. Hence, subjective image quality is a must to fulfil security requirements by involving the human factor in evaluating stego image quality. Subjective assessment involves techniques that use human beings for judgment and such experiments are statistical in nature; so the subjective response will be analysed using statistical measurements to describe the score distribution across the assessors. A subjective method in Chapter 6 namely, DSCQS was used to complement the objective evaluation metric in order to guarantee the imperceptibility of our proposed images embedding schemes. In doing so, we meet our third objective: *Evaluating the reliability of proposed work by both Objective and subjective Quality Evaluation methods.*

The performance of the implemented methods is evaluated by measuring the perceived qualities of the resultant stego image of these methods subjectively. Thus, an experiment was designed in order to investigate the three evaluation criteria which are:

- 1) Which method in the subjective evaluation the participant did not identify the embedded image?
- 2) Did the participant in the subjective evaluation identify the embedded image due to the increased amount of hidden data?
- 3) What is the effect of using different cover images?

To answer these questions, an adaptive double stimulus continuous quality scale (DSCQS) method is used to perform the subjective evaluation of the implemented methods. The DSCQS method is a designed experiment where the assessor is required to observe a pair of images one of which is the original image (reference) and the other is the image under test. The series of presentations are internally random and randomly presented; accordingly, each presentation or pair of images consists of one unimpaired (reference) image while the other one may or may not contain impairments. Then the assessors are asked to evaluate the quality of both images without being informed if the image is referenced or not, since the position of the reference image is changed randomly (ITU-R-BT.500-11, 2002).

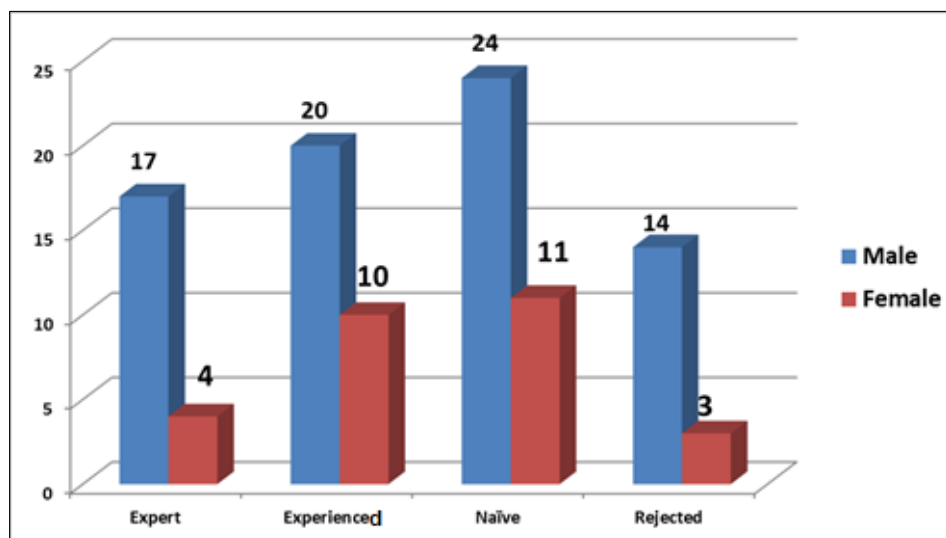
This method was developed by Simone et al. (2009). Thus, a subjective evaluation method for still images was derived from the quality evaluation of moving images described in the ITU standard (ITU-R-BT.500-11, 2002), due to lack of standardisation for still images evaluation. Building on their work, we modified their method within the ITU standard to achieve more accurate results. Drawing from the ITU standard, four main factors should be considered in the methodology for subjective assessment of image quality in this experiment, as stated earlier in Chapter 2: 1) assessor, 2) stimuli, 3) scaling and comparisons, and 4) evaluation tasks.

The assessor is the person taking part in a quality evaluation test and classified into three categories (naïve, experienced, and expert). Two yes and no questions were displayed in the stimuli in order to be able to classify the participants in this evaluation test. The two questions are 1) have you taken any academic course related to image processing?, and 2) have you published any academic papers related to image processing? If both answers are yes, then the participant is considered an expert. If both answers are no, then the participant is considered naïve while the participant is considered experienced if he/she took an academic course but did not publish any academic papers related to image processing. Moreover, it has been stated in (ITU-R-BT.500-11, 2002) that “Prior to a session, the observers should be screened for normal visual acuity on the Snellen or Landolt chart, and for normal colour vision using specially selected charts (Ishihara, for instance)”. Therefore, the Snellen Eye Chart was used to test vision acuity and the Ishihara test was used to check the colour blindness in fulfilment to the guidelines described in the ITU standard.

A Snowball sampling technique was used to recruit participants for the study. Snowball sampling relies on a small number of initial informants to nominate other participants through their social networks. These participants would need to meet a set of criteria and a specific set of skills that would potentially contribute to the paradigm under study. The term snowball sampling is derived from the notion of a snowball rolling and increasing in size as it collects more snow. This is a

metaphor to indicate that the more relationships built through mutual association, the more connections that can be made to recruit more participants (Patton, 2002). Prior to starting the recruitment process, an Ethical approval was obtained from the Ethics Committees at Brunel University in London, England and Thebes Academy in Cairo, Egypt.

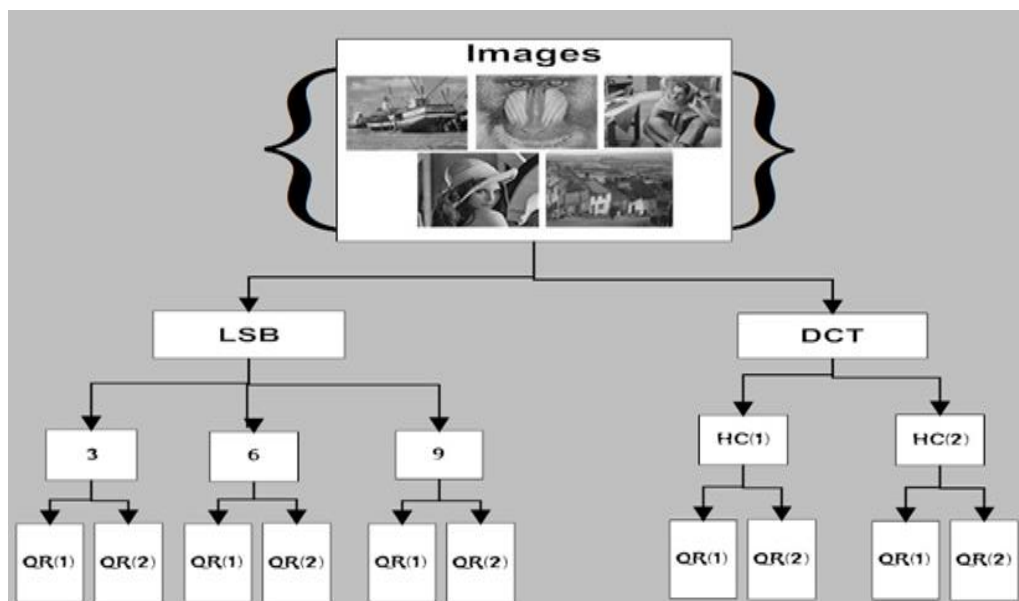
The study took place at Brunel University and Thebes Academy, where 103 assessors, mostly students and academic staff, participated in this experiment after being screened for correct visual acuity and colour vision using Snellen charts and Ishiara charts, respectively. The age of the participants ranged from 20 to 55 years old. The average time of each experiment session was 25.37 minutes per participant while the maximum and minimum times were 32.35 and 12.48 minutes, respectively. 17 assessors' results were rejected because they left without completing the whole test or their test results contained deficiencies. Thus the remaining 86 assessors were classified into expert, experienced and naïve according to their answers to the two questions displayed earlier in the stimuli. Figure 3-6 shows the categorisation of the participants who took part in the subjective test, 29% of whom were female.



**Figure 3-6: The Categorisation of Participants**



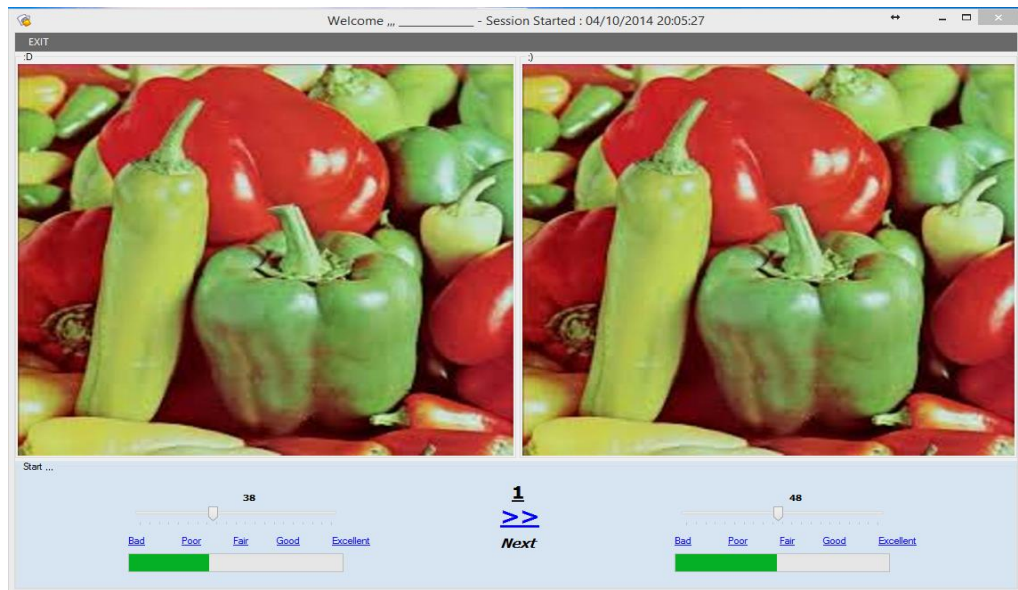
The stimuli are the tested materials presented to the participant during the study, and are characterised by content and treatment. The content is a sequence of images where the treatment is generated. Treatment represents the independent variables which are the implemented methods in this thesis and the five different cover images (five colour images and their greyscale versions) used in the experiment namely: Baboon, Barbara, Boat, Gold-Hills and Lena. The stimuli contain a series of presentations which are internally random and randomly presented; accordingly, each presentation or pair of images consists of one unimpaired (reference) image, while the other one contains impairments. In this experiment, each method in Chapter 5 is tested with five different images (512x512 pixel dimension image) and two different payload hiding information either with one QR code or 2xQR codes. This results in 10 different stego images for each method; this adds up to 50 impaired images displayed with their unimpaired image for five methods in the stimuli, as illustrated in Figure 3-7.



**Figure 3-7: Five Methods Used to Generate the Test Sample**

At the beginning of the evaluation session, oral instructions were provided by the researcher to explain the task, and a viewing session was performed to allow the subject to be familiarised with the assessment procedure. Moreover, assessors were introduced with two dummy presentations to familiarise him/her with the

grading scale, evaluation process and the graphical user interface (GUI) in Figure 3-8. The example the image used (Peppers) is not from the actual evaluated set of images; therefore, the obtained results are not considered. The collection of the evaluation scores was stored electronically into a Microsoft Access database linked to the application presenting the subjective test.



**Figure 3-8: The GUI for DSCQS Method**

The name of the adopted method (double stimulus continuous quality scale) explains the scaling and the comparisons used in the quality evaluation research. Double stimulus studies are used for pair-wise comparisons between two stimuli (explained in the previous paragraph). The scale used in measurement is continuous ranging from 0 to 100 as follows: Excellent (100-80), Good (79-60), Fair (59-40), Poor (39-20) and Bad (19-0). Thus, in this method, the images are shown simultaneously in each presentation and the assessor has no time limit to evaluate the quality of each image. Afterwards, the difference between these two scores (reference image and test image) is calculated. The scores obtained, however, should not be treated as absolute scores (Simone et al., 2009).

According to the ITU standard, the evaluation task is defined as an effective measurement if an overall quality evaluation uses heterogeneous stimuli material

to build up the global or holistic judgment of quality. It is assumed that both stimuli-driven sensorial processing and high-level cognitive processing including knowledge, expectations, emotions and attitudes are integrated into the final quality perception of stimuli. However, the evaluation process of the obtained subjective results is interpreted as follows. For each slide presentation the assigned value for the reference image is divided by the assigned value of stego image. The output of this division will be assigned the value Y and it is categorised into one of the five grades, as illustrated in Table 3-1.

**Table 3-1: Five-Grade Quality**

Quality Scale		Y Value
5	Excellent	$Y < 0.8$
4	Good	$0.8 \leq Y < 1$
3	Fair	$Y = 1$
2	Poor	$1 < Y \leq 1.2$
1	Bad	$1.2 < Y$

The value of Y is Excellent if the assessor gave a 20 percent higher quality evaluation score to the stego image than the reference image. This means that the method used to embed the QR code in the cover image produces a stego image whose perceived quality by the assessor is far higher than the actual cover image. If the assessor gave the same quality evaluation score for both the stego image and reference image, then the value of Y is fair as the assessor did not distinguish between the perceived qualities of both images. The value of Y is bad if the assessor gave a higher by more than 20 percent quality evaluation score for the reference image than the stego image. This means that the method used for embedding has resulted in a visualised distortion recognised by the assessor.

The goal of the experiment is to investigate the sensitivity of quality measures to distortions that arise from embedding into cover images. In other words, it is to find the degree to which a quality measure can discriminate the coding artefacts in

stego images and translate it into a meaningful score using a subjective method. Subjective assessment involves techniques that use human beings for judgment and such experiments are statistical in nature. Therefore, the subjective response was analysed using statistical measurements in order to describe the score distribution across the assessors for each of the test conditions (combination of five methods, five images, and two QR-codes).

Consequently, the results of the experiments present the evaluated performance of the five steganographic methods by measuring the quality of their resultant stego images with respect to their reference images. The numeric format of the results is transformed into using descriptive statistics frequency distribution in a graphic form. This allows us to visualise where the data tends to cluster, the largest and the smallest values, and the general shape of the obtained data. Moreover, several measures of dispersion, such as range, percentiles and the standard deviation are computed to describe the variation or the spread in our data set of observations. The population of the carried experiments contain three groups (naïve, experienced and expert) with different experience levels and qualifications, they cannot be treated the same. Therefore, a weighted sum was assigned to each group to distinguish their opinion score, where expert is multiplied by three, experience multiplied by two and naïve multiplied by one. The descriptive statistics will answer the first objective of the evaluation criteria which was *“Which method did the participant in the subjective evaluation identify as the embedded image?”* However, it is important to know the distribution of the data under analysis (normality of distribution) when performing statistical analysis. A sample of the collected data was analysed using the Kolmogorov-Smirnov statistic test which verified the normality of its distribution. Therefore, parametric statistics were used to analyse the collected data (Lind, Marshal, and Wathem, 2012).

In the design of the experiment, two distortion levels (QR (1) and QR (2)) were set to measure the influence of increasing the coding artefacts in stego images. Thus, a paired-sample t-test will be performed on the subjective opinions score to investigate whether the participants were capable of recognising the stego image

due to the distortion level. Furthermore, the method capability of embedding more data without being noticed was also observed. Consequently, the second evaluation criteria defined earlier in this chapter was met. The two-sample t-test starts with the assumption that the two groups are equal, the null hypothesis is usually written as  $H_0: \mu_1 = \mu_2$ ; while the alternative hypothesis  $H_A: \mu_1 \neq \mu_2$  (Lind, Marshal, and Wathem, 2012). Statistical software (SPSS) was used to conduct a paired-sample t-test and a fixed p-value corresponding to 95% confidence interval for the difference between the two means was calculated. The decision is based on whether or not the calculated p-value is below the threshold chosen (0.05) for statistical significance. If it is, then the null hypothesis is rejected in favour of the alternative hypothesis.

Another statistical test to analyse the differences between and among the three groups (naïve, experienced and expert) means and their associated procedures is analysis of variance (ANOVA). ANOVA is a statistical hypothesis testing heavily used in the analysis of experimental data to indicate whether or not the means of several groups are equal, and therefore, generalises the t-test to the three groups for statistical significance. Here, a statistical test (ANOVA) is used to determine whether the groups are actually different in the measurement of quality score given to the artefacts caused by the five steganographic methods. The null hypothesis  $H_0: \mu_1 = \mu_2 = \mu_3$  (mean values of all groups are equal) against the alternative hypothesis  $H_A: \mu_1 \neq \mu_2$  or  $\mu_1 \neq \mu_3$  or  $\mu_2 \neq \mu_3$  (mean values of at least two or more groups are not equal). The test result is based on the p-value (Lind, Marshal, and Wathem, 2012). If the test yields any p-value less than the user defined significant level (0.05) in our case, the null hypothesis will be rejected in favour of the alternative hypothesis. Otherwise, the conclusion will be that the alternative hypothesis is not confirmed.

### **3.4 Conclusion**

In this chapter, the DSR (Design Science Research) methodology was chosen and its appropriateness for this particular research was justified. The aim of this research is highly consistent with the general aim of DSR, since the main aim is to change a current situation related to organisational or social systems into a more desirable one through the development of novel artefacts. The four main processes of the DSR methodology (Awareness of Problem, Suggestion, Development and Evaluation) were explained to show how the research will be conducted in line with the DSR research process. The Awareness of Problem is the literature review in Chapter 2 which explains the knowledge building of the research problem. Suggestion is explained in this chapter which is precisely the DSR methodology that was conducted to achieve the desired outcome of the implementation of the proposed framework. The development is the implementation phase of the conducted research for the proposed framework, illustrated in depth in Chapters 4 and 5. Last but not least, the evaluation process involves measuring the efficiency of the proposed framework according to the identified evaluation criteria, mainly subjective evaluation of the outcome of the final product, explained in Chapter 6.

## **Chapter 4: Document Key-Print and QR-Code Generation**

### **4.1 Introduction**

A document is a primary form of written communication as well as record keeping in our societies. A document can be defined as a material reproduction of the author's thoughts with an objective to transmit, communicate and store his/her thoughts as accurately as possible. There are different types of documents that are exchanged and circulated in large volumes on a daily basis, such as birth certificates, identification documents, financial instruments, legal documents and many others. A few decades ago, only paper documents were used, until digital storage become more available and cheaper in cost, which facilitated the use of documents in the form of electronic files nowadays. In many applications, it is essential to verify the authenticity and integrity of a document. Authentication may involve identifying by whom, when, and where the document was created or finding out whether the content of a document was tampered with after creation. Paper authenticating techniques include the use of special paper, special inks, watermarks, barcodes, and personal signature. These techniques have evolved for authenticating electronic documents mainly into digital signature and digital watermarks. In digital signature, a hash code or a digest of the original file is usually appended to the end of the document file. In digital watermarking, a digital mark (often invisible) is embedded into a document at some selected locations, as discussed in Chapter 2.

The structure of this chapter is as follows: Section 4.2 discusses the architecture of a digital document. In Section 4.3, a proposed method to verify the authenticity and integrity of digital document called Text-Key Print is presented. Moreover, two scenarios of attack that the digital document could be subject to are presented

to evaluate the proposed method. Section 4.4 discusses the generation of fingerprint that encapsulates Text-Key print and Quick Response Code. Finally, Section 4.5 sums up the main aspects of Chapter 4.

## 4.2 Architecture of Text-Based Documents

The architecture of a document is composed of a logical and a physical structure (Arno et al, 1985), the hierarchy of a logical and a physical document structure is displayed in Figure 4-1. A document is a logical unit formalised under the construction rules derived from the syntax and semantics of a language to describe an author's comprehension in textual presentation. The information within documents is often presented in a hierarchy treelike structure having distinct levels, where each level is composed of text elements. Text elements could be paragraphs, quotations, formulas, figures or tables. For instance, a chapter is composed of a title and a number of sections. Each section has a title and subsections, which might have a title and a paragraph. A paragraph could be broken into sentences, which are formed through phrases, including words; in turn, these words are the represented in forms of letters, digits, special character or logos. Usually a predefined layout for each of the standard text elements exists which allows a document contents to be positioned on a presentation medium.

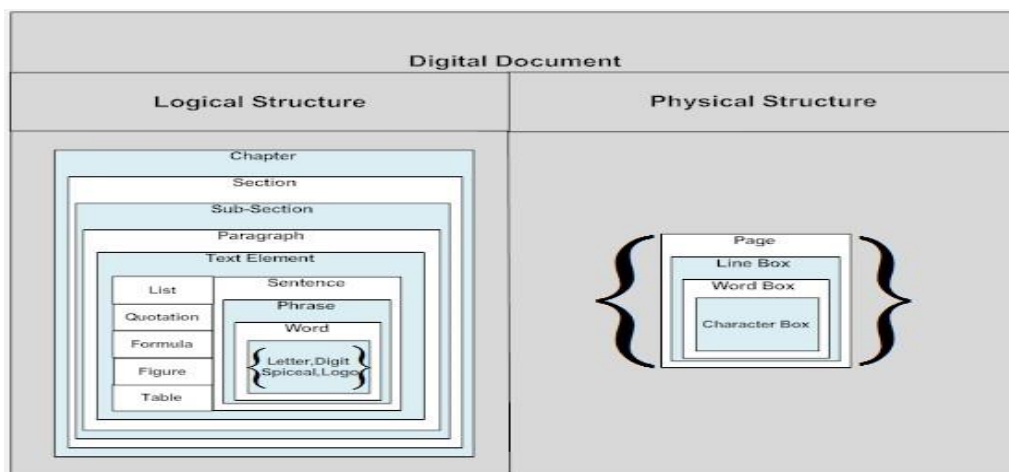


Figure 4-1: Document Logical and Physical Structure



On the other hand, the physical structure reflects the allocation of text in the presentational medium. The page forms the unit of presentation of the document contents, which is a further refined to “composite of boxes” containing text element from the logical structure. The hierarchy of these boxes starts with a line boxes encompassing word boxes, which themselves comprise character boxes. Therefore, the character presents the primitive element connecting the logical structure to the physical structure. Another factor related to the physical structure is the formatting process which is concerned with the positioning within the page and the presentation shape “style” of every basic symbol.

### **4.3 Document Key-Print Algorithm**

The Key-Print method aims to protect digital documents’ authenticity and integrity against alteration and tampering by generating a text digital fingerprint. The Text Key-print is a novel method which employs the basic element of the language (characters) to achieve the goal through the transformation of the physical structured of the document into a logical structured relationship. The logical structure asserts the position of the alphabets in the document in order to discover any alteration in the original document. The resultant dimensional matrix is then converted into a binary stream and encapsulated with a serial number or URL inside a Quick response Code (QR code) to form a digital fingerprint mark. Fingerprinting is similar to watermarking, except a different secret message is embedded in every distributed cover message. This may allow us not only to detect when theft has occurred, but also to trace the copyright violator. A typical fingerprint includes a vendor, product, or customer identification numbers.

Authentication techniques can be classified into two main types: complete data verification and content verification. In complete data verification, the authenticated data has to exactly match the original data. Changing just one bit of the original data will show the unauthenticity of the marked object. In content verification, multimedia data are authenticated based on the meaning of their contents rather than the exact match in data bits. The method presented here

belongs to content verification techniques, since our prime objective is the content within a digital document and not the way it is presented.

This section exemplifies the design and implementation of an algorithm that captures and links the content of a text based document into a matrix. The two dimensional matrix presents the content of a text document making it easy to detect any form of alteration to the original content of the text. The first dimension is the twenty-six characters of the English alphabet and space (SP). The second dimension is the relationship between the characters and their position within the text. Each character reports the number of occurrences of the consecutive character in the alphabet based on 3 dimensions presented below:

- L.C.B (Letter Count Before): counting the number of occurrences of the consecutive letter in text before the first occurrence of the current letter.
- L.C.A (Letter Count After): counting the number of occurrences of the consecutive letter in text after the first occurrence of the current letter.
- T.L.I (Total letter Index): the summation of a particular letter's positions in text.

Table 4-1 explains the relationship between a subset of the text which is 27 characters and three logical relationships. These logical relationships aim to use the subset of text to report reference points and to save the positions of characters among text. These three logical relationships use each letter to report on the next letter according to its position in the text, while TLI is a counter for the positions that the letter has occupied in text. For example:

(A, L.C.B):- counts the number of B characters occurring before the first A in text

(A, L.C.A):- counts the number of B characters occurring after the first A in text

(A, T.L.I):-  $\sum$  of the position of B characters in text

(SP, L.C.B):- counts the number of A characters occurring before the first SP in text

(SP, L.C.A):- counts the number of A characters occurring after the first SP in text

(SP, T.L.I):-  $\sum$  of the position of SP characters in text

In other words, all characters in the text are linked to each other according to their position among the text. Table 4-1, therefore, contains the relationship between the letters in the text and acts like a map for the content of a text base document.

**Table 4-1: TEXT KEY-PRINT MATRIX**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SP
L.C.B																											
L.C.A																											
T.L.I																											

The proposed algorithm for generating the Text Key-print matrix of a document is presented in Figure 4-2. Table 4-1 will be used as the original reference to the document as the 27 letters present facts about relationships between words, strings and substrings in the text. It also stores the position of the letters in text in each letter T.L.I. Any alteration to the original text content could be detected. Furthermore, it could be analysed to know what exactly has changed by using the detecting alteration algorithm, presented in Figure 4-3. We illustrate the robustness of our Text Key-Print algorithm with two scenarios featuring “Cut and Paste” attacks on text documents in the next sub-section, thus highlighting how the authenticity and the integrity of text are preserved by the Text Key-Print algorithm.

Begin:

1. Read the associated text :
  - A. Catch characters first occurrence
  - B. Catch characters positions in the associated text
  - C. Store characters first occurrence and their positions in the associated text in table

Character	A	B	C	D	E	.	.	.	.	X	Y	Z	sp
1 <sup>st</sup> occurrence													
Position													

2. Create the matrix presented Table 4.1
  - A. Start sub-iteration
  - B. Get the character and its position from the text document index
  - C. Add the character position(value) to the character T.L.I
  - D. Compare the character position to the previous alphabet stored in Table generated from 1-C:

Index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Text																						

- I. If the previous alphabet does not exist: increment L.C.A
- II. Else if less than the previous alphabet stored in Table: increment L.C.B
- III. Else: increment L.C.A

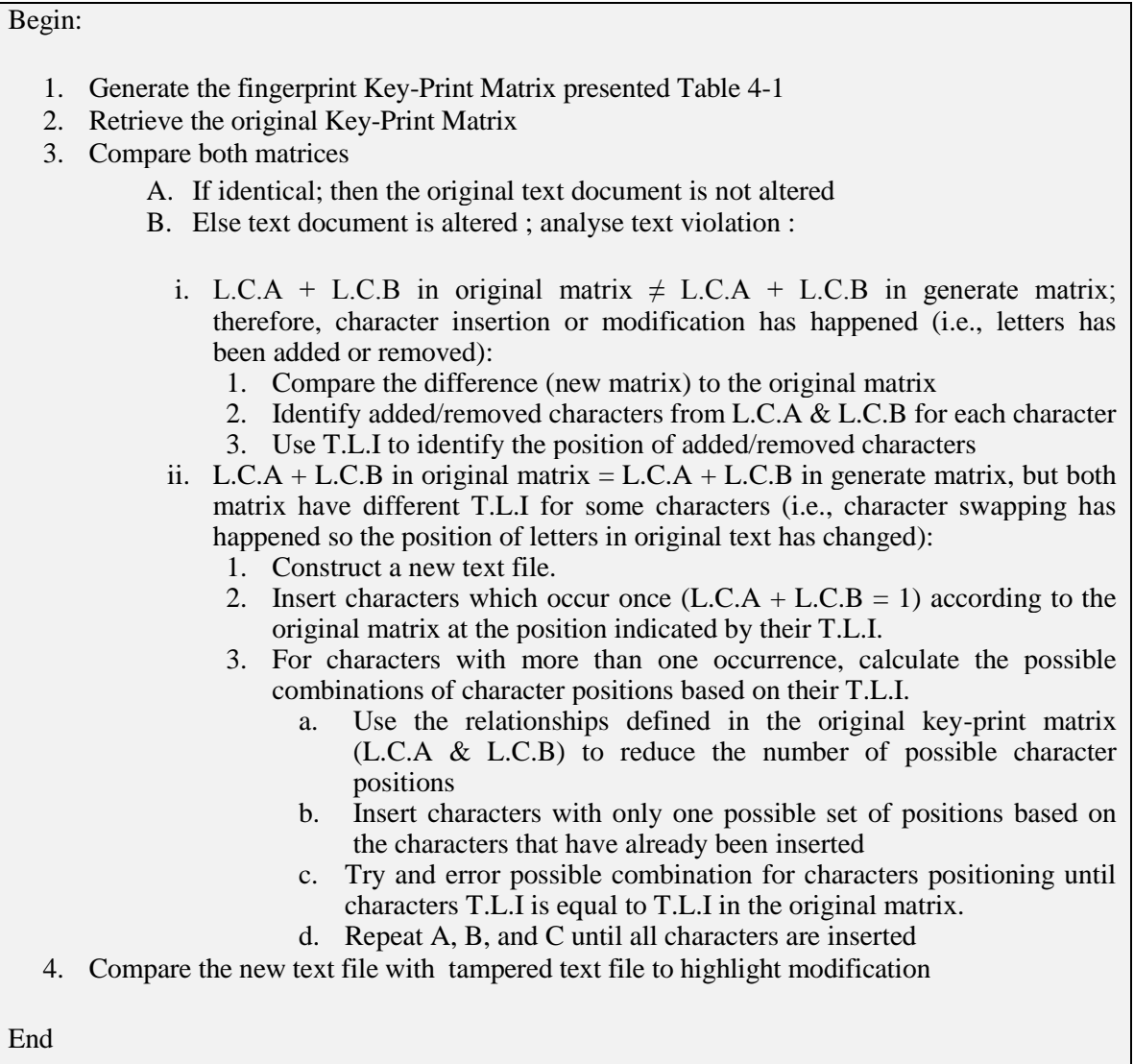
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SP
L.C.B																											
L.C.A																											
T.L.I																											

- E. Get next character and it's position from the document
- F. Check end of file
  - I. If End of file :go to 2F
  - II. Else : go to 2B
- G. End sub-iteration

3. Save Text Key-print

End

**Figure 4-2: Text Key-Print Generation Algorithm**



**Figure 4-3: Text Key-Print Detecting Alteration Algorithm**

## 4.4 Propose system verification against “Cut and Paste” attacks

This section discusses the proposed system validation process against cut and paste vulnerabilities in small and moderate size text documents such as in web pages and email attachments. For this purpose, two scenarios are proposed.

For both scenarios, assume the text index generation algorithm receives the original text “Alice lends Bob money”. This algorithm will generate the corresponding associated text index as shown in Table 4-2.

**Table 4-2: THE ASSOCIATED TEXT INDEX**

Index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Text	A	l	i	c	e		l	e	n	d	s		B	o	b		m	o	n	e	y	.

The result shown in Table 4-2 is then applied as an input to the Text Key-print algorithms mentioned in Figure 4-2; this algorithm will generate the original fingerprint matrix as follow:

- Executing steps 1-A and 1-B in Text Key-print Algorithms will process the associated text index and generates the results shown in Table 4-3.

**Table 4-3: CHARACTERS FIRST OCCURRENCE AND THEIR POSITIONS IN THE ASSOCIATED TEXT**

Character	A	B	C	D	E	I	L	M	N	O	S	Y	Sp
1 <sup>st</sup> occurrence	1	13	4	10	5	3	2	17	9	14	11	21	6
Position	1	13,15	4	10	5,8,20	3	2,7	17	9,19	14,18	11	21	6,12,16

- Executing the rest of steps in the Text Key-print algorithms generates the results shown in Table 4-4.

**Table 4-4: ORIGINAL KEY-PRINT MATRIX**

Chars	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	sp	
L-C-B	0	1	0	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
L-C-A	2	0	1	1	0	0	0	1	0	0	2	1	1	2	0	0	0	1	0	0	0	0	0	1	0	3	0	
T-L-I	28	4	10	33	0	0	0	3	0	0	9	17	28	32	0	0	0	11	0	0	0	0	0	21	0	34	1	

The interpretation of the results presented in Table 4-4 implies the following:

- character B occurred twice after the first occurrence of character A with TLI= 13+15=28
- character C occurred once before the first occurrence of character B with TLI=4

- character D occurred once after the first occurrence of character C with TLI=10
- character E occurred three times twice before and once after the first occurrence of character D with  $TLI=5+8+20=33$
- character I occurred once after the first occurrence of character H with TLI= 3
- character L occurred twice after the first occurrence of character K with TLI=9
- character M occurred once after the first occurrence of character L with TLI=17
- character N occurred once before and another after the first occurrence of character M with  $TLI=9+19=28$
- character O occurred twice after the first occurrence of character N with  $TLI= 14+18=32$
- character S occurred once after the first occurrence of character R with TLI=11
- character Y occurred once after the first occurrence of character X with TLI= 21
- character SP occurred three times after the first occurrence of character Z with  $TLI=6+16+16=34$
- character A occurred once before the first occurrence of character SP with TLI= 1 and it is the first character in the associated text

#### 4.4.1 Scenario (1): Bob lends Alice money

In this scenario, assume that the word “Bob” and “Alice have been swapped using a “Cut and Paste” attack on the original text in the base document. As a result, the text will now be “*Bob gave Alice money*”. The text index generation algorithm receives this text and generates the corresponding associated modified text index as shown in Table 4-5, which includes characters position changes.

**Table 4-5: THE ASSOCIATED TEXT INDEX**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
B	o	b		l	e	n	d	s		A	l	i	c	e		m	o	n	e	y	.

This will lead to a different understanding from the original context. The result of the attack is that Alice could be forced to pay twice. Moreover, the attack changed the liabilities, meaning Alice cannot claim back her money and might be forced to pay it again. The text Key-print proposed in this thesis can prevent such an attack. This will be illustrated in Figure 4-4 using the Key-print alteration detection algorithm Text Key-print will receive the associated text index in Table 4-5 as an input to generate the fingerprint matrix using Text Key-print algorithms in Figure 4-2. Table 4-6 presents the processed input after executing steps 1-A and 1-B in text Key-print algorithms.

**Table 4-6: CHARACTERS FIRST OCCURRENCE AND THEIR POSITIONS IN THE ASSOCIATED TEXT**

Chars	A	B	C	D	E	I	L	M	N	O	S	Y	SP
1 <sup>st</sup> occurrence	1	1	14	8	6	13	5	17	7	2	9	21	4
Position	11	1,3	14	8	6,15,20	13	5,12	17	7,19	2,18	9	21	4,10,16

Executing all steps of Text Key-print algorithms will produce the generated Key-Print matrix presented in Table 4-7, while the original Key-print matrix in Table 4-4 was kept safe, unaltered and is now retrieved correctly.

**Table 4-7: Generated Key-print Matrix**

Chars	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SP	
L-C-B	2	0	1	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
L-C-A	0	1	0	2	0	0	0	1	0	0	2	1	1	1	0	0	0	1	0	0	0	0	0	1	0	3	0	
T-L-I	4	14	8	31	0	0	0	13	0	0	17	17	26	20	0	0	0	9	0	0	0	0	0	21	0	30	11	

The interpretation of the results presented in Table 4-7 implies the following:

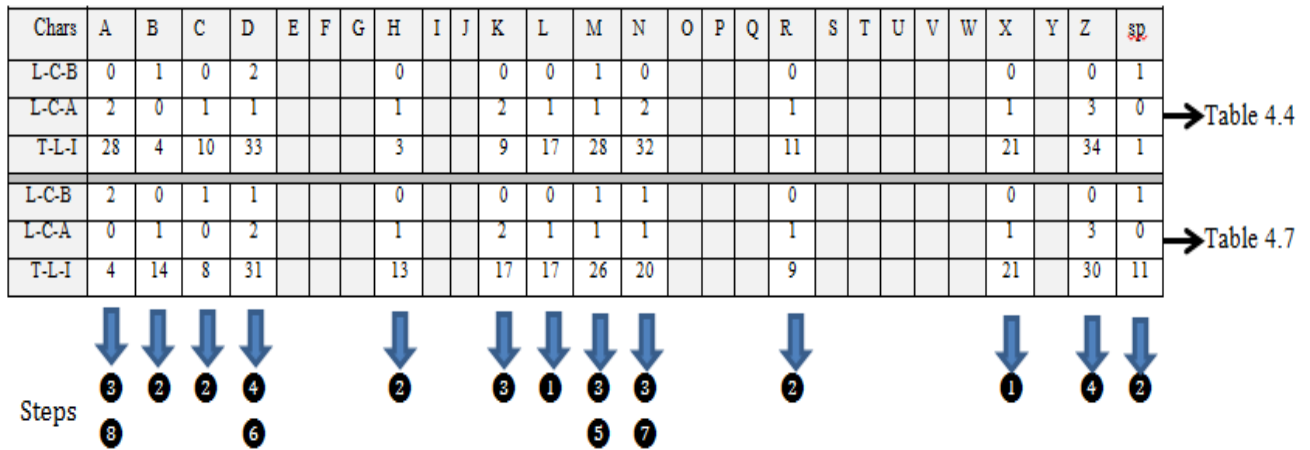
- character B occurred twice before the first occurrence of character A with TLI= 4



- character C occurred once after the first occurrence of character B with TLI=14
- character D occurred once before the first occurrence of character C with TLI=8
- character E occurred three times twice after and once before the first occurrence of character D with TLI=31
- character I occurred once after the first occurrence of character H with TLI= 13
- character L occurred twice after the first occurrence of character K with TLI=17
- character M occurred once after the first occurrence of character L with TLI=17
- character N occurred once before and another after the first occurrence of character M with TLI=26
- character O occurred twice once before and another after the first occurrence of character N with TLI= 20
- character S occurred once after the first occurrence of character R with TLI=9
- character Y occurred once after the first occurrence of character X with TLI= 21
- character SP occurred three times after the first occurrence of character Z with TLI=30
- character A occurred once before the first occurrence of character SP with TLI= 11

The difference between the matrices in Table 4-4 and 4-7 will show what happened to the original text, by analysing the changes in the two interpretations of the Key-Print. This will reveal that the characters listed in the original Key-Print are the same in the generated Key-Print but the T.L.I in the generated Key-Print is different from the original Key-Print; therefore, the position of letters in original text has changed (i.e. character swapping has happened). These changes

will be highlighted in the analysis in Figure 4-4 after executing all the steps in Figure 4-3.



**Figure 4-4: KEY-PRINT ALTERATION DETECTION ALGORITHM**

The interpretation of the results presented in Figure 4-4 implies the following:

- 1) The letters used to construct the original text is the same in the altered text
- 2) The position of some characters (T-L-I) are swapped within the text.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
B	o	b		L	e	n	d	s		A	l	i	c	e		m	o	n	e	y	.

**Steps:**

- 1 Characters that are not altered (cells in Table 4-7 that match with Table 4-4 )

- M occurred once after the first occurrence of L with TLI=17
- Y occurred once after the first occurrence of X with TLI= 21

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
																m				y	

- 2 Characters position that can be retrieved from the original fingerprint directly

- A occurred once before the first occurrence of SP with TLI= 1 and it is the first character in the associated text

- C occurred once before the first occurrence of B with TLI=4
- D occurred once after the first occurrence of C with TLI=10
- I occurred once after the first occurrence of H with TLI= 3
- S occurred once after the first occurrence of R with TLI=11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
A		i	c						d	s						m					y	

3 Characters positions from possible combinations in reconstructed text. Sets written in red face means that these combinations are not possible because of position already occupied in reconstructed text or the information retrieved from the (L-C-B or L-C-A) indicate where the position of the character should be.

- B = 28 → {20+8} or {19+9} or {16+12} or {15+13}
- L = 9 → {2+7} or {3+6} or {4+5} or {1+8}
- O = 32 → {20+12} or {19+13} or {18+14}
- N occurred once before and another after the first occurrence of M ( at position 17) with TLI = 28 → {20+8} or {19+9} or {16+12} or {15+13}

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
A	l	i	c			l			d	s						m					y	

4 Find characters possible position combination after excluding already occupied positions in reconstructed text.

- E occurred three times twice before and once after the first occurrence of D( at position 10 ) with TLI= 33 → {5+8+20} or {5+9+19} or {6+8+19} or {6+9+18} or {8+9+16}
- SP = 34 → {5+9+20} or {6+8+20} or {6+9+19} or {5+13+16} or {6+12+16} or {5+14+15} or {6+13+15} or {8+12+14}

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
A	l	i	c			l			d	s						m					y	

5 In the altered text N positions were 7 and 19, but position 7 is occupied now and the available possible combination are {19+9} or {20+8}. Try {19+9} for N to see if it will result in the appropriate match in the text building process. Exclude any possible combination for other letters containing these positions {19+9}.

- B = 28 → {20+8} or {16+12} or {15+13}
- O = 32 → {20+12} or {18+14}
- E = 33 → {5+8+20}
- SP = 34 → {6+8+20} or {5+13+16} or {6+12+16} or {5+14+15} or {6+13+15} or {8+12+14}

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A	l	i	c			l		n	d	s						m		n		y	

6 Try the only possible combination left for E and excluding sets containing 5, 8, and 20.

- B = 28 → {16+12} or {15+13}
- O = 32 → {18+14}
- SP = 34 → {6+12+16} or {6+13+15}

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A	l	i	c	e		l	e	n	d	s						m		n	e	y	

7 Try the only possible combination left for O and excluding sets containing 14 and 18.

- B = 28 → {16+12} or {15+13}
- SP = 34 → {6+12+16} or {6+13+15}

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A	l	i	c	e		l	e	n	d	s			o			m	o	n	e	y	

⑧ The letter O between the two B’s was shifted 12 position backward, so adding 12 to the positions of the two B’s in the altered text will result in position{15+13}. Try this combination to see if the altered text will match the original text.

- $SP = 34 \rightarrow \{6+12+16\}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A	l	i	c	e		l	e	n	d	s		B	o	b		m	o	n	e	y	

### 4.4.2 Scenario (2): Alice lends Alex money.

In this scenario, assume that the word “Bob” in the original text has been removed and the word “Alex” is inserted in its stead. Editing the content of text is another kind of “Cut and Paste” attack on text in the base documents. In this case, most characters associated within the text did not change, except letters for the word (B, O, B) being replaced with letters for the word (A, L, E, X) shown in Table 4-8.

**Table 4-8: THE ASSOCIATED TEXT INDEX**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	l	i	c	e		l	e	N	d	s		A	l	e	x		m	o	n	e	y	.

This will lead to a different understanding from the original context. The result of the attack is that Alice could lose the money that she gave to Bob. The attack changed the liabilities, meaning Alice cannot claim her money from Bob because she actually gave it to someone else. The text Key-print proposed in this thesis can prevent such an attack. This will be illustrated in Figure4-5 using the Key-print alteration detection algorithm. Text Key-print will receive the associated text index presented in Table 4-8 as an input and generates the fingerprint matrix using Text Key-print algorithms in Figure 4-2. Table 4-9 presents the processed input after executing steps 1-A and 1-B in text Key-print algorithms.

**Table 4-9: CHARACTERS FIRST OCCURRENCE AND THEIR POSITIONS IN THE ASSOCIATED TEXT**

Chars	A	C	D	E	I	L	M	N	O	S	X	Y	SP
1 <sup>st</sup> occurrence	1	4	10	5	3	2	18	9	19	11	16	22	6
Position	1,13	4	10	5,8,15,21	3	2,7,14	18	9,20	19	11	16	22	6,12,17

Executing all steps of Text Key-print algorithms will produce the generated Key-Print matrix presented in Table 4-10, while the original Key-print matrix in Table 4-4 was kept safe, unaltered and is now retrieved correctly.

**Table 4-10: GENERATED KEY-PRINT MATRIX**

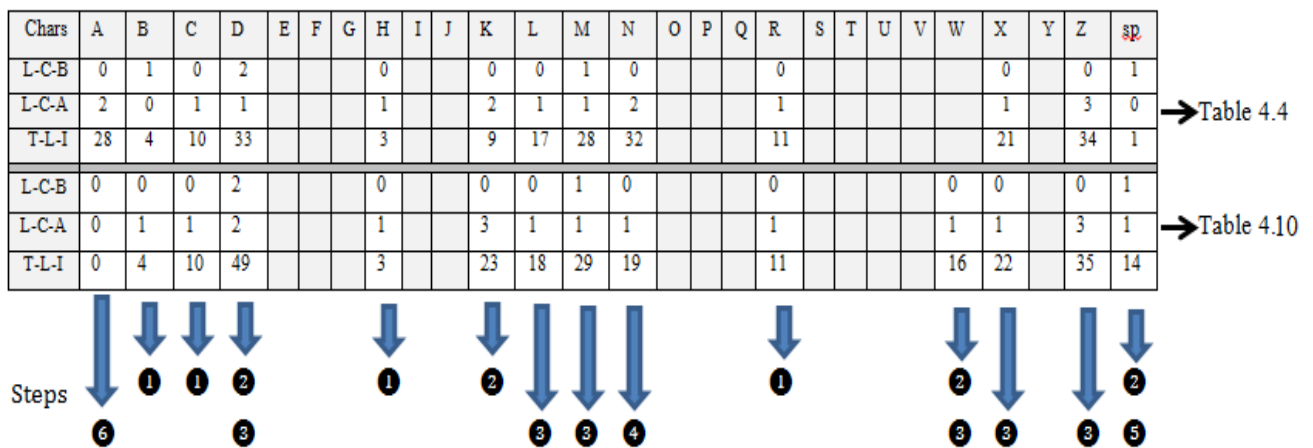
Chars	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SP	
L-C-B	0	0	0	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
L-C-A	0	1	1	2	0	0	0	1	0	0	3	1	1	1	0	0	0	1	0	0	0	0	1	1	0	3	1	
T-L-I	0	4	10	49	0	0	0	3	0	0	23	18	29	19	0	0	0	11	0	0	0	0	16	22	0	35	14	

The interpretation of the results presented in Table 4-10 implies the following:

- character C occurred once after the first occurrence of character B with TLI=4
- character D occurred once after the first occurrence of character C with TLI=10
- character E occurred four times twice after and twice before the first occurrence of character D with TLI= 5+8+15+21=49
- character I occurred once after the first occurrence of character H with TLI= 13
- character L occurred three times after the first occurrence of character K with TLI=2+7+14=23
- character M occurred once after the first occurrence of character L with TLI=18
- character N occurred once before and another after the first occurrence of character M with TLI=9+20=29

- character O occurred once after the first occurrence of character N with TLI= 19
- character S occurred once after the first occurrence of character R with TLI=11
- character X occurred once after the first occurrence of character W with TLI= 16
- character Y occurred once after the first occurrence of character X with TLI= 22
- character SP occurred three times after the first occurrence of character Z with TLI=6+12+17=35
- character A occurred twice once before and another after the first occurrence of character SP with TLI= 1+13=14

Comparing the results presented in Table 4-4 and 4-10 determines what happened to the original text, by analysing the changes in the two interpretations of the Key-Print. This will reveal that some characters listed in the original Key-Print are not present in the generated Key-Print (B & O) and some new characters have been inserted to the associated text (A, L, E & X); therefore, character insertion or modification has happened (i.e. letters has been added and removed). These changes will be highlighted in the analysis in Figure 4-5 after executing all the steps in Figure. 4-3



**Figure 4-5: KEY-PRINT ALTERATION DETECTION ALGORITHM**

The interpretation of the results presented in Figure 4-5 implies the following:

- 1) Three letters are missing (two B's and one O) from the original message
- 2) Four extra letters are inserted (A, E, L, and X) in the original message

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	l	i	c	e		l	e	n	d	s		A	l	e	x		m	o	n	e	y	.

**Steps:**

**1** Characters that are not altered (cells in Table 4-10 that match with Table 4-4 )

- C occurred once with TLI=4
- D occurred once with TLI=10
- I occurred once with TLI= 3
- S occurred once with TLI=11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		i	c						d	s												

**2** Analysing the changes in the two interpretations of the Key-Print reveals

- In the altered Key-Print A occurred twice once before and another after the first occurrence of SP with TLI= 14, while in the original Key-Print A occurred only once with TLI= 1. Therefore, 14-1=13 is the position of the extra inserted A.
- In the altered Key-Print L occurred three times with TLI=23, while in the original Key-Print L occurred with TLI=9. Therefore, 23-9= 14 is the position of the extra inserted L.
- $L = 9 \rightarrow \{2+7\}$
- In the altered Key-Print X occurred once with TLI= 16, while in the original Key-Print X did not exist at all. Therefore, 16 is the position of the extra inserted X.



- In the altered Key-Print E occurred four times twice after and twice before the first occurrence of character D (at position 10) with TLI=49, while in the original Key-Print E occurred three times twice before and once after the first occurrence of character D with TLI=33. Therefore, there is one extra E from the two E's after the first occurrence of character D (either in position 15 or 21).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	L	i	c	e		L	e		d	s				?						?		

- 3 Three letters were deleted and four letters were added; x(at position 16) did not exist before and all the letters after it M, N, Y, and SP were shifted by one. Therefore, the letters in the word money are shifted by one.

- $E = 49 - 5 - 8 - 21$  (E at position 21 is part of the word money which is shifted by one) = 15 is the position of the extra inserted E
- $N = 28 \rightarrow 28 - 19 = 9$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	L	i	c	e		l	e	n	d	s						m	o	n	e	y		

- 4 Try the only possible combination left for O and excluding sets containing 14 and 18.

- $B = 28 \rightarrow \{16+12\}$  or  $\{15+13\}$
- $SP = 34 \rightarrow \{6+12+16\}$  or  $\{6+13+15\}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	L	i	c	e		l	e	n	d	s			o			m	o	n	e	y		

- 5 Find characters possible position combination after excluding already occupied positions in reconstructed text

- $B = 28 \rightarrow \{16+12\}$  or  $\{15+13\}$
- $SP = 34 \rightarrow \{6+12+16\}$  or  $\{6+13+15\}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	l	i	c	e		l	e	n	d	s			o			m	o	n	e	y		

⑥ The letter O between the two B's was shifted 12 position backward, so adding 12 to the positions of the two B's in the altered text will result in position{15+13}. Try this combination to see if the altered text will match the original text.

▪  $B = 28 \rightarrow \{15+13\}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
A	l	i	C	e		l	e	n	d	s		B	o	b		m	o	n	e	Y		

Taking all together, the results obtained by executing the proposed text index generation, Text Key-print and Key-print alteration detection algorithms, as well as their interpretations in both scenarios assures the validity of using these proposed algorithms for detecting and preventing the cut and paste vulnerabilities in small and moderate size text documents.

## 4.5 Fingerprint Generation

Fingerprints are features of an object that tend to distinguish it from other similar objects. The nature of the objects could be of a physical fingerprinting (i.e. human fingerprint, iris patterns and so on) or a digital fingerprinting which a computer can process. Fingerprinting refers to the process of adding fingerprints to an object or of identifying fingerprints that are already genuine to an object. Fingerprinting schemes are technical means to discourage people from illegally redistributing the digital contents they have legally purchased. They have various applications: they can be used for copyright protection of data, they should be tamper-resistant, and enable the owner to trace authorised users distributing them illegally. Moreover, it provides only detection and not prevention; the ability to detect illegal use may help prevent individuals from committing these acts. One of the main

requirements of fingerprinting for copy tracing and copy reduction is collusion tolerance; it is to say even if attackers have access to a certain number of copies (objects), they should not be able to find, generate, or delete the fingerprint by comparing the copies. In particular, the fingerprints must have a common intersection that does not significantly decrease the usefulness or quality of the object (Katzenbeisser and Petitcolas, 2000).

Analysing the complexity of the established relationships presents a mechanism to detect unauthorised tampering with a document's textual content. The mathematical operations include creating logical relationships, treating the elements of text (characters) as numbers in a matrix and keeping a specially encoded key-print of the original contexts of a digital document. This information forms a key that cannot only guarantee an author's intellectual property but can also enforce copyright protection in digital document. This mechanism needs a cover to help it perform its task, alongside another mechanism which is needed to distinguish it from other similar existing documents. Therefore, we propose the use of QR codes to store the proposed mechanism. In so doing, we utilise its main function as a unique identification method. A QR code is a member of 2D barcodes, which can store large amounts of data in a small area to support information distribution and detection. Moreover, it has unique features such as high capacity encoding of data, small printout size, dirt and damage resistance, readable from any direction in 360°, and a structure append feature; all of these feature can help us to create a robust key fingerprint. Thus, we are one step closer to meeting requirements of fingerprints such as copyright protection of data, tamper-resistance and enabling owners to trace authorised users distributing them illegally. However, where to hide the fingerprint in the QR code is the last step to have an integrated solution.

## **4.6 Conclusion**

This chapter has presented a novel method called Text Key-Print to protect the textual component of digital document by operating on the basic element of the language (characters) to achieve the goal through the transformation of the physical structured of the document into a logical structured relationship. The logical structure asserts the position of the alphabets in the document in order to discover any alteration in the original document. The resultant dimensional matrix is then converted into a binary stream and encapsulated with a serial number or URL inside a Quick response Code (QR code) to form a digital fingerprint mark.

As highlighted earlier in Chapter 2 the research work focusing on text based document is quite inadequate. Many problems of modern multimedia management and multimedia security require efficient tools which can provide content identification. Consequently, the evolution of barcode technology can be utilized to prove a unique identification (UID) for multimedia authentication and integrity. Since QR code is a binary image and most digital document usually is composed of textual as well as graphical representation, we suggest the use of image steganography techniques to embed Text Key-Print in the graphical presentation of text documents illustrated in next chapter.

## **Chapter 5: Robust QR-Code Image Steganography**

### **5.1 Overview**

In the previous chapters, the fact that digital documents consist of textual and graphical representations was highlighted. The graphical representations are visual illustrations of verbal statements useful mainly for thinking, problem solving and communicating in various disciplines such as design. Usually, graphical representations such as logos, figures, diagrams or any digitally drawn artefact are stored in image formats. Due to the large amount of redundancy created due to the way in which digital images are represented, an image is the most appropriate carrier type for steganography. Therefore, this chapter focuses on image steganography and provides two methods that were specially developed for images in the spatial and the transform domains.

The structure of this chapter is as follows Section 5.2 provides the principles of image steganography which will guide the two proposed methods and image formats used here. In Section 5.3, the first proposed image steganography method in the spatial domain is presented. The second image steganography method proposed in the transform domain is then presented in Section 5.4. The hiding capacity, stego image imperceptibility and robustness of the secret message are evaluated for the proposed methods in Section 5.5. Finally, the results for both methods will be discussed in Section 5.6, which concludes the chapter.

### **5.2 Image Steganography**

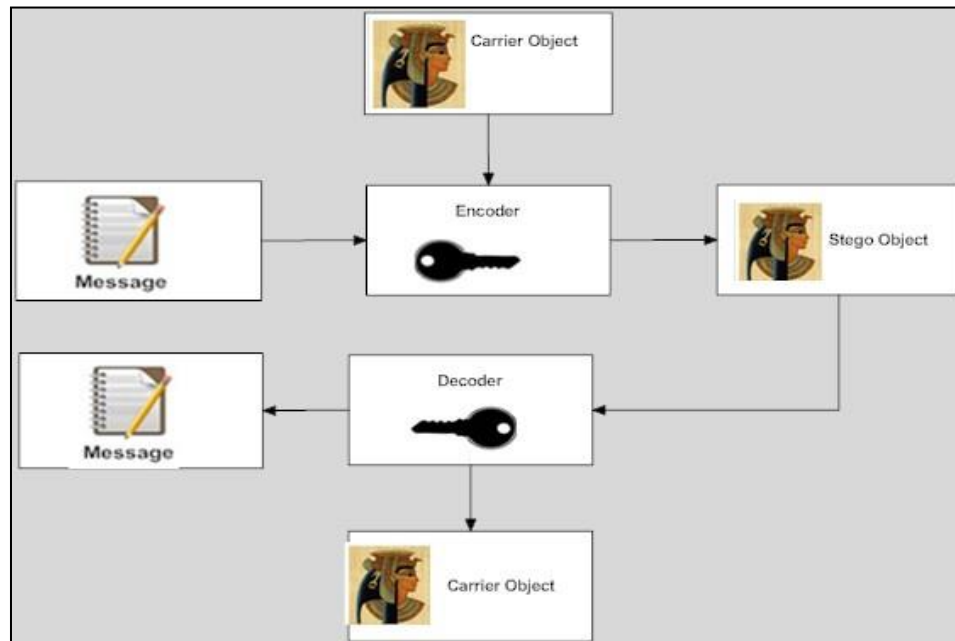
Image steganography has been the focus of a significant body of research because of the large amount of redundancy in an image file that could be potentially

utilised to hide communication. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture elements). Greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue. Each primary colour is represented by 8 bits. Thus, in one given pixel, there can be 256 different quantities of red, green and blue.

In this work, the Portable Network Graphics (PNG) image format is utilised for the cover image. An image fidelity in PNG images is maintained because of their use of lossless compression algorithms. The PNG format used here stores light intensities in 24 bits for the RGB colour model and 16 bits for greyscale images. The 24 bit RGB colour image will be used in the spatial domain method, while the 16 bit greyscale image will be used in the transform domain method.

Basically, the steganography process contains three main components: a message, a carrier file and a key as shown in Figure 5-1. The message is the QR code file that is going to be embedded (hidden) in the carrier. The carrier file (image file) is the object that carries the message. The key is used to decode (extract) the hidden message from the carrier file. This process can be mathematically represented by:

$$y(k) = s(k) + \alpha w(k) \quad (5.1)$$



**Figure 5-1: The Steganography Process**

The message,  $w(k)$ , and the carrier file,  $s(k)$ , are independent from each other. They both have continuous values. Depending on the key, some of the values of the message,  $w(k)$ , can have zero as its value. The parameter, “ $\alpha$ ” determines the value of the strength of the message, which can be changed depending on its perceptual characteristics, robustness properties etc. Typically it has values greater than zero, i.e.  $\alpha > 0$ . If the decoder has access to the cover message,  $s(k)$ , then it will be easy to know the hidden message by subtracting  $s(k)$  and  $y(k)$ :

$$\alpha W(k) = y(k) - s(k) \quad (5.2)$$

On the other hand, if the decoder does not know the cover message,  $s(k)$ , then a slightly more secure system for the sender and receiver would be to share a secret key that specifies the method of obtaining  $w(k)$ . Even if an adversary suspects the usage of steganography, without the secret key, there will be no way of determining the pixels to target. The key in the steganography formula is comprised of the embedding methods and its applied algorithms which are used to embed and extract  $w(k)$ .

### 5.3 Spatial Domain Method

As already discussed in Chapter 2, least significant bit (LSB) insertion is a simple approach for embedding information in which the hidden message is transformed to a stream of bits which replace the LSBs of pixel values in the cover image. This enables authenticated receivers to extract the message from the LSB of embedded pixel of the host image with a secret key. A pseudorandom number generator (PRNG) will be used to scatter the message into a set of arbitrary pixels. To make use of a PRNG, it first demands a seed. Seeding is the technical term for giving it an initial value, from which it can shoot out a sequence. If a PRNG is given a similar seed, then it will give the same set of numbers every time. Thus the secret key is the seed which will identify the place and order of the laid out hidden message. It is very difficult to retrieve the hidden message without the same secret key. Hence, by using a secret key, we can increase the security level of the hidden message in LSB-based image steganography.

In this method, the hiding technique is based on RGB images. The secret message (QR code) will be converted into a binary stream where the value of black pixels will be represented by ‘0’ and white pixels by ‘1’. On the cover side, the least three significant bits of each colour channel will be used to store between one to three bits of the secret message. Thus, this technique provides us with three different hiding capacities, as illustrated in Figure 5-2.

Bits Per Pixel	Red								Green								Blue							
	0	1	1	1	0	0	0	0	0	1	1	1	0	1	0	1	1	0	0	0	1	0	0	1
3	0	1	1	1	0	0	0		0	1	1	1	0	1	0		1	0	0	0	1	0		
6	0	1	1	1	0			0	1	1	1	0	1			1	0	0	0	1	0			
9	0	1	1	1	0				0	1	1	1	0				1	0	0	0	1			

Figure 5-2: Three Different Hiding Capacities based on RGB images



Besides hiding and extracting the QR code from a cover image in a safe manner, the main objective of the proposed method is to identify which of the three proposed hiding capacity techniques which is best suited to increase the hiding capacity of the stego image, while maintaining the level of distortion to a minimum so that it remains unrecognisable by the human visual system. This will be discussed in detail in the experimental Section 5.5. The proposed method consists of two procedures: data embedding and data extraction. The data embedding and data extraction procedures are used to transfer the data. Both the data embedding stage and data extraction stage are used to cover and protect the data in a secure manner.

### **5.3.1 Data Embedding Procedure**

The process of embedding into a cover image starts by converting the QR code (secret message) into a binary stream and adding its size at the beginning of the binary stream to notify the size of the embedded message to the recipient. This is followed by a search for the smallest value in the red channel at the first row in the cover image in order to embed the secret key into its blue and green channels. The secret key consists of two main functions: the blue channel value which is the seed for the pseudorandom number generator while the two least significant values of the green channel determine the hiding capacity of the pixel. This method has three different embedding capacities; therefore, a pixel can carry 3 bits or 6 bits or 9 bits of secret message within the 24 bits of a pixel. In other words, the least three significant bits of each colour channel can be used to embed one or two or three bits per channel. The embedding procedure consists of five main steps as shown in Figure 5-3.

*Embedding Procedure:* -

- Inputs: image + secret message (QR-code).
- Output: Stego image.

Begin:

1. Generate the embedded secret message:
  - A. Represent the size of QR code in 8 binary bits (e.g. 177x177=10110001).
  - B. QR code image data represented in 0's for black pixels and 1's for the white pixels.
  - C. Save the converted QR code image into a binary stream starting with QR size.
2. Find the first smallest value in red channel at the first row of the cover image.
3. Select the pixel and process the green and blue channels' intensity value
  - A. Use the intensity value in the blue channel as a seed to generate a random sequence in order to scatter the message into a set of arbitrary pixels.
  - B. Change the least two significant bits in the green channel of the selected pixel according to the look up table which determines the amount of embedding per channel.

Bits per pixel	Bits per channel	Indicator code
3	1	01
6	2	10
9	3	11

4. Start sub-iteration
  - A. Start replacing the least significant bits of the generated sequence with the stream bits from step (1C) according to the information acquired from step (3B) until end of the secret stream:
    - If indicator code: 01, Replace 1<sup>st</sup> least significant bit in each channel
    - Else, if indicator code: 10, Replace 1<sup>st</sup> and 2<sup>nd</sup> least significant bits in each channel
    - Else, indicator code: 11, Replace 1<sup>st</sup>, 2<sup>nd</sup>, and 3<sup>rd</sup> least significant bits in each channel
  - B. Save the new pixel value carrying the QR code and check for the end of secret bits stream
    - If the secret bits stream is not finished yet; go to step (4A)
    - Else, go to step 4C
  - C. End sub-iteration
5. Save the stego-image

End

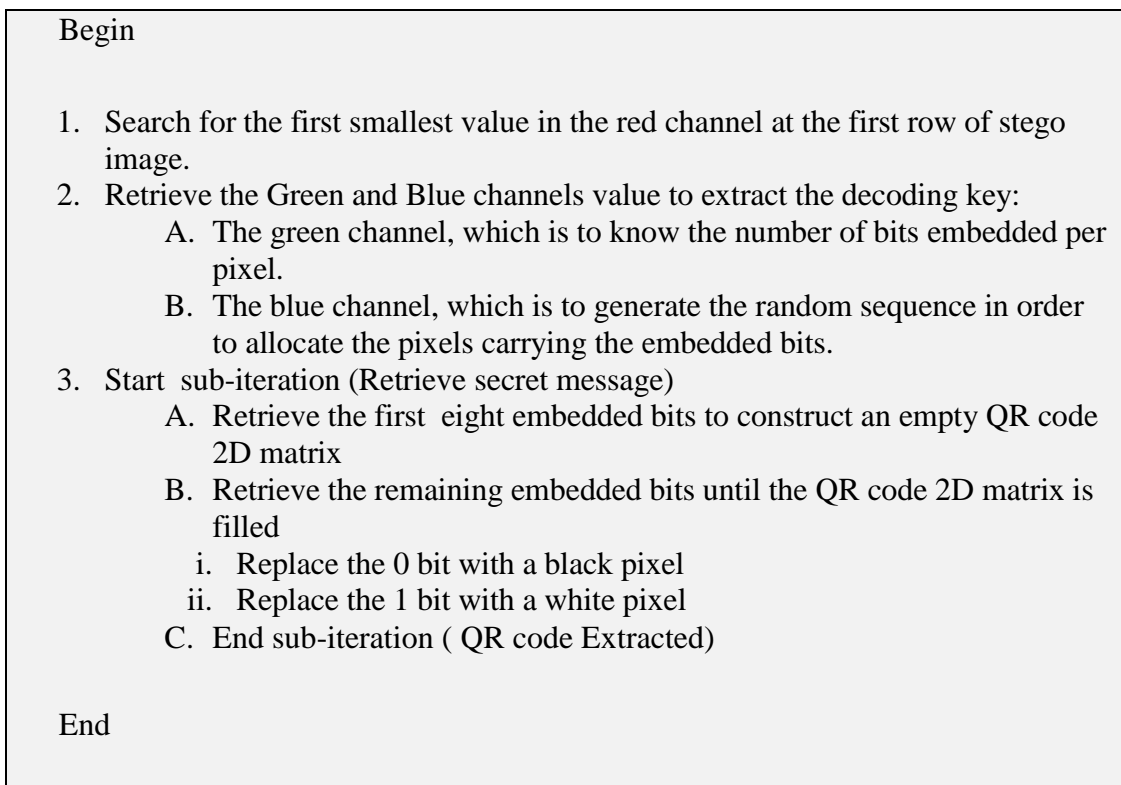
**Figure 5-3: Embedding Procedure**

### 5.3.2 Data Extraction Procedure

The extraction process is the inverse of the embedding process and is used to recover hidden data from the stego image. The first row of the stego image is processed to extract the secret key which is used for embedding. Upon allocating the pixel, the green channel value will indicate the number of bits which is embedded in each pixel (3 or 6 or 9) while the blue channel will generate the random sequence to allocate the pixels storing the hidden data. The first extracted eight bits are used to generate an empty QR code matrix. Then the hidden data will be retrieved to fill the QR code matrix. The extracting process consists of three main iterations, as shown in Figure 5-4.

*Extraction Procedure: -*

- Input: Stego image.
- Outputs: Distorted image + secret message (QR-code).



**Figure 5-4: Extraction Procedure**

## 5.4 Adaptive Transform Domain Method

As we recall from the spatial domain, the quantity of hidden information is large and the speed of embedding and extracting information is fast. However, most algorithms in the spatial domain are based on embedding the key in the image's LSB pixels. These algorithms not only have a weak robustness against attacks, but many of them are also easily detectable (Wang and Wang, 2004). For the sake of robustness of hidden information, many scholars have suggested algorithms based on the transform domain, as mentioned in (Wang and Wang, 2004) who state that, "... by imbedding data in the transform domain, the hidden data reside in more robust areas, spread across the entire image and provide better resistance against signal processing attacks". However, in the transform domain, the embedding process can usually hide less information in images than the spatial domain can.

One of the necessary attributes of any image steganography method is its hiding capacity, i.e. the amount of secret information that can be hidden into a cover image. The challenge that we have to face when increasing the embedding capacity comes in the form of the level of distortion. As a result, the level of distortion introduced into the stego image obtained after embedding the secret information is directly proportional to the embedding capacity of the steganography method. Hence, the main objective of this method is to increase the hiding capacity of the stego image while maintaining the level of distortion to a minimum so that the distortion introduced is unrecognisable by the human visual system (HVS).

The method which we will be proposing is based on transform domain solutions, which converts a signal from the spatial domain into a frequency representation with the embedding process being applied in the transformed coefficients. The proposed transform method, thus, hides the information in the frequency coefficients of a cover image in order to provide a higher capacity, better stego image imperceptibility and robustness of hidden information. To achieve these results, an adaptive approach is designed which is operated in three phases:

choose the location, identify the embedding strength and embedding and extracting. These will now be described in detail.

### 5.4.1 Phase One: Choose the Locations

If the information is to be spread over a number of different locations in the document, then the locations should be chosen with as much care as practically possible. As discussed in Chapter 2, discrete cosine transform (DCT) allows an image to be broken up into different frequency bands, namely the high, middle and low frequency bands. This makes it easier to choose the band in which embedding can take place. The literature survey undertaken in Chapter 2 reveals that it is mostly the middle frequency band which is used for embedding, as the HVS is much more sensitive to low frequencies than high ones. Moreover, hiding information in the low frequency of DCT has better robustness while hiding it in the middle and high frequencies has better imperceptibility. To compound the challenge, the rounding error which exists in the DCT inverse transformation may destroy information embedded in the high frequencies even without lossy compression. In addition, experiments show that noisy data may easily corrupt information embedded in high frequency. Therefore, many scholars tend to choose middle frequency coefficients (Tan et al, 2008), low frequency coefficients (Cox et al, 1997) and even the DC component (Huang et al, 2000) as host sequence. However, the hiding capacity in the middle and low frequency coefficients cannot be too large in comparison with the spatial domain techniques. This is the biggest deficiency of the algorithm, which is based on the DCT (Jianqan et al, 2009).

In this algorithm, the DCT is used to transform successive 8x8 non overlapping pixel blocks of the image into 64 DCT coefficients in each block. The QR code is embedded in the middle frequency ranges under a predefined threshold in the 64 DCT coefficients. Depending on the embedding location, the algorithm has two different hiding capacities (HC)-1 and (HC)-2, as shown in Figure 5-5. The threshold is calculated to determine the DCT coefficients to embed in. The shaded DCT coefficients shown in Figure 5-5 are allocated for embedding the secret

message by adaptively adjusting DCT coefficients according to the threshold value discussed in the next subsection. The idea behind the proposed block-based adaptive scheme is to introduce a local visual masking effect to control the embedded data based on the host image content. The reason for choosing the middle frequency range locations to embed the QR code is that their coefficient values are usually small and, therefore, a small range threshold when embedded might go unnoticed. Moreover, the cover image used is in PNG format, which means there is no loss of data during compression because of the lossless compression algorithms used in PNG. This ensures the extraction of hidden information is accurately accomplished and that a considerable amount of hidden information can be embedded with the assistance of the QR code's error correction feature.

(HC)-1									(HC)-2								
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7
0									0								
1									1								
2									2								
3									3								
4									4								
5									5								
6									6								
7									7								

**Figure 5-5: (HC)-1 and (HC)-2 technique in embedding 64 DCT coefficient per Block**

### 5.4.2 Phase Two: Identify the Embedding Strength

A slightly more secure system for the sender and receiver is to share a secret key that specifies only certain pixels which are to be changed. Even if an adversary suspects the usage of steganography, there will be no way of knowing which pixels to target without the secret key. The key to successful steganography is to embed in the shaded DCT coefficient in middle under a predefined threshold value. Thresholding is one of the first low-level image processing techniques, used before the document analysis step, for obtaining a binary image from its

greyscale. Thresholding algorithms depend on a multitude of factors such as the grey level distribution of the document, local shading effects, the presence of denser, non-text components such as the quality of the photographs etc. Each of the threshold methods has its advantages and disadvantages. It is sometimes useful to try all the methods before deciding the best method which could be applied to a particular class of images. However, this decision of choosing  $\alpha$  – coefficient that measures the strength of the embedding process – is actually based on the choice of the threshold value. We calculate the DCT transformation and adjust the DCT coefficients so that a certain binary pattern is encoded. We start by defining a geometric sequence of real numbers, parameterised by  $\alpha \in (0,1)$ . For  $x > 1$ ,  $x_i \leq x < x_{i+1}$  we define an index function:  $\text{Ind}(x) = (-1)^i$ .

It is easy to see that any real number  $x > 1$  can be modified by adding or subtracting at most  $\alpha x$  to change its index  $\text{ind}(x)$ . The index function is depicted in the equation,

$$x_{i+1} = \frac{1+\alpha}{1-\alpha} x_i, \quad x_0 = 1, \quad (5.3)$$

Therefore, we carefully choose the threshold value using a specialised software called IGOR Pro, so that the probability of false detections is below  $5.7 \times 10^{-7}$ . For this reason, we embedded a  $512 \times 512$  test image “Baboon” with one QR code and then tested the presence of 1000 randomly generated stego images. Then, we calculated the mean,  $m$  and the standard deviation,  $\sigma$  of the resulting correlation values and set the threshold to  $\text{Th} = m + 5\sigma$ . On the condition that the correlations are Gaussian distributed, we found that the probability of a false detection is less than  $5.7 \times 10^{-7}$ . Thus, we used  $\text{Th}$  as a threshold condition, which is also a condition for  $\alpha$  selection. We found that for the best signal strength,  $\alpha=0.3$  is the best choice which means  $\text{Ind}(|b_i'|) \approx 2$ .

### 5.4.3 Phase three: Embedding and Extracting

This section aims to overcome the challenges of the limited hiding capacity of the DCT technique by choosing the middle frequency range locations in order to embed data, since they present the majority of the DCT coefficients. As stated earlier, embedding in the middle frequency bands may lead to loss of the embedded information due to rounding errors which exist in the DCT inverse transformation. Therefore, a novel embedding strategy is adopted to ensure that the reversible extraction of the embedded information is successful. The adopted strategy is based on two key concepts. First, to identify a threshold that would increase the hiding capacity with a minimal distortion effect on imperceptibility. Second, utilise the QR code to benefit from its characteristics, especially the error correction capabilities, as a cover for hiding secret information. The method depends on transforming the cover image from the spatial to the frequency domain and converts the secret message into a binary form (bit stream). The embedding procedure hides the bits of this secret message in a chosen area within the frequency domain media. This is done after identifying the threshold coefficient that measures the strength of the embedding method on the chosen transformed coefficients in order to get a safe area to hide the secret bit sequence. The pre-processing of the proposed scheme first involves partitioning a cover image into non-overlapping blocks of 8x8 pixels, then performing the 2-dimensional DCT to transform each block into an 8x8 block of DCT coefficients. The proposed method consists mainly of two procedures: data embedding (Figure 5-6) and data extraction (Figure 5-7).



*Embedding Procedure:* - .

- Inputs: image + secret message (QR-code).
- Output: Stego image.

Begin:

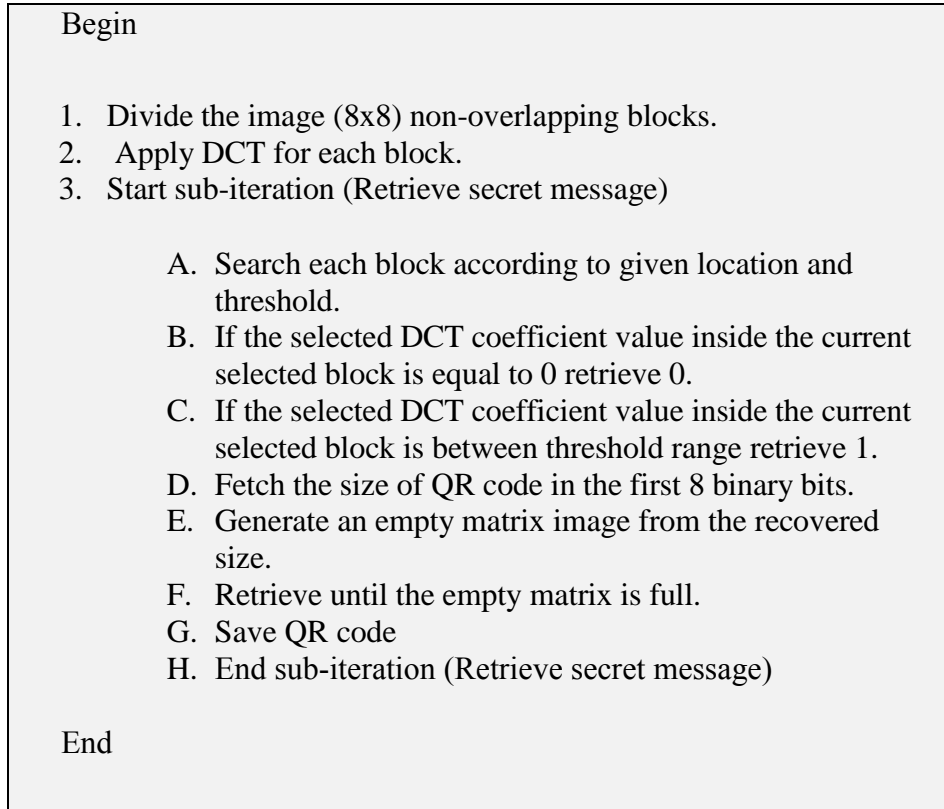
1. Generate the embedded secret message:
  - A. Represent the size of QR code in 8 binary bits
  - B. QR code image data represented in 0's for black pixels and 1's for the white pixels.
  - C. Save the converted QR code image into a binary stream starting with QR size.
2. Start sub-iteration
  - A. Divide the image into (8x8) non-overlapping blocks.
  - B. Apply DCT For each block
  - C. Apply the injection algorithm in block until the end of secret message Data.
    - i. Search each block according to the predefined DCT coefficient locations and threshold (TH).
    - ii. Catch suitable value according to the predefined DCT coefficient locations and (TH).
    - iii. Start embedding:
      - If DCT coefficient value equal to  $\pm TH$ ; add  $-b_i$  if negative or  $+b_i$  if positive to DCT coefficient.
      - Else if the embedded bit is equal to 0 then apply 0 to the selected DCT coefficient
      - Else the embedded bit is equal to one and DCT coefficient less than Th :
        - a. Replace the positive DCT Coefficient with  $Th - b_i$ .
        - b. Replace the negative DCT Coefficient with  $-Th + b_i$ .
        - c. Replace zero with  $-Th + b_i$ .
    - iv. Save new DCT coefficient carrying the QR and check for end of secret bits stream
      - If secret bits stream not finished yet; go to step 2C
      - Else go to step 2D
  - D. End sub-iteration
3. Apply the IDCT to generate the stego-image

End

**Figure 5-6: Embedding Procedure**

*Extraction Procedure:* -

- Input: Stego image.
- Outputs: Distorted image + secret message (QR-code).



**Figure 5-7: Extraction Procedure**

An example for the data embedding in (HC)-1 and (HC)-2 in the first 64 DCT coefficients of the Baboon cover image is shown in Figure 5-8. Note that the shaded DCT coefficients in Figure 5-8 are the result of embedding the secret message which starts with the QR code size represented in eight bits (177 in binary). As stated earlier, a rounding error which exists in the DCT inverse transformation may result in some values being affected during the transformation phase by  $(\pm 1)$ . Therefore, we push the coefficient values equal to  $-/+$  threshold ( $T_h$ ) to the safety region by adding  $(\pm 2)$  to prevent the coefficient value from falling within the range of threshold during extraction. In (HC)-1 and (HC)-2, the threshold is equal to four; the coefficients have three different values:  $-/+$  two means coefficient carrying one and zero means coefficient carrying zero from the secret bit stream, while six means that the coefficient was pushed outside the threshold to the safety region by adding  $(\pm 2)$ .

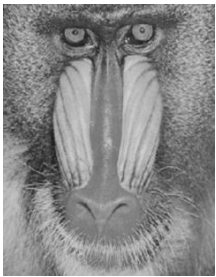

Image Baboon 512x512	1st 64 DCT coefficient										QR code177x177										
		0	1	2	3	4	5	6	7												
	0	967	-69	-89	29	-12	0	-2	1	0											
	1	-157	15	58	-4	4	10	-1	0												
	2	-131	38	-28	36	11	-8	11	-1												
	3	25	-18	-46	0	-1	-3	11	0												
	4	-13	1	-5	1	0	0	0	0												
	5	-5	4	5	11	0	0	0	0												
	6	0	-2	2	-2	0	0	0	0												
7	1	0	0	0	0	0	0	0													
<b>(HC)-1 on 1st 64 DCT coefficient</b>											<b>(HC)-2 on 1st 64 DCT coefficient</b>										

Figure 5-8: An example for the data embedding in (HC)-1 and (HC)-2

## 5.5 Methods Evaluation Results

Now that, the designed artefact has been implemented in the spatial and the transform domains, it is time for its evaluation. According to the design science research methodology: “the *artefact* is evaluated according to the criteria that are always implicit but frequently made explicit in the *proposal*”. The main objective of the proposed method was to increase the hiding capacity while maintaining the level of distortion to a minimum so that the distortion introduced is unrecognisable by the HVS. Thus, the evaluation of this objective is presented here. This evaluation will consider the three most important aspects of any steganography system: the capacity of the payload, the imperceptibility of the stego image, and the robustness of the secret message.

An experiment was therefore set to evaluate the objective of the proposed methods based on three evaluation criteria for image steganography algorithms.

Thus, five 24-bit RGB colour images and their greyscale equivalents, i.e. Baboon, Barbara, Boat, Gold-Hills and Lena with 256x256 and 512x512 pixel dimensions are used as cover images in the experiment. The objective is to hide the largest QR code, a binary image with 177x177 pixels dimension equal to 31, 329 bits plus the 8 bits added to the binary representation of the size of QR code making a total of 31,337 bits. The cover images were processed with the proposed techniques and their different hiding capacities, discussed earlier in this chapter, are used to embed the QR code in Figure 5-9, which contains the URL (<http://www.brunel.ac.uk/>) as a digital mark. Moreover, in order to investigate the impact of increasing the payload on imperceptibility, the secret message is doubled making a total of 62,666 bits.

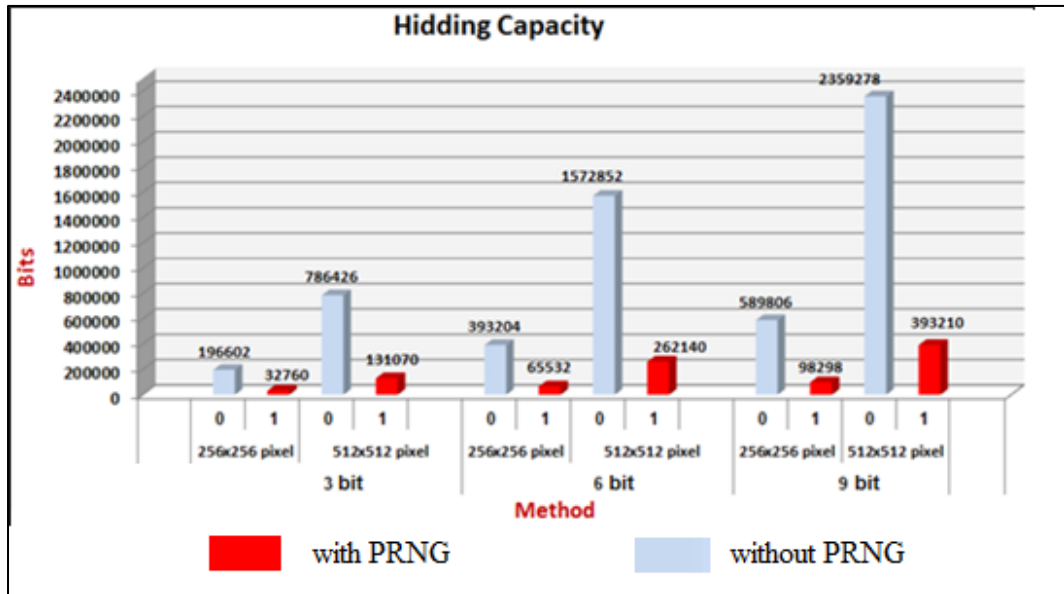


Figure 5-9: QR code (<http://www.brunel.ac.uk/>)

### 5.5.1 Payload Capacity

The first criterion is payload capacity, which is used to measure the hiding capacity for each method with two different cover image pixel dimensions. Before the evaluation process starts in the spatial domain, the pseudorandom number generator (PRNG) is unified, because PRNG was obtained randomly from the blue channel with the smallest red channel value at the first row in the cover image. This means that a different random sequence could be generated depending on each image colour plate intensity value. However, the functionality of the PRNG is only to add a security dimension to the embedding process. We decide to perform the embedding process for all test cover images with PRNG and without PRNG to measure the influence on the security dimension. Figure 5-10 shows the capacity (bits) for the three least significant bits insertion methods: 3bit,

6bit, and 9bit in different cover image pixel dimensions (256x256 and 512x512 pixels) with two different hiding capacities 0 (without PRNG) and 1 (with PRNG).



**Figure 5-10: Hiding capacity for the three spatial domain methods**

According to the calculation in Figure 5-10, methods with PRNG (1) have less embedding space for the secret message than the same methods without PRNG (0). This is because embedding is sequentially done and utilise all the cover hiding space when using methods without PRNG (0), while methods with PRNG (1) scatter the secret message according to a randomly generated sequence. The results also show that cover images with pixel dimensions 256x256 can accommodate the secret message more than once without using PRNG. However, when a PRNG is used, the hiding capacity for the three methods drops to an extent that 3bit method can accommodate only QR (1) and not 62,666 bits of QR (2) and 6bit method can justly accommodate QR (2). Furthermore, there is no need to calculate the cover capacity for each image as they will have the same results due to the sequences used in the embedding process. In the transform domain, Figure 5-11 shows the capacity (bits) in the five cover images with two different hiding capacities (HC)-1 and (HC)-2 and different cover image pixel dimensions (256x256 and 512x512 pixels) of our steganography methods. In order to

understand the result, the maximum hiding capacity (MHC) of a cover is calculated as follows:

$$MHC = \frac{\text{image pixel dimensions} \times \text{coefficient used for embedding (20 in (HC)-1 and 35 in (HC)-2)}}{\text{Block}(8 \times 8 \text{ pixels})} \quad (5.4)$$

HC-(1) uses 20 DCT coefficients to embed the secret message in a block so its maximum hiding capacity in a 256x256 cover image is  $20 \times (256 \times 256) / (8 \times 8) = 20,480$  secret bits. In a 512 x512 cover image it is  $20 \times (512 \times 512) / (8 \times 8) = 81,920$  secret bits. HC-(2), on the other hand, uses 35 DCT coefficients to embed the secret message in a block so its maximum hiding capacity in a 256x256 cover image is  $35 \times (256 \times 256) / (8 \times 8) = 35,840$  secret bits and in a 512 x512 cover image is  $35 \times (512 \times 512) / (8 \times 8) = 143,360$  secret bits. According to these calculations, the HC-(1) technique does not have enough embedding space for the secret message. While HC-(2) should have been able to accommodate the secret message, since its maximum hiding capacity is equal to 35,840 bit. However, the experimental results displayed in Figure 5-11 reveal that the five cover images (256x256 dimensions) are smaller than the amount of secret bits required to be embedded for a QR code with 177x177 pixels dimension as it requires 31,337 bits.

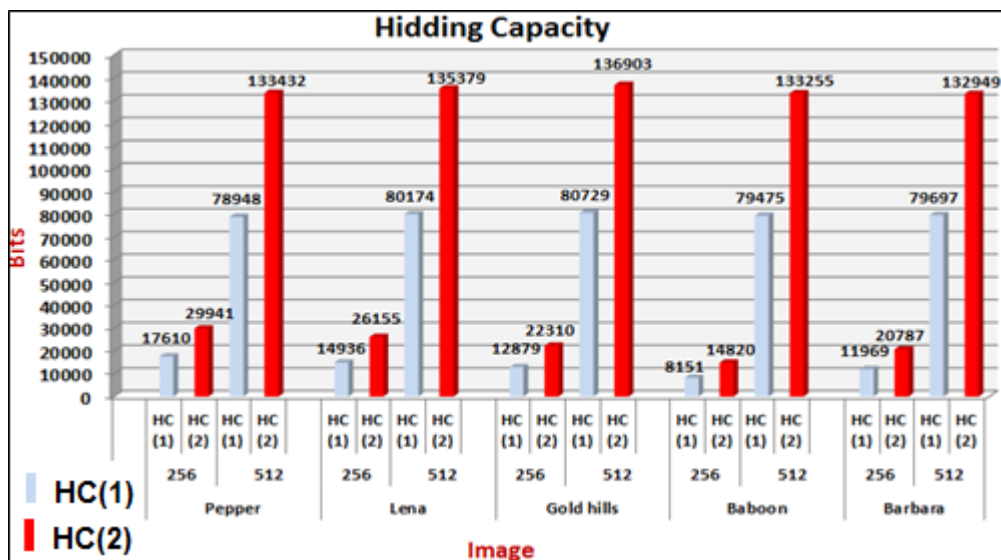


Figure 5-11: The Capacity (bits) of Proposed Method for Five Cover Images

Thus, this cover pixel dimension (256x256 pixels) is dispatched because the secret message tested in this experiment requires a much bigger hiding capacity, which is only realised for 512x512 pixel images. The embedding was only preformed on cover images whose pixel dimensions are 512x512, since such cover has a larger capacity than the amount of secret message bits we need to hide using our proposed methods in this experiment. Thus, creating a total of 50 stego images as each of the five proposed methods generate ten stego images as explained earlier in the evaluation section of Chapter 3.

One of the main steps in this experiment is to test the influence of hiding two QR codes to establish an understanding of the significance of distortion when utilising the majority of the embedding capacity. Since the secret message has a fixed size, the number of pixels needed to carry the embedded data is also of a fixed quantity. Figure 5-12 displayed the percentage of the pixels affected by embedding one and two QR codes from the total cover image (512x512 pixels) using the 3bit, 6bit and 9bit methods. An image with 512x512 pixel dimensions has 262,144 pixels; when two QR codes are embedded, the percentage of the hiding capacity needed for any method is almost doubled, but the pixels needed for each method to hide this payload varies due to the amount of bits which each method can embed per pixel. In other words, as the number of embedded bits increase per pixel, the less number of pixels is needed for embedding the same secret message.

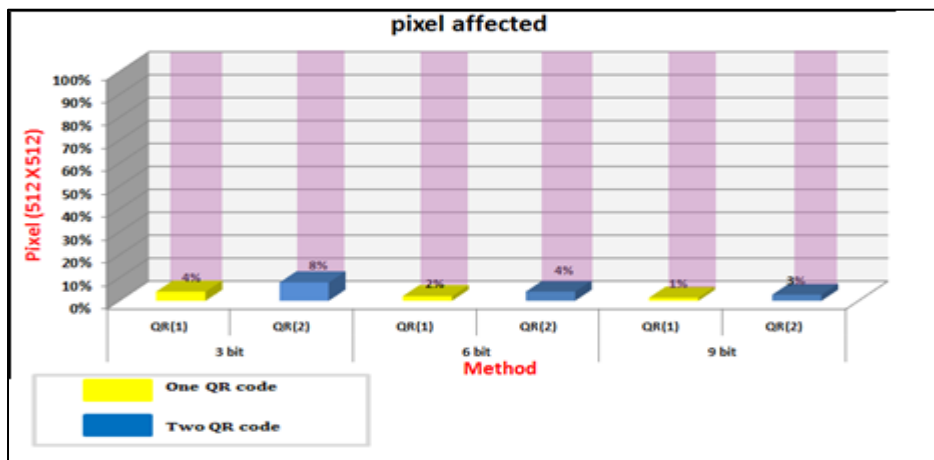
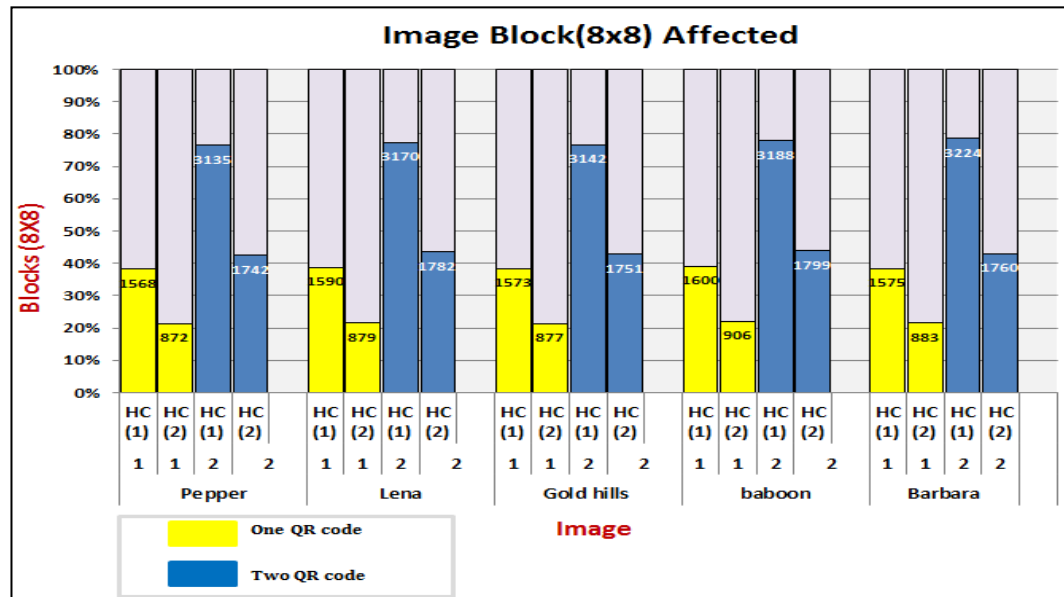


Figure 5-12: Pixel Affected by Embedding One and Two QR code

In the transform domain, an image with 512x512 pixel dimensions has (512x512)/(8x8pixel) equal 4096 blocks. Figure 5-13 presents the number of blocks (8x8) affected by embedding one and two QR codes by using HC (1) and HC (2).



**Figure 5-13: Blocks (8x8) Affected by Embedding One and Two QR code**

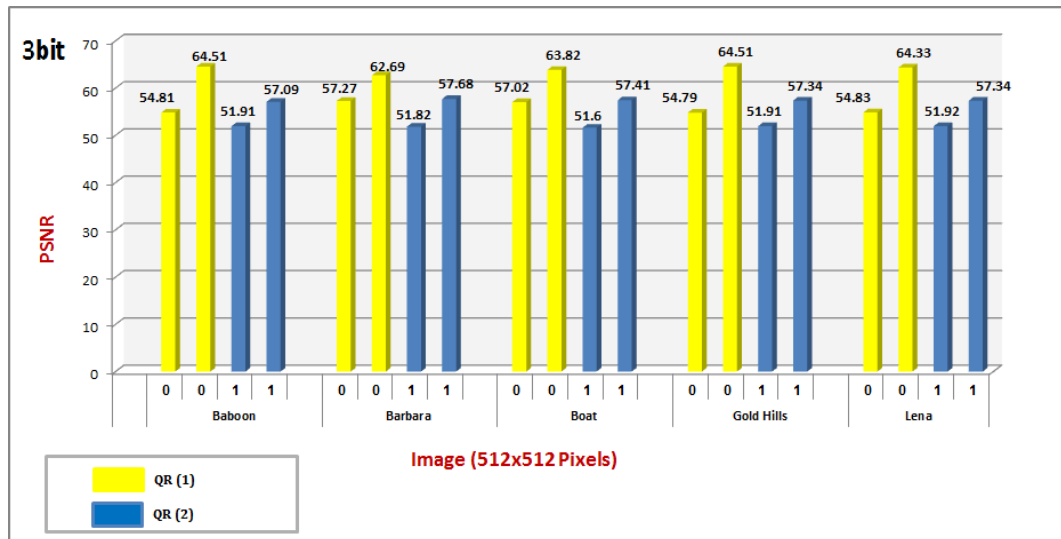
The results from Figure 5-13 show that around 38 percent of the hiding capacity is needed by HC-(1) and around 22 percent of the hiding capacity is needed by HC-(2) to embed one QR code with 177x177 pixels dimension. Thus, HC-(2) affects less blocks than HC-(1) as HC-(2) used more DCT coefficients than HC-(1). When two QR codes are embedded in cover images, the percentage of the hiding capacity needed by both techniques doubles. However, the significance of utilising the imbedding capacity should be reflected on the image quality measured by PSNR, as will be shown in the next subsection.

### 5.5.2 Imperceptibility

The second criterion, imperceptibility, measures the effect of embedding on the quality of the cover image, since embedding in the least significant bits or the transformed coefficients of the cover image has the same effect of adding distortion to an image. The imperceptibility of the stego image is evaluated using

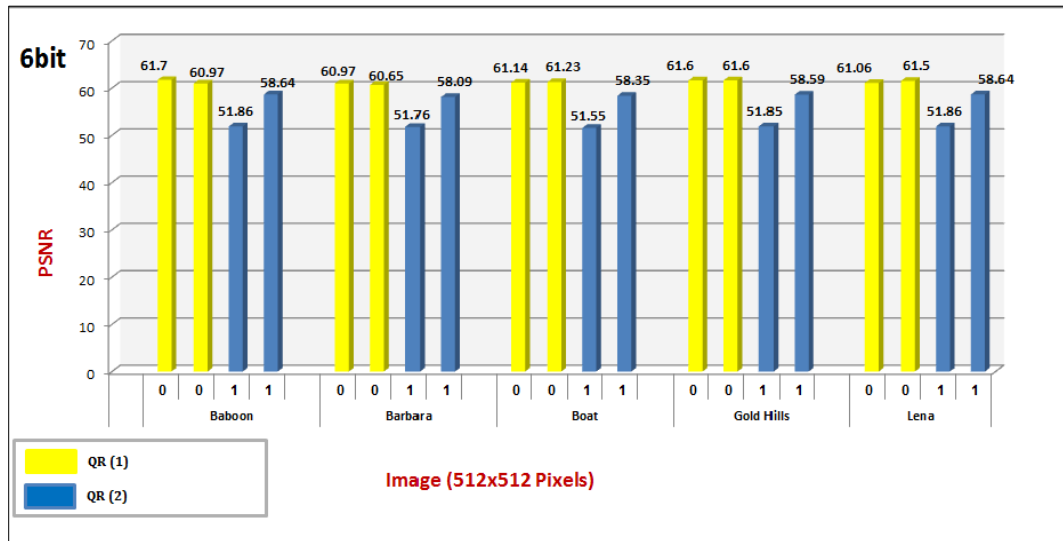


PSNR image quality metrics. The quality of the obtained stego images from embedding one and two QR codes will be measured using PSNR; a stego-image has good imperceptibility if its overall PSNR value is above 36 dB (Wu and Hwang, 2007). Figure 5-14, 5-15, and 5-16 presents the measurements of the quality of stego images for the three methods in the spatial domain.



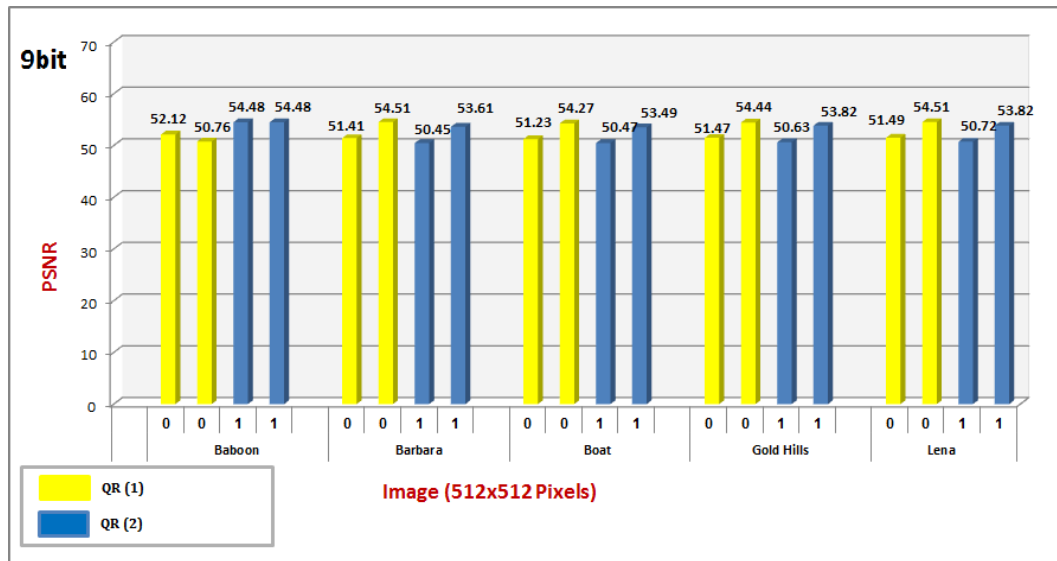
**Figure 5-14: PSNR values for five cover images using 3bit method**

In Figure 5-14, the result for the 3bit method shows that the method with PRNG (1) has a significant better PSNR value for the five cover images tested than the same method without PRNG (0). This can be seen as stego images embedded with QR (1) using PRNG (1) have a PSNR value above 62 dB; while, stego images embedded with QR (1) without using PRNG (0) have a PSNR value above 54 dB. Thus, the use of PRNG so far has provided a better stego image quality even with doubling the embedding payload. The results shows stego images embedded with QR (2) using PRNG have a PSNR value above 57 dB, while stego images embedded with QR (2) without using PRNG have a PSNR value above 51 dB. Doubling the embedded payload has affected the quality of the stego images by around 7dB (64-57 dB) less than the stego images with QR (1). The PSNR values are similar for the five cover images.



**Figure 5-15: PSNR values for five cover images using 6bit method**

In Figure 5-15, the result for the 6bit method shows that the five stego images embedded with QR (1) without PRNG (0) has a slightly better (Baboon and Barbara) or the same (Gold hills) PSNR value in comparison with the same five stego images without PRNG (0). The stego images embedded with QR (1) using PRNG (1) have a PSNR value of approximately 61 dB; this is the same PSNR value for stego images embedded with QR (1) without using PRNG (0). When the payload is doubled, the results for the five stego images embedded with QR (2) using PRNG (1) show a better PSNR value than the five stego images embedded with QR (2) using PRNG (0). Thus, the use of PRNG only provides a better stego image quality when the embedding payload is doubled in this method. The results show stego images embedded with QR (2) using PRNG have a PSNR value above 58 dB, while, stego images embedded with QR (2) without using PRNG have a PSNR value above 51 dB. The doubling of the embedded payload has affected the quality of the stego images by around 3dB (61-58dB) less than the stego images with QR (1). The PSNR values are almost the same for most of the five cover images.



**Figure 5-16: PSNR values for five cover images using 9bit method**

In Figure 5-16, the result for the 9bit method shows that the method using PRNG (1) has a significant better PSNR value for the four cover images than the same method without PRNG (0), except in baboon image. In the Baboon image, the PSNR value (52 dB) of the stego image embedded with QR (1) without PRNG (0) is better than the PSNR value (50dB) of the stego image embedded with QR (1) using PRNG (1). Moreover, when the payload is doubled, the Baboon image embedded with QR (2) using PRNG (1) have a PSNR value of approximately 54 dB; this is the same PSNR value for stego images embedded with QR (2) without using PRNG (0). The rest of the stego images embedded with QR (2) using PRNG (1) show better PSNR value than the stego images embedded with QR (2) using PRNG (0). Thus, the use of PRNG only provides a slightly better stego image quality than the same stego images used without PRNG expect for Baboon image. The doubling of the embedded payload has affected the quality of the stego images by around 1dB (54-53 dB) less than the stego images with QR (1). The PSNR values are almost the same for the remaining four cover images.

Comparing the obtained PSNR results from the three different hiding techniques shows the following the quality of stego images embedded with QR (1) using PRNG (1) is better when fewer bits embedded per pixel. Nevertheless, when the

payload is doubled, the 6bit method has better PSNR results than the 3bit method, which in turn has better PSNR results than 9bit. In the transform domain, the overall PSNR results are considered acceptable and have good imperceptibility, especially if PSNR values are above 36 dB. From the experimental results displayed in Figure 5-17, we can notice that (HC)-2 method perform slightly better than (HC)-1 method in terms of PSNR values, even though (HC)-2 uses more DCT coefficients inside a block (8x8 pixels) to hide than (HC)-1. Moreover, doubling the embedded data (two QR codes) has slightly affected the PSNR from hiding one QR code around 3dB and still obtaining a high PSNR value. Thus, these results show that we have met our objective so far by providing a large hiding capacity while maintaining the level of distortion to a minimum. To complete this objective, the subjective test in Chapter 6 will determine if the distortion introduced is unrecognisable by HVS or not.

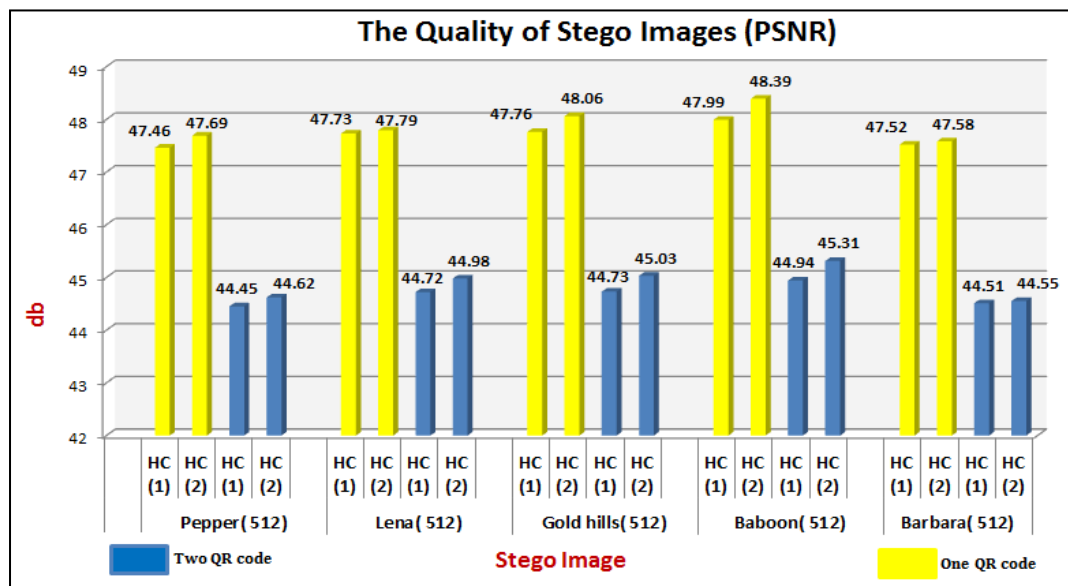












Figure 5-17: PSNR (dB) of Stego Images

### 5.5.3 Robustness

The third criterion is the robustness of the secret message. The robustness of framework is measured for each method through the success of the extracting process. The extracting process aims to recover the hidden data from the stego

image by reverse engineering the embedding process. However, the experimental results of extracting the QR code from the 50 stego images was successful as the application used to scan the extracted QR code redirects to the URL (<http://www.brunel.ac.uk/>). A sample of the extracted QR codes is presented in Table 5-1 with the name of the image and method used in the embedding process.

**Table 5-1: A sample of the extracted QR codes**

				
Baboon-3bit	Barbara-6bit	Gold Hill-9bit	Lena-HC(1)	Boat-HC(2)
				
Gold-Hills-3bit	Lena-6bit	Boat -9bit	Baboon-HC(1)	Barbara-HC(2)

The reason behind choosing the QR code as a secret message is due to its abilities to protect the carried data by utilising the error correction feature, since a considerable amount of the secret bits could be lost though the processes or get mixed up with noise data. It can be seen from the sample that although the obtained QR image is slightly different from the original QR code image, the secret content is restored exactly the same. Moreover, if an adversary suspects the usage of steganography and retrieves the secret bits, he/she has no way of knowing that these bits can construct a QR code to retrieve the secret information. Thus, the extraction of the QR code not only shows the robustness of the secret message, but also proves the reversibility of our proposed scheme.

## 5.6 Conclusion

The work in this chapter presents the continuation of our proposed solution to hide the QR code carrying Text key-print into the graphical representation component of digital text document using image steganography techniques. Thus, two image steganography techniques were developed based in the spatial and the transform domains. In the spatial domain, three methods were proposed and implemented based on the least significant bit (LSB) insertion technique and the use of a pseudorandom number generator (PRNG) to scatter the message into a set of arbitrary pixels. These methods utilise the three colour channels in RGB model-based images to embed one, two or three bits per the eight bit channel, thus resulting in three different hiding capacities. The second technique is the adaptive approach in the transform domain where a threshold value is calculated to identify its embedding strength under a predefined location. This technique contains two methods that differ in the number of transformed coefficients used for embedding and hence provides two different hiding capacities. Therefore, this chapter describes five methods based on two different techniques; each method provides a different hiding capacity and each has its own effect on imperceptibility.

In image steganography, two fundamental aspects – payload capacity and imperceptibility are at odds with each other, since it is quite challenging to increase the payload capacity while maintaining the stego image quality (imperceptibility). This is due to the amount of artefacts introduced to the cover file from the embedding process. Therefore, a trade-off between these two fundamental aspects is needed to achieve a secure system (Venkatraman et al., 2004). In this regard, evaluating the quality of stego images is a significant measure to evaluate the performance of the image steganography techniques (Wu and Hwang, 2007). There are two primary ways to measure image quality: objective and subjective quality methods (Stoica et al., 2003). The objective method is an automated measurement of the physical aspects of images. In this chapter, an objective metric was used for evaluating the five implemented methods. Peak Signal-to-Noise Ratio (PSNR), which is a statistical analysis

measurement, was used for the digital image quality. Moreover, the biggest QR code size was used for embedding the secret data in order to evaluate each method under maximum distortion.

Subjective methods, on the other hand, are based on human observers to evaluate the quality of the images. Since the strength of image steganography lies in its ability to remain unnoticed by the human eye, the visual difference between the cover and the stego image must be perfectly imperceptible for the human visual system. Thus next chapter will evaluate the five proposed methods using a subjective evaluation metric.

## Chapter 6: Subjective Performance Evaluation

### 6.1 Objective Evaluation Metrics

Many objective evaluation metrics have been proposed and developed based on Human Visual System (HVS) characteristics incorporating perceptual quality measurements to provide quality estimation (Baroncini, 2006; Nyman et al., 2006; Pinson and Wolf, 2003; Simone et al., 2009; Stoica et al., 2003; Wu and Rao, 2006). Despite all this effort, objective quality estimation can't replace human judgment for the perceived quality of digital image and the reliability of such metrics is always questioned due to lack of standardisation (Simone et al., 2009).

Although, PSNR and MSE are the most common objective evaluation metrics used to measure image quality for digital image steganography; they are extensively criticised for their poor correlation with actual measurements of perceived quality (Wang et al., 2002a; Wang et al., 2002b). For instance, adding noise to an image can be perceived as a better quality by human observers in some cases, while the added noise will reduce the PSNR value. Furthermore, images with the same PSNR value can actually have different perceived qualities. Additionally, these two objective metrics do not take into account the effects of distortions into different image regions such as smooth areas and textured regions. This explains the criticism that these metrics are inaccurate measures of quality for images affected with different kinds of distortion (Wu and Rao, 2006).

Since, the quality evaluation of stego image is a mandatory requirement for assessing a steganographic technique and the strength of image steganography lies in the ability to be unnoticed by the human eye; subjective evaluation metrics will



be more appropriate to determine the performance of the proposed methods in Chapter 5.

## **6.2 Overview**

Imaging systems may introduce some amounts of distortion or artefacts in the signal during acquisition, processing, storage, transmission and reproduction, so assessing the perceived quality of digital images is an important aspect. PSNR is the widely used objective image quality metric to evaluate the quality of stego images or the imperceptibility of steganography methods (Wu and Rao, 2006). It is also used to measure the efficiency of a particular steganography method over another in terms of imperceptibility or stego image quality. For this reason, PSNR was used in Chapter 5 to evaluate the performance of the proposed methods. The obtained results in Chapter 5 implied that stego image quality of the spatial domain methods had better imperceptibility than the transform domain methods. Moreover, the obtained PSNR results for different testing images in the same methods showed a little fluctuation between testing images. Since there is no standardisation for evaluating steganographic methods and these observations needed more clarification; another research in relevant literature was conducted for evaluation criteria before drawing any hypothesis. The comprehensive literature review revealed that PSNR does not offer good results, in terms of human perception, with colour images, and that it is not a reliable predictor of perceived quality (Stoica et al., 2003). Hence, another evaluation method was needed to evaluate our designed artefact which was found in the work of Simone et al. (2009) who developed a subjective evaluation method for still images. Their work inspired us to adopt a subjective evaluation method, namely double stimulus continuous quality scale (DSCQS) described in Chapter 3.

The adoption of the (DSCQS) subjective method makes sense in evaluating the proposed methods in Chapter 5, since the first and foremost image steganography requirement is the ability not to be noticed by the human eye. Therefore, this chapter aims to measure the efficiency of the implemented methods in this

research by evaluating the stego image quality of the proposed methods in Chapter 5 using subjective image quality evaluation methods. The subjective image quality evaluation results will be analysed using statistical tools to determine the best methods within each technique.

## 6.3 Experiment Results

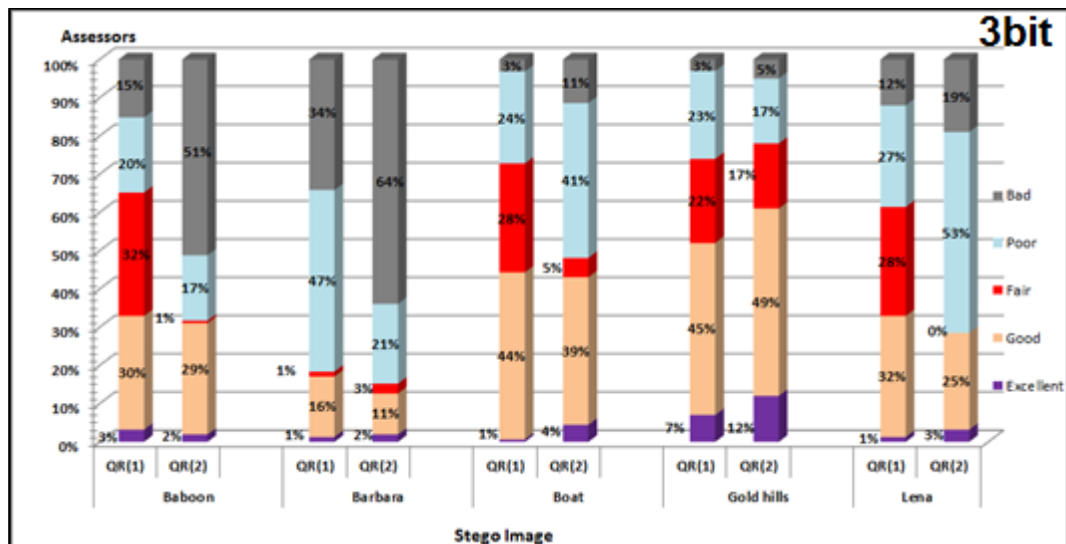
This section illustrates the results of the subjective opinions score carried for the five steganographic methods presented in this thesis. The measuring methods discussed in Chapter 3 will be calculated for each method and presented separately. Thus, this section is divided into five sub-sections displaying the results for each method. Five images were used for each method yielding five stego images containing QR(1) and another five stego images containing QR(2) evaluated by 86 assessor. This resulted in 860 observations for each method, where the mean opinion score of each stego image with respect to its reference image was calculated and assigned a grade. The 86 obtained grades representing the opinion score of three types of assessors in an image are multiplied by the weights discussed in Chapter 3 to generate a weighted sum equal to  $(21 \times 3 + 30 \times 2 + 35 \times 1) = 63 + 60 + 35 = 158$ . Thus each of these details is displayed in tables representing the obtained results for each method.

### 6.3.1 Spatial Method (3bit)

Table 6-1 shows the results of the obtained subjective quality scores converted into the five grade scale. These results are used to construct Figure 6-1, which represents the weighted opinion of the 86 assessors for QR (1) and QR (2). In Figure 6-1, the x axis presents the image used containing results for QR (1) and QR (2), while the y axis presents the percentage of the five weighted quality grade out of 158 (total weighted sum). A comparative evaluation between the results obtained using QR (1) and QR (2) for each image will reveal the influence of increasing the embedding payload.

**Table 6-1: Results of Three Bits per pixel method**

3 bit	QR(1)					QR(2)			
		Expert	Experienced	Naive	WS	Expert	Experienced	Naive	WS
		x3	x2	x1	158	x3	x2	x1	158
Baboon	Excellent	0	1	3	5	0	0	3	3
	Good	0	16	15	47	1	17	9	46
	Fair	16	1	1	51	0	0	1	1
	Poor	4	4	11	31	1	5	14	27
	Bad	1	8	5	24	19	8	8	81
Barbara	Excellent	0	0	2	2	0	0	3	3
	Good	1	7	8	25	1	1	12	17
	Fair	0	0	2	2	1	0	1	4
	Poor	6	20	17	75	1	9	12	33
	Bad	14	3	6	54	18	20	7	101
Boat	Excellent	0	0	1	1	0	2	3	7
	Good	3	25	10	69	2	21	13	61
	Fair	14	1	1	45	0	3	2	8
	Poor	4	4	18	38	14	4	14	64
	Bad	0	0	5	5	5	0	3	18
gold hills	Excellent	2	2	1	11	4	3	1	19
	Good	12	12	11	71	13	13	12	77
	Fair	6	8	1	35	3	5	8	27
	Poor	1	8	18	37	1	9	6	27
	Bad	0	0	4	4	0	0	8	8
Lena	Excellent	0	0	2	2	0	0	5	5
	Good	6	8	16	50	4	8	12	40
	Fair	11	6	0	45	0	0	0	0
	Poor	4	8	14	42	16	13	9	83
	Bad	0	8	3	19	1	9	9	30



**Figure 6-1: Weighted Assessors Opinion for Quality Grade for each Stego Image**

Figure 6-1 shows that the Gold hills image presents the best results for this method, since most assessors' subjective opinion was not able to distinguish between the reference image and the stego image. Moreover, the increased

influence of embedding more data represent by QR (2) was perceived as a better quality than stego image containing QR (1). The results reveal that 51% of the assessors perceived the quality of Gold hills image containing QR (1) as excellent and good, 22% fair and 26 % poor and bad; in contrast, they perceived the quality of Gold hills image containing QR (2) as follows: 61% excellent and good, 17% fair and 22% poor and bad. Barbara's image, on the other hand, is the worst image for this method as assessor were able to identify the stego image containing QR (1) and QR (2) by giving the reference image much higher score. The remaining three stego images (Baboon, Boat and Lena) results imply that stego images containing QR (2) reflected the distortion resulting from the increased amount of the embedded data, since more than 50% of assessors graded them as poor and bad. In comparison their stego image containing QR (1) was perceived on average by the assessor as 37% excellent and good, 29 % fair and 34 % poor and bad.

Since the results shows that stego images containing QR (2) have lower subjective quality score than those with stego images containing QR (1), a paired-sample t-test will measure the statistical variance between stego images containing QR (1) and QR (2) for different assessor groups. The results of the paired-sample t-test show the following (Table 6-2):

- There are significant differences between the views of experts users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ).
- There are significant differences between the views of experienced users in evaluating the four stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ). Only Lena's image is not significant; therefore the decision will be to accept the null hypothesis.

- There are no significant differences between the views of naïve users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to accept the null hypothesis.

**Table 6-2: Paired-sample t-test for Three Bits per pixel**

Paired Differences										
Assessors	Image	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		t	df	Sig.	star code
					Lower	Upper				
Expert	Baboon	-.51668-	0.25499	0.05564	-.63275-	-.40061-	-9.285-	20	0	***
	Barbara	-.27621-	0.22947	0.05007	-.38066-	-.17176-	-5.516-	20	0	***
	Boat	-.13958-	0.06729	0.01468	-.17021-	-.10895-	-9.506-	20	0	***
	gold hills	0.10343	0.04398	0.0096	0.08341	0.12344	10.777	20	0	***
	Lena	-.09656-	0.05444	0.01188	-.12134-	-.07178-	-8.128-	20	0	***
Experienced	Baboon	-.01888-	0.04285	0.00782	-.03488-	-.00288-	-2.414-	29	0.022	*
	Barbara	-.14752-	0.11474	0.02095	-.19037-	-.10468-	-7.042-	29	0	***
	Boat	0.0406	0.05883	0.01074	0.01863	0.06257	3.78	29	0.001	**
	gold hills	-.02661-	0.29574	0.05399	-.13704-	0.08382	-.493-	29	0.626	
	Lena	0.04206	0.04154	0.00758	0.02654	0.05757	5.545	29	0	***
Naïve	Baboon	-.03369-	0.1699	0.02872	-.09205-	0.02467	-1.173-	34	0.249	
	Barbara	-.02384-	0.5768	0.0975	-.22198-	0.1743	-.245-	34	0.808	
	Boat	0.05807	0.26629	0.04501	-.03341-	0.14954	1.29	34	0.206	
	gold hills	-.06790-	0.34096	0.05763	-.18503-	0.04922	-1.178-	34	0.247	
	Lena	-.01277-	0.18238	0.03083	-.07542-	0.04988	-.414-	34	0.681	

After the results of the paired sample t-test, another statistical test (ANOVA) is calculated to measure the statistical variance between the three groups and within each group for the five stego images once for QR (1) and another for QR (2). The result of the ANOVA test in Table 6-3 indicates that the decision will be to accept the null hypothesis for the Baboon stego image containing QR (1) and Lena stego image containing QR (2), as there is no difference between the mean of the three groups in these two images. On the other hand, the decision for the remaining eight stego images will be to reject the null hypothesis and accept the alternative; thus we conclude that for these images, there are statistically significant differences between the three groups and within each group.

**Table 6-3: ANOVA test for Three Bits per pixel**

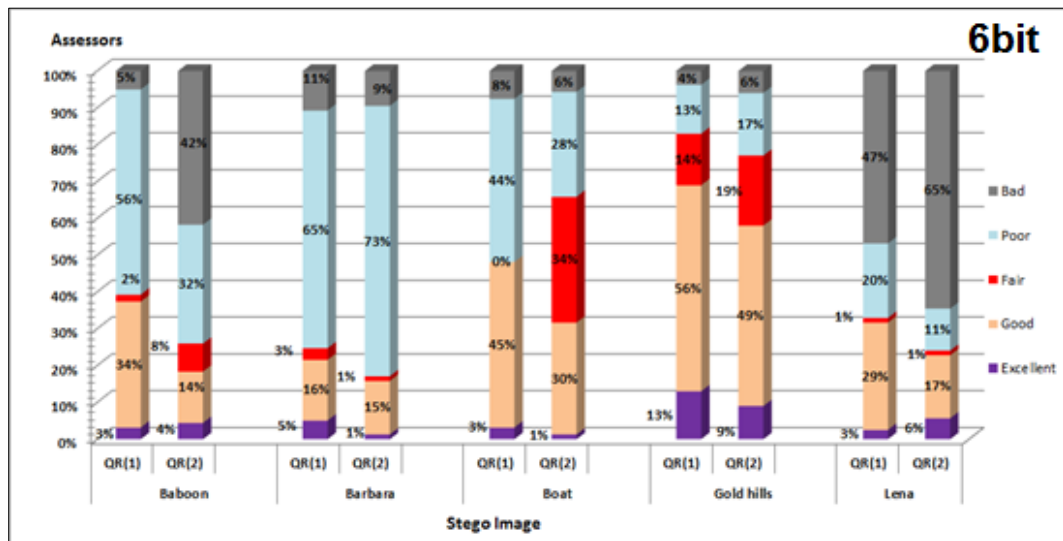
3bit		QR(1)					QR(2)				
		Sum of Squares	df	Mean Square	F	Sig.	Sum of Squares	df	Mean Square	F	Sig.
Baboon	Between Groups	.003	2	.001	.043	.957	3.611	2	1.806	49.742	.000
	Within Groups	2.613	83	.031			3.013	83	.036		***
	Total	2.616	85				6.624	85			
Barbara	Between Groups	.423	2	.212	6.858	.002	2.090	2	1.045	10.761	.000
	Within Groups	2.561	83	.031		**	8.061	83	.097		***
	Total	2.985	85				10.151	85			
Barbara	Between Groups	.175	2	.088	7.003	.002	.157	2	.078	4.589	.013
	Within Groups	1.038	83	.013		**	1.417	83	.017		*
	Total	1.214	85				1.574	85			
gold hills	Between Groups	.192	2	.096	4.464	.014	.878	2	.439	10.073	.000
	Within Groups	1.786	83	.022		*	3.618	83	.044		***
	Total	1.978	85				4.496	85			
Lena	Between Groups	.163	2	.081	4.628	.012	.159	2	.079	2.058	.134
	Within Groups	1.460	83	.018		*	3.199	83	.039		
	Total	1.623	85				3.358	85			

### 6.3.2 Spatial Method (6bit)

Table 6-4 shows the results of the obtained subjective quality scores converted into the five grade scale. These results are used to construct Figure 6.2 which represents the weighted opinion of the 86 assessors for QR (1) and QR (2).

**Table 6-4: Results of Six Bits per pixel method**

6 bit		QR(1)				QR(2)			
		Expert x3	Experienced x2	Naive x1	WS 158	Expert x3	Experienced x2	Naive x1	WS 158
Baboon	Excellent	0	0	5	5	0	0	7	7
	Good	0	22	10	54	1	4	11	22
	Fair	1	0	0	3	0	5	2	12
	Poor	20	8	12	88	2	17	11	51
	Bad	0	0	8	8	18	4	4	66
Barbara	Excellent	0	1	6	8	0	0	2	2
	Good	2	6	8	26	2	1	15	23
	Fair	0	2	1	5	0	0	2	2
	Poor	16	20	14	102	18	26	10	116
	Bad	3	1	6	17	1	3	6	15
Boat	Excellent	0	0	5	5	0	0	2	2
	Good	2	25	15	71	2	14	14	48
	Fair	0	0	0	0	15	4	1	54
	Poor	18	5	6	70	4	11	11	45
	Bad	1	0	9	12	0	1	7	9
gold hills	Excellent	4	3	3	21	1	6	0	15
	Good	12	20	12	88	14	12	11	77
	Fair	4	4	2	22	4	5	8	30
	Poor	1	3	12	21	2	5	11	27
	Bad	0	0	6	6	0	2	5	9
Lena	Excellent	0	0	4	4	0	0	9	9
	Good	4	9	16	46	4	1	13	27
	Fair	0	1	0	2	0	0	2	2
	Poor	0	12	8	32	0	5	8	18
	Bad	17	8	7	74	17	24	3	102



**Figure 6-2: Weighted Assessors Opinion for Quality Grade for each Stego Image**

Figure 6-2 shows that Gold hills image presents the best results for this method, since most assessors' subjective opinion was not able to distinguish between the reference image and the stego image. The results reveal that 69% of the assessors perceived the quality of Gold hill image containing QR (1) as excellent and good, 14% fair and 17 % poor and bad; while they perceived the quality of Gold hills image containing QR (2) as follows: 58% excellent and good, 19% fair and 23% poor and bad. Barbara's image, on the other hand, is the worst image for this method as assessors were able to identify the stego image containing QR (1) and QR (2) by giving the reference image a much higher score. Boat's stego image containing QR (2) has better subjective opinion score than Boat's stego image containing QR (1), since the assessors perceived the quality of QR (2): 34% fair and 34 poor and bad in comparison with 0% fair and 52% poor and bad for QR (1). The results obtained for the remaining two stego images (Baboon and Lena) imply that stego images containing QR (2) reflected the distortion resulting from the increased amount of the embedded data, since more than 60% of assessors graded them as poor and bad. In contrast, their stego image containing QR (1) was perceived on average by the assessor as 34% excellent and good, 2 % fair and 64 % poor and bad.

A paired-sample t-test measures the statistical variance between stego images containing QR (1) and QR (2) for different assessor groups. The results of the paired sample t-test show the following (Table 6-5):

- There are significant differences between the views of experts users in evaluating the four stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ). Only Lena's image is not significant; therefore, the decision will be to accept the null hypothesis.
- There are significant differences between the views of experienced users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ).
- There are no significant differences between the views of naïve users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to accept the null hypothesis.

**Table 6-5: Paired-sample T-test for Six Bits per pixel**

Paired Differences							t	df	Sig.	star code
Assessors	Image	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference					
					Lower	Upper				
Expert	Baboon	-0.42986	0.19846	0.04331	-0.52020	-0.33952	-9.926	20	0	***
	Barbara	0.02624	0.04973	0.01085	0.00361	0.04888	2.418	20	0.025	*
	Boat	0.08624	0.04517	0.00986	0.06567	0.1068	8.748	20	0	***
	gold hills	0.04181	0.18727	0.04087	-0.04344	0.12705	1.023	20	0.318	
	Lena	0.48853	0.22524	0.04915	0.386	0.59105	9.939	20	0	***
Experienced	Baboon	-0.11434	0.06278	0.01146	-0.13778	-0.09089	-9.976	29	0	***
	Barbara	-0.06628	0.14259	0.02603	-0.11953	-0.01304	-2.546	29	0.016	*
	Boat	-0.08460	0.07153	0.01306	-0.11131	-0.05789	-6.478	29	0	***
	gold hills	0.09104	0.05912	0.01079	0.06897	0.11311	8.435	29	0	***
	Lena	-0.18982	0.12508	0.02284	-0.23653	-0.14312	-8.312	29	0	***
Naive	Baboon	0.03371	0.28605	0.04835	-0.06455	0.13197	0.697	34	0.49	
	Barbara	0.00559	0.15013	0.02538	-0.04599	0.05716	0.22	34	0.827	
	Boat	-0.00115	0.34478	0.05828	-0.11959	0.11728	-0.020	34	0.984	
	gold hills	0.09882	0.57272	0.09681	-0.09791	0.29556	1.021	34	0.315	
	Lena	0.06535	0.3261	0.05512	-0.04667	0.17736	1.186	34	0.244	



The result of the ANOVA test (Table 6-6) indicates that the decision will be to accept the null hypothesis for Barbara and Gold Hill stego images containing QR (1) and Boat stego image containing QR (2), as there is no difference between the mean of the three groups in these three images. On the other hand, the decision for the remaining seven stego images will be to reject the null hypothesis and accept the alternative; thus we conclude that for these images, there are statistically significant differences between the three groups and within each group.

**Table 6-6: ANOVA test for Six Bits per pixel**

6bit		QR(1)					QR(2)				
		Sum of Squares	df	Mean Square	F	Sig.	Sum of Squares	df	Mean Square	F	Sig.
Baboon	Between Groups	.169	2	.084	3.354	.040	3.698	2	1.849	55.038	.000
	Within Groups	2.089	83	.025	*		2.788	83	.034	***	
	Total	2.257	85				6.486	85			
Barbara	Between Groups	.077	2	.038	1.387	.256	.120	2	.060	4.000	.022
	Within Groups	2.289	83	.028			1.247	83	.015	*	
	Total	2.366	85				1.367	85			
Barbara	Between Groups	.393	2	.196	6.233	.003	.012	2	.006	.442	.644
	Within Groups	2.615	83	.032	**		1.154	83	.014		
	Total	3.008	85				1.166	85			
gold hills	Between Groups	.498	2	.249	2.414	.096	3.814	2	1.907	65.059	.000
	Within Groups	8.556	83	.103			2.433	83	.029	***	
	Total	9.053	85				6.247	85			
Lena	Between Groups	19.077	2	9.539	53.878	.000	17.641	2	8.820	49.667	.000
	Within Groups	14.694	83	.177	***		14.740	83	.178	***	
	Total	33.772	85				32.380	85			

### 6.3.3 Spatial Method (9bit)

Table 6-7 shows the results of the obtained subjective quality scores converted into the five grade scale. These results are used to construct Figure 6-3, which represents the weighted opinion of the 86 assessors for QR (1) and QR (2).

Table 6-7: Results of Nine Bits per pixel method

9 bit		QR(1)				QR(2)			
		Expert	Experienced	Naive	WS	Expert	Experienced	Naive	WS
		x3	x2	x1	158	x3	x2	x1	158
Baboon	Excellent	0	0	6	6	0	0	5	5
	Good	0	1	10	12	2	1	4	12
	Fair	1	0	3	6	0	0	0	0
	Poor	3	28	9	74	0	16	15	47
	Bad	17	1	7	60	19	13	11	94
Barbara	Excellent	0	0	4	4	0	0	1	1
	Good	1	2	10	17	1	2	13	20
	Fair	1	0	3	6	0	0	1	1
	Poor	0	15	10	40	1	7	18	35
	Bad	19	13	8	91	19	21	2	101
Boat	Excellent	0	0	3	3	0	0	1	1
	Good	1	2	12	19	3	1	14	25
	Fair	1	0	1	4	0	0	2	2
	Poor	18	13	9	89	0	20	12	52
	Bad	1	15	10	43	18	9	6	78
gold hills	Excellent	0	0	1	1	0	0	3	3
	Good	4	2	11	27	1	1	15	20
	Fair	0	0	2	2	1	1	2	7
	Poor	1	20	9	52	16	9	9	75
	Bad	16	8	12	76	3	19	6	53
Lena	Excellent	0	0	5	5	0	0	5	5
	Good	2	1	8	16	1	2	10	17
	Fair	0	0	2	2	0	0	0	0
	Poor	0	10	14	34	0	2	14	18
	Bad	19	19	6	101	20	26	6	118

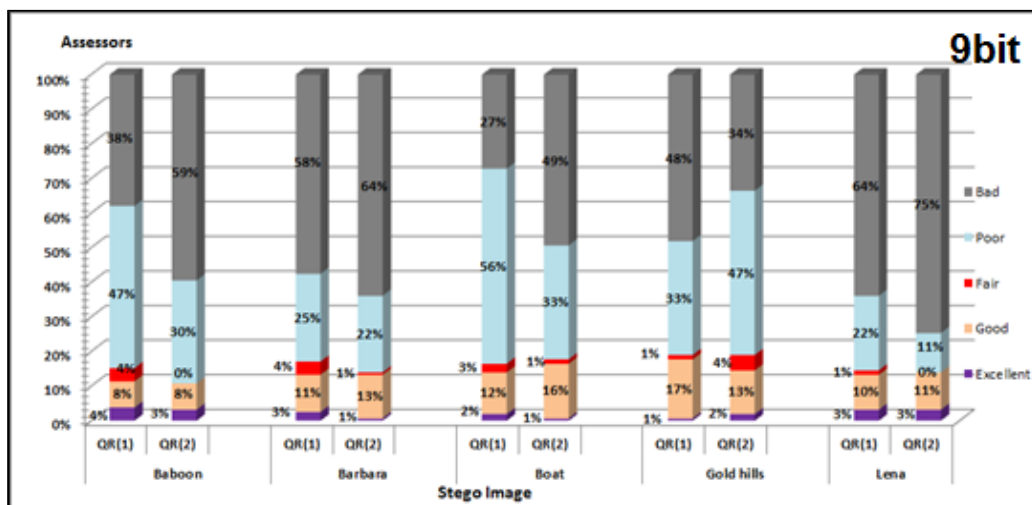


Figure 6-3: Weighted Assessors Opinion for Quality Grade for each Stego Image

The general trend of the results (Figure 6-3) indicates that the distortion caused by this method was obvious, as more than 80% of the assessors perceived the quality of all stego images resulting from this method as poor and bad. Thus we

can conclude that the reference images were mostly given higher subjective quality score than stego images.

**Table 6-8: Paired-sample T-test for Nine Bits per pixel**

Paired Differences							t	df	Sig.	star code
Assessors	Image	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference					
					Lower	Upper				
Expert	Baboon	-0.63891	0.61921	0.13512	-0.92077	-0.35704	-4.728	20	0	***
	Barbara	0.44223	0.51337	0.11203	0.20855	0.67592	3.948	20	0.001	**
	Boat	-0.33440	0.20377	0.04447	-0.42716	-0.24165	-7.520	20	0	***
	gold hills	0.09081	0.17389	0.03795	0.01165	0.16996	2.393	20	0.027	*
	Lena	-0.18883	0.12328	0.0269	-0.24494	-0.13271	-7.019	20	0	***
Experienced	Baboon	-0.10813	0.06281	0.01147	-0.13159	-0.08468	-9.429	29	0	***
	Barbara	-0.09345	0.17965	0.0328	-0.16053	-0.02637	-2.849	29	0.008	**
	Boat	0.07717	0.17766	0.03244	0.01082	0.14351	2.379	29	0.024	*
	gold hills	-0.12952	0.08578	0.01566	-0.16155	-0.09749	-8.270	29	0	***
	Lena	-0.08179	0.13982	0.02553	-0.13400	-0.02958	-3.204	29	0.003	**
Naïve	Baboon	0.00632	0.69425	0.11735	-0.23216	0.2448	0.054	34	0.957	
	Barbara	0.04085	0.29892	0.05053	-0.06183	0.14354	0.809	34	0.424	
	Boat	0.06042	0.30495	0.05155	-0.04433	0.16518	1.172	34	0.249	
	gold hills	0.11947	0.35106	0.05934	-0.00113	0.24006	2.013	34	0.052	
	Lena	0.116	0.68779	0.11626	-0.12026	0.35226	0.998	34	0.325	

A paired-sample t-test will measure the statistical variance between stego images containing QR (1) and QR (2) for different assessor groups. The results of the paired-sample test show the following (Table 6-8):

- There are significant differences between the views of experts users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ).
- There are significant differences between the views of experienced users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ).

- There are no significant differences between the views of naïve users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to accept the null hypothesis.

The result of the ANOVA test (Table 6-9) indicates that the decision will be to accept the null hypothesis for Gold Hill and Lena stego images containing QR (1), as there is no difference between the mean of the three groups in these two images. On the other hand, the decision for the remaining eight stego images will be to reject the null hypothesis and accept the alternative; thus we conclude that for these images, there are statistically significant differences between the three groups and within each group.

**Table 6-9: ANOVA test for Nine Bits per pixel**

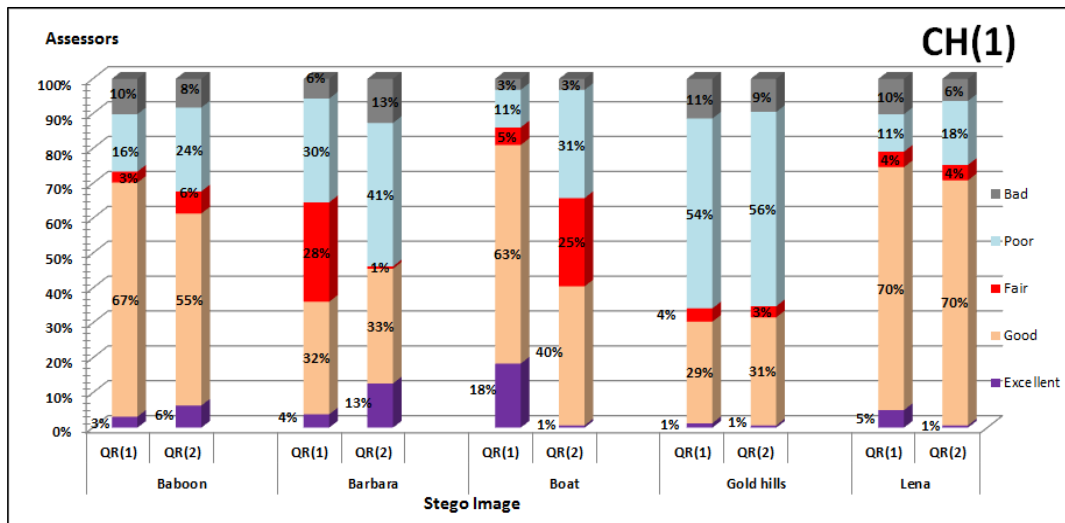
9bit		QR(1)					QR(2)				
		Sum of Squares	df	Mean Square	F	Sig.	Sum of Squares	df	Mean Square	F	Sig.
Baboon	Between Groups	1.665	2	.833	5.831	.004	13.395	2	6.698	47.941	.000
	Within Groups	11.851	83	.143	**		11.595	83	.140	***	
	Total	13.516	85				24.990	85			
Barbara	Between Groups	13.393	2	6.697	51.327	.000	4.222	2	2.111	64.736	.000
	Within Groups	10.829	83	.130	***		2.706	83	.033	***	
	Total	24.223	85				6.928	85			
Barbara	Between Groups	.526	2	.263	3.815	.026	1.854	2	.927	28.166	.000
	Within Groups	5.717	83	.069	*		2.731	83	.033	***	
	Total	6.243	85				4.585	85			
gold hills	Between Groups	.178	2	.089	2.154	.122	1.153	2	.576	20.496	.000
	Within Groups	3.428	83	.041			2.334	83	.028	***	
	Total	3.606	85				3.486	85			
Lena	Between Groups	.406	2	.203	1.603	.208	3.224	2	1.612	46.099	.000
	Within Groups	10.514	83	.127			2.902	83	.035	***	
	Total	10.920	85				6.126	85			

### 6.3.4 Transform Domain Method CH(1)

Table 6-10 shows the results of the obtained subjective quality scores converted into the five grade scale. These results are used to construct Figure 6-4 which represents the weighted opinion of the 86 assessors for QR (1) and QR (2).

**Table 6-10: Results of CH (1) method**

CH(1)		QR(1)				QR(2)			
		Expert	Experienced	Naive	WS	Expert	Experienced	Naive	WS
		x3	x2	x1	158	x3	x2	x1	158
Baboon	Excellent	0	2	1	5	1	3	1	20
	Good	18	22	8	106	13	21	6	99
	Fair	1	0	2	5	2	0	4	7
	Poor	1	6	11	26	4	6	14	22
	Bad	1	0	13	16	1	0	10	10
Barbara	Excellent	0	0	6	6	0	8	4	20
	Good	3	19	4	51	1	19	11	52
	Fair	12	3	3	45	0	0	1	1
	Poor	5	8	16	47	15	3	14	65
	Bad	1	0	6	9	5	0	5	20
Boat	Excellent	4	7	3	29	0	0	1	1
	Good	17	18	12	99	1	25	10	63
	Fair	0	2	4	8	12	2	0	40
	Poor	0	3	11	17	8	3	19	49
	Bad	0	0	5	5	0	0	5	5
gold hills	Excellent	0	0	2	14	0	0	1	1
	Good	2	16	8	54	2	15	13	49
	Fair	0	2	2	4	0	2	1	5
	Poor	16	12	14	68	17	13	11	88
	Bad	3	0	9	18	2	0	9	15
Lena	Excellent	2	0	2	20	0	0	1	1
	Good	18	24	8	100	20	23	5	111
	Fair	0	2	3	7	0	3	1	7
	Poor	0	3	11	17	0	3	23	29
	Bad	1	1	11	14	1	1	5	10



**Figure 6-4: Weighted Assessors Opinion for Quality Grade for each Stego Image**

The general trend of the results (Figure 6-4) indicates that the stego images obtained from this method did not degrade the perceived quality even with the increased amount of hidden data. The results reveal that two stego images (Baboon and Lena) received more than 60% excellent and good subjective grades for both stego images containing QR (1) and QR (2) from assessors. Boat stego

image containing QR (1) have received the highest evaluation score (80% excellent and good), but when the amount of embedded data increases, its evaluation drops to 41 % excellent and good and 25% fair. Gold Hill stego image containing QR (1) and QR (2), on the other hand, is the worst cover image for this method as more than 60% of assessors grade it as poor and bad.

A paired-sample t-test measures the statistical variance between stego images containing QR (1) and QR (2) for different assessor groups. The result of the paired-sample test shows the following (Table 6-11):

- There are significant differences between the views of experts users in evaluating the two stego images (Barbara and Boat) between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ). On the other hand, there are no significant differences in evaluating the three stego images (Baboon, Gold Hill and Lena) between QR (1) and QR (2); therefore the decision will be to accept the null hypothesis.
- The result of the t-test for experienced users is the same as expert's results. Therefore, the decision in evaluating the two stego images (Barbara and Boat) between QR (1) and QR (2) will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ). Similarly, the decision in evaluating the three stego images (Baboon, Gold Hill and Lena) between QR (1) and QR (2) will be to accept the null hypothesis.
- There are no significant differences between the views of naïve users in evaluating the five stego images between QR (1) and QR (2); therefore the decision will be to accept the null hypothesis.

**Table 6-11: Paired-sample T-test for CH (1) method**

Assessors	Image	Paired Differences					t	df	Sig.	star code
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference					
					Lower	Upper				
Expert	Baboon	-0.0095	0.19549	0.04266	-0.09853	0.07945	-0.224	20	0.825	
	Barbara	-.16000	0.14347	0.03131	-.22531	-.09469	-5.111	20	0	***
	Boat	-.17337	0.18973	0.0414	-.25974	-.08701	-4.188	20	0	***
	gold hills	0.00703	0.04673	0.0102	-.01425	0.0283	0.689	20	0.499	
	Lena	-.01030	0.0519	0.01132	-.03392	0.01333	-.909	20	0.374	
Experienced	Baboon	0.00252	0.10311	0.01883	-.04102	0.03599	-0.134	29	0.895	
	Barbara	0.10601	0.07157	0.01307	0.07928	0.13273	8.113	29	0	***
	Boat	-.03727	0.05718	0.01044	-.05862	-.01592	-3.570	29	0.001	**
	gold hills	-0.0017	0.14915	0.02723	-0.05738	0.05401	-0.062	29	0.951	
	Lena	-0.0306	0.13454	0.02456	-0.08085	0.01963	-1.246	29	0.223	
Naïve	Baboon	0.02968	0.24074	0.04069	-.05302	0.11238	0.729	34	0.471	
	Barbara	0.03627	0.34097	0.05764	-.08086	0.1534	0.629	34	0.533	
	Boat	-.04995	0.2185	0.03693	-.12501	0.02511	-1.352	34	0.185	
	gold hills	-.12623	0.63987	0.10816	-.34604	0.09357	-1.167	34	0.251	
	Lena	0.04114	0.2702	0.04567	-.05168	0.13395	0.901	34	0.374	

The results of the ANOVA test (Table 6-12) indicate that the decision will be to accept the null hypothesis for the Baboon stego image containing QR (1) and Gold Hill stego image containing QR (2), as there is no difference between the mean of the three groups in these two images. On the other hand, the decision for the remaining eight stego images will be to reject the null hypothesis and accept the alternative; thus we conclude that for these images, there are statistically significant differences between the three groups and within each group.

**Table 6-12: ANOVA test for CH (1) method**

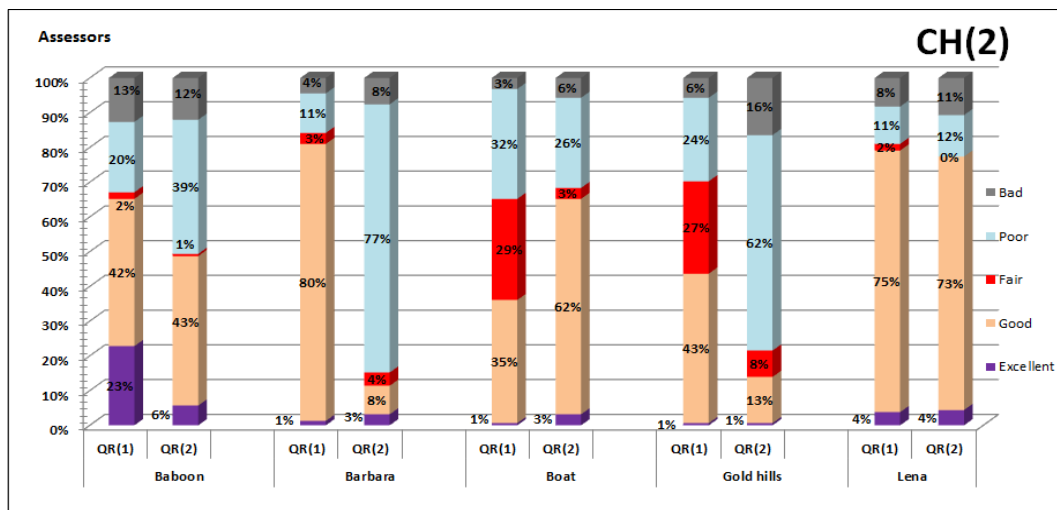
CH(1)		QR(1)					QR(2)				
		Sum of Squares	df	Mean Square	F	Sig.	Sum of Squares	df	Mean Square	F	Sig.
Baboon	Between Groups	.443	2	.222	1.712	.187	.712	2	.356	12.795	.000
	Within Groups	10.751	83	.130			2.309	83	.028		***
	Total	11.194	85				3.021	85			
Barbara	Between Groups	.573	2	.286	7.309	.001	1.278	2	.639	23.940	.000
	Within Groups	3.254	83	.039		**	2.216	83	.027		***
	Total	3.826	85				3.494	85			
Barbara	Between Groups	.436	2	.218	10.801	.000	.314	2	.157	13.833	.000
	Within Groups	1.676	83	.020		***	.942	83	.011		***
	Total	2.112	85				1.257	85			
gold hills	Between Groups	.910	2	.455	4.436	.015	1.008	2	.504	2.481	.090
	Within Groups	8.515	83	.103		*	16.862	83	.203		
	Total	9.425	85				17.870	85			
Lena	Between Groups	1.134	2	.567	14.058	.000	.612	2	.306	16.377	.000
	Within Groups	3.346	83	.040		***	1.551	83	.019		***
	Total	4.480	85				2.162	85			

### 6.3.5 Transform Domain Method CH(2)

Table 6-13 shows the results of the obtained subjective quality scores converted into the five grade scale. These results are used to construct Figure 6-5 which represents the weighted opinion of the 86 assessors for QR (1) and QR (2).

**Table 6-13: Results of CH (2) method**

CH(2)		QR(1)				QR(2)			
		Expert x3	Experienced x2	Naive x1	WS 158	Expert x3	Experienced x2	Naive x1	WS 158
Baboon	Excellent	11	1	1	36	1	0	6	9
	Good	9	16	8	67	19	2	7	68
	Fair	0	1	1	3	0	0	1	1
	Poor	0	10	12	32	0	23	15	61
	Bad	1	2	13	20	1	5	6	19
Barbara	Excellent	0	0	2	2	0	0	5	5
	Good	20	26	14	126	1	1	8	13
	Fair	0	0	5	5	0	0	6	6
	Poor	0	4	10	18	19	27	11	122
	Bad	1	0	4	7	1	2	5	12
Boat	Excellent	0	0	1	1	0	0	5	5
	Good	0	22	12	56	19	17	7	98
	Fair	12	3	4	46	0	2	1	5
	Poor	9	5	13	50	2	10	15	41
	Bad	0	0	5	5	0	1	7	9
gold hills	Excellent	0	0	1	1	0	0	1	1
	Good	3	25	9	68	2	2	11	21
	Fair	13	1	1	42	1	3	3	12
	Poor	5	3	17	38	13	22	15	98
	Bad	0	1	7	9	5	3	5	26
Lena	Excellent	0	1	4	6	0	0	7	7
	Good	19	24	14	119	19	25	9	116
	Fair	0	1	1	3	0	0	0	0
	Poor	0	3	11	17	0	4	10	18
	Bad	2	1	5	13	2	1	9	17



**Figure 6-5: Weighted Assessors Opinion for Quality Grade for each Stego Image**



Figure 6-5 shows that the Lena image presents the best results for this method, since most assessors' subjective opinion was not able to distinguish between the reference image and the stego image. The results reveal that 79% of the assessors perceived the quality of Lena image containing QR (1) as excellent and good, 2% fair and 19 % poor and bad; while they perceived the quality of Lena image containing QR (2) as follow: 77% excellent and good and 23% poor and bad. Barbara stego image containing QR (1) have received the highest evaluation score (81% excellent and good), but when the amount of embedded data increases its evaluation drop significantly to 11 % excellent and good and 4% fair. Baboon stego image containing QR (1) have received the highest excellent subject grade by 23% from the assessor subjective opinion score. Thus, the general trend of the results implies two (Barbara and Gold Hill) out of five images degrade the perceived quality when the amount of hidden data was increased.

A paired-sample t-test will measure the statistical variance between stego images containing QR (1) and QR (2) for different assessor groups. The result of the paired-sample test shows the following (Table 6-14):

- There are significant differences between the views of experts users in evaluating the four stego images between QR (1) and QR (2); therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ). Only the results of Lena's image are not significant; therefore the decision will be to accept the null hypothesis in this case.
- The result of the t-test for experienced users is the same as expert's results. Therefore, the decision in evaluating the four stego images between QR (1) and QR (2) will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ). Similarly, the decision when evaluating Lena's stego images when QR (1) and QR (2) are applied will be to accept the null hypothesis.

- There are no significant differences between the views of naïve users in evaluating the four stego images between QR (1) and QR (2); therefore the decision will be to accept the null hypothesis. Only the results for the Baboon’s image are significant; therefore the decision will be to reject the null hypothesis ( $\mu_1 = \mu_2$ ) and accept the alternative hypothesis ( $\mu_1 \neq \mu_2$ ).

**Table 6-14: Paired-sample T-test for CH (2) method**

Paired Differences							t	df	Sig.	star code
Assessors	Image	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference					
					Lower	Upper				
Expert	Baboon	-.08749	0.04249	0.00927	-.10683	-.06815	-9.435	20	0	***
	Barbara	-.12883	0.05956	0.013	-.15594	-.10172	-9.912	20	0	***
	Boat	0.07323	0.08385	0.0183	0.03506	0.1114	4.002	20	0.001	**
	gold hills	-.14190	0.12568	0.02743	-.19911	-.08469	-5.174	20	0	***
	Lena	-.02706	0.07322	0.01598	-.06039	0.00627	-1.693	20	0.106	
Experienced	Baboon	-.15145	0.17172	0.03135	-.21557	-.08733	-4.831	29	0	***
	Barbara	-.15256	0.09347	0.01707	-.18747	-.11766	-8.940	29	0	***
	Boat	-.03777	0.09261	0.01691	-.07235	-.00319	-2.234	29	0.033	*
	gold hills	-.15902	0.11873	0.02168	-.20335	-.11468	-7.336	29	0	***
	Lena	-.01174	0.07778	0.0142	-.04078	0.0173	-.827	29	0.415	
Naive	Baboon	0.12728	0.27349	0.04623	0.03334	0.22123	2.753	34	0.009	**
	Barbara	0.00876	0.18424	0.03114	-.05453	0.07205	0.281	34	0.78	
	Boat	0.10983	0.66355	0.11216	-.11811	0.33777	0.979	34	0.334	
	gold hills	0.03904	0.12564	0.02124	-.00412	0.0822	1.838	34	0.075	
	Lena	-.04263	0.1857	0.03139	-.10642	0.02116	-1.358	34	0.183	

The result of the ANOVA test (Table 6-15) indicates that the decision will be to accept the null hypothesis for Boat stego image containing QR (1) and Gold Hill and Boat stego images containing QR (2), as there is no difference between the mean of the three groups in these three images. On the other hand, the decision for the remaining seven stego images will be to reject the null hypothesis and accept the alternative; thus we conclude that for these images, there are statistically significant differences between the three groups and within each group.

**Table 6-15: ANOVA test for CH (1) method**

CH(2)		QR(1)					QR(2)				
		Sum of Squares	df	Mean Square	F	Sig.	Sum of Squares	df	Mean Square	F	Sig.
Baboon	Between Groups	.392	2	.196	10.325	.000	.121	2	.060	3.488	.035
	Within Groups	1.577	83	.019	***		1.439	83	.017	*	
	Total	1.969	85				1.560	85			
Barbara	Between Groups	.103	2	.051	3.237	.044	.141	2	.071	3.749	.028
	Within Groups	1.317	83	.016	*		1.561	83	.019	*	
	Total	1.419	85				1.702	85			
Barbara	Between Groups	.737	2	.369	2.945	.058	.172	2	.086	3.019	.054
	Within Groups	10.388	83	.125			2.367	83	.029		
	Total	11.125	85				2.540	85			
gold hills	Between Groups	.169	2	.085	3.380	.039	.282	2	.141	2.759	.069
	Within Groups	2.077	83	.025	*		4.240	83	.051		
	Total	2.246	85				4.522	85			
Lena	Between Groups	1.497	2	.749	21.656	.000	.592	2	.296	8.717	.000
	Within Groups	2.869	83	.035	***		2.819	83	.034	***	
	Total	4.367	85				3.411	85			

## 6.4 Summary of Experiment Results

Processing the results obtained indicates that the steganography methods used in this work have introduced different types of degradation into evaluated stego images. These stego images have been evaluated using subjective methods to identify the appropriate steganography method to use for providing content identification with a minimal effect on user perceived quality. Hence, the subjective quality measurement Mean Opinion Scores (MOS) were calculated in Table 6-16 to rank the five proposed method from best to worse according to the perceived quality from the assessors' point of view.

**Table 6-16: MOS Results for Stego Images**

	Baboon		Barbara		Boat		Gold hill		Lena	
	QR(1)	QR(2)	QR(1)	QR(2)	QR(1)	QR(2)	QR(1)	QR(2)	QR(1)	QR(2)
3bit	2.907	2.3372	2.1977	1.9302	3.0465	2.9767	3.1163	3.2558	2.8372	2.5116
6bit	2.8372	2.3953	2.5349	2.3953	3.0349	2.907	3.4186	3.2209	2.4535	2.2442
9bit	2.2209	1.8372	2.0233	1.9302	2.1744	2.093	2.0349	2.2209	1.9419	1.8721
CH(1)	3.093	3.0465	2.9419	3.0349	3.593	2.9767	2.5814	2.6395	3.2093	3.1163
CH(2)	2.9767	2.314	3.4651	2.3837	2.9884	3.1163	3.4302	3.3372	3.0581	2.7674

The frequency domain methods showed superiority over spatial domain methods being ranked as follow: I) HC (1), II) HC (2), III) 3bit, IV) 6bit and lastly V) 9bit. It can be seen from Table 6-16 that some stego images have an MOS value above 3; these stego images received a higher evaluation score than the reference image from the assessors' point of view. These results were even confirmed by the statistical t-test which investigated the influence of increasing the embedding payload by comparing the subjective opinion score between stego images containing QR (1) and QR (2). Table 6-17 shows which assessor groups did not distinguish between stego images containing QR (1) and QR (2), as resulted from the conducted t-tests.

**Table 6-17: Groups of Users Unable to Distinguish between Stego Images Containing QR (1) and QR (2)**

	<b>Baboon</b>	<b>Barbara</b>	<b>Boat</b>	<b>Gold hill</b>	<b>Lena</b>
<b>3bits</b>	Naïve	Naïve	Naïve	Naïve and Experienced	Naïve
<b>6bits</b>	Naïve	Naïve	Naïve	Naïve and Expert	Naïve
<b>9bits</b>	Naïve	Naïve	Naïve	Naïve	Naïve
<b>HC(1)</b>	Naïve , Experienced, and Expert	Naïve	Naïve	Naïve , Experienced, and Expert	Naïve , Experienced, and Expert
<b>HC(2)</b>	None	Naïve	Naïve	Naïve	Naïve , Experienced, and Expert

The results of the t-test revealed that expert and experienced users were able to distinguish between stego images containing QR (1) and QR (2), with the exception of CH (1) method, where the MOS scores for three images (Baboon, Gold hill and Lena) out of the five in our experimental dataset were not statistically significant. Moreover, the stego images that score above 3 in Table 6-16 are the same images for whom viewer differences are not statistically significant in Table 6-17. Therefore, it confirms that expert and experienced users were not able to distinguish these stego images from the reference images. On the contrary, these assessors gave these stego images much higher scores than the

reference images. Another important observation is that the majority of t-test results for the naïve group were not statistically significant. Given the profile of these users we can accordingly say that they lack the knowledge and experience to understand the distortion presented in stego images. Since the results of t-tests showed the opinion of expert and experience to be almost the same, the statistical ANOVA test was conducted to measure the variance in each group and between groups. The ANOVA results revealed that there is a significant difference in the opinion of the three groups for the perceived quality. However, this only happens for a subset of our image dataset.

## 6.5 Conclusion

Since the visual difference between the cover and the stego image must be perfectly imperceptible to the human visual system, it was logically convenient to ask human observers with different qualifications and experience in the field of image processing to evaluate the perceived quality of the cover and the stego image. Accordingly, this chapter has measured the efficiency of the implemented methods in this research by evaluating the stego image quality of the proposed methods in Chapter 5 by using subjective image quality evaluation methods. Although subjective assessment is often criticised as inconvenient, expensive and time consuming, and useless for real-time applications, the obtained subjective responses showed that it is the appropriate and accurate solution for image steganography transparency evaluation. Their response indicated that using a particular steganography method for different test images affects the quality of the reconstructed stego images differently unlike the results obtained using PSNR in Chapter 5. PSNR as a general quality measures is not a strong indicator of the perceived stego image quality, but not a bad interpreter also of the actual quality of stego images. Measuring the perceived quality to evaluate the performance of the implemented methods in Chapter 5 revealed that increasing the hidden amount of data in the spatial domain methods was statistically significantly distinguishable for most assessors; however, in the transform domain was not that distinguishable even for expert and experience assessors. Moreover, the results

indicate that the CH (1) method was the best steganography method in the perceived stego image quality among the five proposed methods.

## Chapter 7: Conclusions

### 7.1 Overview

Copyright protection and authentication of information has become necessary with the dawn of Internet based communication technologies, such as smart phones, digital libraries and other similar technologies. The ease of dissemination and reproduction of digital content have made it difficult to protect its copyright. Threats to electronic publishing, such as the illegal copying and redistribution of copyrighted material, plagiarism, digital counterfeiting and other forms of violations of copyright laws have to be dealt with. Thus, this research has proposed an artefact based on a steganographic solution to generate a digital fingerprint (Text Key-Print) and encapsulate it with a serial number or URL inside a Quick response Code, thus forming a digital fingerprint mark for digital document authentication. A QR is a binary image and most digital documents are usually composed of textual as well as graphical representations such as logos, figures, diagrams or any digitally drawn artefacts stored into an image format. Therefore, we implemented two image steganography techniques in the spatial and the transform domains to embed the digital fingerprint mark (i.e. Text Key-print and serial number or URL) in five cover images. These five cover images were used to examine the reliability of the proposed artefact by measuring the perceived quality of the two image quality evaluation metrics (PSNR and DSCQS), since the product of the proposed solution depends on any image quality degradation being undetectable.

Thus, this chapter provides a summary of the conducted research. Firstly it gives a brief recapitulation of the aim which was set at the beginning of the research. Then it gives an overview of the findings in light of the set objectives. The chapter then provides the research contribution made through this thesis. It also explains

the limitations of the research and how this work can be used as a step by future researchers for further research.

The next section gives a chapter by chapter summary of the research work, to provide a quick reference to the reader for understanding how the aim and objectives of the research work were achieved.

## 7.2 Thesis Overview

**Chapter 1** is the introduction of this thesis, in which the main motivations for conducting this research were stated. The discussion highlighted requirements and limitations of existing techniques for digital copyright protections such as cryptography, steganography, watermarking and fingerprinting. For instance, the key generation technique used in cryptography and the dependence of the watermarking technique on the structure and format of the text compromises their efficiency. As explained in detail in Section 1.3, cryptography poses a problem in the management of the generated key, whereas just by changing the format of a document, its authenticity in watermarking can easily be compromised. Hence, this chapter provided the starting mark for this project, which was to come up with a framework for a new algorithm to protect the textual representation of a digital document using image steganographic techniques. Consequently, the aim of the research was identified, which was to develop the above stated framework in order to provide a tool that fulfils the security and performance expectations of a steganographic system. Thereafter, the steps to achieve this aim were identified as the objectives of this thesis together with a brief explanation of the research approach.

**Chapter 2** is the literature review of this thesis, which presented an overview of digital steganography basics and the key techniques used to embed secret data. It also provided an in depth discussion of information hiding techniques in different cover files such as text watermarking and image steganography. Thereafter, the explanation of the evaluation criteria and fundamental properties of steganography



method evaluation were discussed to establish an understanding about measuring the efficiency of a steganography technique. Since QR (Quick Response) codes can store large amounts of data in a small area to support information distribution and detection, it was introduced in this chapter as a vital part of the proposed scheme. Finally, this chapter explained the main techniques of steganalysis, the counter technology that can be used to defeat steganography.

**Chapter 3** explained the research methodology undertaken in this thesis. A theoretical grounding of Design Science Research (DSR) was presented to justify the adoption of this method for this research. The research conducted in this thesis was then explained in line with the DSR research process. Four iterations were identified and presented to accomplish the development of the framework. These are, “Awareness of the Problem, Suggestion, Development and Evaluation”. The literature review in Chapter 2 has explained the first step of the framework as summarised above. Suggestion is explained in this chapter, which is precisely the framework itself. The development of algorithm as part of the framework was explained in Chapter 4, while the development of the embedding technique as part of the framework was explained in Chapter 5. Chapter 6 then gave a subjective evaluation of the outcome of the final product of the framework.

**Chapter 4** implemented a digital fingerprint called Text Key-Print, a novel method proposed to protect the textual component of a digital document by operating on the basic element, i.e. language (characters). Through this operation the physical structure of the document is transformed into a logical structured relationship. The logical structure asserts the position of the alphabets in the document in order to discover any alteration in the original document. The outcome of the method is a dimensional matrix converted into a binary stream and encapsulated with a serial number or URL inside a Quick response Code to form a digital fingerprint mark.

**Chapter 5** continued our proposed solution to hide the QR code carrying Text key-print into the graphical representation component of digital text document using image steganography techniques. Thus, two image steganography

techniques were developed based in the spatial and the transform domains. Respectively in the spatial domain, three methods were proposed and implemented based on the least significant bit (LSB) insertion technique and the use of a pseudorandom number generator (PRNG) to scatter the message into a set of arbitrary pixels. The second technique is an adaptive approach in the transform domain where a threshold value is calculated to identify the embedding strength under a predefined location for embedding. A secret message (QR (1) and QR (2)) was embedded in five different cover images to evaluate the payload capacity and stego image quality (imperceptibility) for each of the proposed methods. PSNR and MSE, the most common objective evaluation metrics, were used to measure image quality for stego image generated by each of the proposed methods. The obtained results for each method were evaluated under the imperceptibility subsection using PRNG, which enhanced the perceived quality of the stego image better than embedding sequentially. Moreover, the PSNRs of the five cover images used fall in a specific range within a particular method with a small variation in its value for each image. The idea was to find a significant difference in the perceived quality of the stego images by using cover files. This, however, could not be found.

**Chapter 6** designed an experiment to evaluate stego image quality of the proposed methods in Chapter 5 by using subjective image quality evaluation methods. Since the visual difference between the cover and the stego image must be perfectly imperceptible for the HVS, it was logically convenient to ask human observers with different qualifications and experience in the field of image processing to evaluate the perceived quality of the cover and the stego image. Although subjective assessment is often criticised as inconvenient, expensive and time consuming, and useless for real-time applications, the obtained subjective responses showed that it is the appropriate and accurate solution for image steganography transparency evaluation. Unlike the results obtained using PSNR in Chapter 5, the responses of the participants on this occasion indicated that using a particular steganography method for different test images affects the quality of the reconstructed stego images differently. PSNR as a general quality measure is not a

strong indicator of the perceived stego image quality, but not a bad interpreter also of the actual quality of stego images. Measuring the perceived quality of stego images to evaluate the performance of the implemented methods in Chapter 5 using statistical tools revealed that increasing the hidden amount of data in the spatial domain methods was significantly distinguishable for most assessors, while in the transform domain it was not that distinguishable even for expert and experience assessors. Moreover, the results indicate that the CH (1) method was the best steganography method in the perceived stego image quality among the five proposed methods.

### 7.3 Research Findings

The aim of this research as described in Chapter 1 is to provide a higher level of security by converting document signature into QR Code which in turn will be embedded in any of the document image formats using an efficient steganography technique. This proposed solution is considered a reversible steganographic scheme which utilise the capabilities of both two dimensional barcodes and a high payload capacity in a cover document while maintaining the stego document quality (imperceptibility) to provide a robust protection for digital documents against alteration and tampering

This aim was explored through the accomplishment of three objectives as shall now be detailed:

**Objective 1:** Design and implementation a digital fingerprint that can detect any form of alteration to the original content of the text Based document.

In this thesis, we suggest the use of QR code to develop a reversible steganographic scheme, which guarantees the extraction of hidden data (QR) due to its error correction capabilities. A QR code which contains the digital fingerprint is hidden within a digital document and has to be reliably extracted whenever it is need to fulfil the security and performance expectations of a steganographic system. The goal was to pick the appropriate embedding

mechanism from the proposed methods to hide the QR code in the image without affecting its visual content, while the extraction routine attempts to reliably recover the hidden fingerprint. A blind steganography scheme was developed where the original cover image is not needed during the detection process to detect the mark; only the key used in the embedding process. For the purpose of enhancing robustness, a pseudorandom number generator was used in the spatial domain methods in order to scatter the message into a set of arbitrary pixels to ensure secure transmission of fingerprint over a noisy communication channel or over one subject to intentional tampering. In the transform domain, a threshold value was calculated to identify the embedding strength of the signal under a predefined location for embedding. Both embedding techniques are less robust in low-pass filtering, lossy compression and small geometric deformations of the image but are highly robust with respect to noise adding. This is because of the embedding process which takes place in the middle in the transform domain and in the first three least significant bits in the spatial domain cannot maintain robustness against these attacks. The experimental results in Chapter 5 show that the information hidden using the QR code was successfully extracted with little to no additional impact on image quality. Thus, the QR code which is encapsulated with the Text Key-Print and a serial number or URL presents an alternative approach to protect text base documents rather than the traditional techniques of digital signature and watermarking. Moreover, the analysis of the two scenarios of an attack in Section 4.4 showed how the detecting alteration algorithm in Text Key-Print can protect the textual component of digital documents by operating on the basic element of the language (i.e. alphabets). The logically structured relationship which asserts the position of the alphabets in the document can be used by Text Key-Print to identify the attack performed on the marked digital document. The obtained results for the proposed framework shows the QR code contains the common intersection that does not significantly decrease the quality of the cover object so even if the attackers have access to a certain number of copies (objects), he/she cannot be able to find, generate or delete the fingerprint by comparing the copies (i.e. collusion tolerance). The QR code also enables the

owner of the digital document to trace authorised users who distribute them illegally. As a result, the provided mechanism fulfils the requirements of fingerprinting schemes as it presents a technical means to discourage people from illegally redistributing the digital contents they have legally purchased and detects unauthorised modification to the marked digital document. In doing so, we meet the first objective of our research.

**Objective 2:** Investigation of the impact of using QR code in increasing payload capacity and its effect on quality using different steganographic techniques.

We also suggested the use of different hiding capacities in each of the two techniques in the spatial and the transform domains for the embedding/extraction processes in this scheme. In the spatial domain, the least significant insertion techniques had three different hiding capacities, which introduce different levels of distortion to enable us to hide more data per pixel. In the transform domain, two different hiding capacities depending on the number of transformed coefficient used for embedding introduce different levels of distortion in order to enable us to hide more data per block (8x8 pixels). These five different hiding capacities were treated as independent methods. These methods were examined to embed the largest QR code, which is a binary image with 177x177 pixels dimension, not only once but sometimes twice to establish an understanding of the significance of the distortion when utilising the majority of the embedding capacity. According to the results of PSNR, in the spatial domain, the use of the PRNG in embedding has provided a better stego image quality compared to sequential embedding, even when the embedding payload is doubled. This, however, is not true when the level of distortion inside the pixel is increased by these methods. The PSNR results for embedding one QR code in the five images by the 3bits method around 64db, the 6bits method around 61db and the 9bits method around 54db. In the transform domain, the PSNR values were lower as compared to their values in the spatial domain. This is because colour images give better image quality than the grayscale images in terms of the PSNR

measurement; however, the PSNR value for embedding one QR code in the five images by the HC (1) and HC (2) methods is around 47 db. These results show that HC(2) had a slightly better PSNR value than HC (1) which embeds in lesser coefficients inside the block. This could also be because HC (1) affects more blocks than HC (2) for a given payload. It is the way a method handles the distortion caused by the embedding of a certain payload which is the trade-off between the two fundamental aspects – payload capacity and imperceptibility – in order to achieve a secure system (Venkatraman et al., 2004). Thus, the influence of increased embedded information on the quality of stego images was investigated using the objective image evaluation metric to meet the second objective of this research, which is the better trade-off between payload capacity and imperceptibility within our proposed scheme.

**Objective 3:** Evaluation of the reliability of proposed work through both objective and subjective Quality Evaluation methods.

The use of different cover images in the embedding process did not significantly affect the measured quality using the objective metric. The PSNR values obtained from the five images used to evaluate each of the proposed methods falls in the same range, with tiny differences and sometimes same value. The amount of hidden data and the method used to embed this data are actually the affecting factor for the PSNR value, since PSNR is just a statistical analysis measurement of noisy approximation. The idea was to find a significance difference in the perceived quality of the stego images by using different cover files which could not be found. Since the strength of image steganography lies in its ability to remain unnoticed by the human eye, the visual difference between the cover and the stego image must be perfectly imperceptible to the human visual system. A subjective evaluation method for still images was derived from the quality evaluation of moving images as described in the ITU standard (ITU-R-BT.500-11, 2002) due to lack of standardisation for still image evaluation. Building on the work of Simone et al. (2009), we modified their method within the ITU standard to achieve more accurate results in Chapter 6. The steganography methods used in

this work have introduced different types of degradation into evaluated stego images. These stego images have been evaluated using subjective methods to identify the appropriate steganography which has a minimal effect on the perceived image quality. Hence, the subjective grades obtained from the evaluated stego images were added up to rank the five proposed method from best to worse according to perceived quality from the assessors' point of view, as shown in Table 6-16. The frequency domain methods showed superiority over the spatial domain methods as evident by the ranking which is: I) HC (1), II) HC (2), III) 3bits, IV) 6bits and lastly V) 9bits. These results were further confirmed by the statistical t-test, which investigated the influence of increasing the embedding payload by comparing the subjective opinion score between stego images containing QR (1) and QR (2). The results of t-test revealed that the expert and experienced participants were able to distinguish between stego images containing QR (1) and QR (2) except in some cases as shown in Table 6-17 where stego images received a higher mean opinion score than the reference cover image. Another important observation is that the majority of t-test results for the naïve group were statistically not significant. The logical justification could be drawn from the two questions presented before the subjective test. In other words, they lack the knowledge and experience to understand the distortion presented in a stego image as most of them considered it a better quality than the reference images.

Since the results of the t-test showed the opinion of expert and experienced users almost to be the same, the statistical ANOVA test was conducted to measure the variance within each group and between groups. The result of ANOVA revealed that there is a significant difference in the opinion of the three groups for the perceived quality in most stego images tested for each method. However, the results obtained from the image hiding techniques evaluation using MOS methods, indicate that CH (1) was able to maintain the trade-off between payload capacity and imperceptibility of the stego object. Even when the amount of secret data was doubled in the transform domain, the distortion caused was not that distinguishable for expert and experience assessors in three out of the five images.

Thereafter, evaluating the quality of the stego images is done to meet the third objective by investigating the reliability of the proposed work.

## **7.4 Research Contribution**

This thesis contributes to the theory and its practical demonstration for communities concerned with data hiding, content identification, image steganography, watermarking and fingerprinting. The integration of these relevant research domains enriched the quality of this research. The main contributions of this thesis are as follows:

### **7.4.1 Proposed Text Key-print Fingerprinting Method**

The feasible proposed steganography method that can be used with a QR code and the digital document in order to construct a digital fingerprint providing security for the authenticity of information used to identify or verify a fingerprint. Since there is need for such schemes to solve many problems of modern multimedia management (content filtering, content retrieval/ search, and content tagging) and multimedia security (copyright protection, broadcast monitoring, etc.), which require efficient tools providing content identification. Thus, the design of the Text Key-print method can provide a digital fingerprint to protect the textual content of a digital document by operating on the basic element of the language (i.e. characters of the alphabet) in order to construct a logical structured relationship which asserts the position of the alphabets in the document. Text Key-Print has illustrated its ability to identify attacks on the marked digital document and to provide content identification. The method proposed is different to traditional watermarking and digital signature, since it presents an alternative approach fulfilling the requirements of fingerprinting schemes to protect text-based documents from unauthorised modification to the marked digital document.



## **7.4.2 Increasing Payload Capacity While Maintaining Imperceptibility**

The two most important aspects of any image based steganographic system are the quality of the stego image and the steganographic payload capacity. Consequently, providing a high steganographic capacity, while maintaining the stego image quality (imperceptibility) represents a contribution. According to the results presented in this thesis, the HC (1) steganography method was able to provide a high hiding capacity while maintaining the stego image quality. HC (1) has a hiding capacity of at least 78,948 bits (Fig 5-11) in 512x512 images under a predefined threshold range in the middle frequency DCT coefficient (20 coefficients out of 64 coefficients). Using PSNR to objectively evaluate the method, it is found that this method has a PNSR value above 47db for embedding QR(1) and a PNSR value above 44db for embedding QR(2). One of the tests conducted was to increase distortion (62,666 bits) by embedding QR (2) to utilise the majority of the embedding capacity. The result of the HC(1) method show MOS values above fair on the subjective quality scale for three images (Gold hills, Baboon and Lena) out of the five images used for this method's evaluation. Moreover, the statistical analyses showed that expert and experienced users were not able to distinguish between stego images containing QR (1) and QR (2) in these three images. In other words, the stego images produced by this method received much higher MOS values than the reference cover images from the expert and experienced users. Thus, the objective and subjective evaluation of this method support the claim that it reached an acceptable trade-off between high payload capacity and perceived stego image quality (imperceptibility) and therefore, provides a suggestion and valid direction to improve image steganography techniques.

## **7.4.3 Proved PSNR Unreliability for Stego Images**

Measuring the quality of digital images represents a significant matter in image processing applications. Mostly, PSNR is used to evaluate the quality of stego

images since it is easy, fast and cost-effective methods. Still, image steganography adds another type of distortion to stego images, in which the visual difference between the cover and the stego image should be absolutely imperceptible for the HVS. Therefore, it was logically convenient to ask human observers with different qualifications and experience in the field of image processing to evaluate the perceived quality of the cover and the stego image.

Although PSNR is the most common objective evaluation metric used to measure image quality for digital image steganography, it is criticised for its poor interpretation for the measurements of perceived quality (Wang et al., 2002a; Wang et al., 2002b). These two objective metrics do not take into account the effects of distortions into different image regions such as smooth areas and textured regions. For instance, adding noise to an image can be perceived as a better quality by human observer as shown in our experimental results (i.e. Gold hills, Baboon and Lena stego images in HC (1)), while added noise will reduce the PSNR value. Furthermore, images with the same PSNR value can actually have different perceived qualities. This was proven with the different conclusions obtained from the assessors' responses which indicated that using a particular steganography method for different test images affects the quality of the reconstructed stego images differently. This is in contrast to the results obtained using PSNR in Chapter 5. Thus, PSNR as a general quality measure is not a strong indicator of the perceived stego image quality, but not a bad interpreter also of the actual quality of stego images. Subjective assessment, on the other hand, is often criticised as inconvenient, expensive, time consuming and useless for real-time applications. However, the obtained subjective responses showed that it is the appropriate and accurate solution for image steganography transparency evaluation. Consequently, the implementation of the subjective method DSCQS to measure the efficiency of the proposed methods by evaluating the assessors' responses and analysing the obtained results using statistical methods is a contribution to subjective image quality evaluation methods for still images evaluation.

## 7.5 Research limitations and Future work

During the course of this study, a few issues were identified as limitations that may be further addressed in future research work.

The first limitation of this research is that transform domain methods were conducted only for greyscale images since transformation of colour images for the purpose of embedding did not provide imperceptible results. During the course of the implementation process, many of the proposed schemes in literature for embedding in colour images using the transform domain techniques were tried and the obtained colour stego images had a noticeable visible distortion and a PSNR value below the 30 dB for embedding only one QR code. Thus, designing or finding out methods that can be embedded in colour images while maintaining imperceptibility still requires further research.

The second limitation is that this research focused on improving the trade-off between steganographic capacity and imperceptibility. As such, it only considered the visual attack like the majority of steganographic methods proposed in the literature. The visual quality of stego images is considered the main indication of a steganographic system security. Therefore, this research did not investigate any other kind of possible attacks or steganalysis methods that might detect or compromise the proposed steganography methods.

Lastly, the key aspect of evaluating steganography systems' performance suffers from a lack of standardisation. For instance, the most common measure used to evaluate the quality of stego images (i.e. PSNR) is not a reliable objective image quality measure. Thus, an objective image quality measure is needed to predict the perceived quality and provide reliable results to evaluate stego images. In addition, there are no fixed criteria to determine whether a steganographic system is better than another system, except by comparing the values of its main aspects (payload capacity, robustness and imperceptibility) with those of another. This shortcoming may again be addressed in future work.

## References

- Almohammad, A., and Ghinea, G., 2010. Stego Image Quality and the Reliability of PSNR, IEEE International Conference on Image Processing Theory, Tools and Applications, Paris, France, pp. 215-220.
- Alwan R. H., Kadhim F. J., and Al-Taani A. T., 2005. Data Embedding Based on Better Use of Bits in Image Pixels, International Journal of Signal Processing, 2 (1), pp. 104-107.
- Anderson, R. 1996. Proceedings of: Information Hiding – First International Workshop, Cambridge, U.K., vol. 1174 of Lecture Notes in Computer Science, Springer-Verlag Inc.
- Anderson, R.J. and Petitcolas, 1998. On the limits of steganography, IEEE Journal on Selected Areas in Communication, 16(4), pp.474-481.
- Arno J. H. Peels, Norbert J. M. Janssen, Wop Nawijn, 1985. Document architecture and text formatting, ACM Transactions on Information Systems (TOIS), 3(4), pp.347-369.
- Artz, D., 2001. Digital Steganography: Hiding data within data, IEEE Internet Computing 5(3), pp.75-80.
- Atallah, Mikhail. J., McDonough, Craig., Nirenburg, Sergei., and Raskin,Victor., 2000. Natural Language Processing for Information Assurance and Security: An Overview and Implementations, Proceedings 9th ACM/SIGSAC New Security Paradigms Workshop, pp. 51–65.
- Bailey, K. and Curran, K., 2006. An Evaluation of Image Based Steganography Methods Using Visual Inspection and Automated Detection Techniques, Multimedia Tools and Applications, 31, pp. 55-88.
- Bailey, K., Curran, K. and Condell, J., 2004. Evaluation of Pixel-Based Steganography and Stego-detection Methods, The Imaging Science Journal, 52, pp. 131-150.
- Baroncini, V., 2006. New Tendencies in Subjective Video Quality Evaluation, IEICE Trans Fundamental Electronic Communication Computer Science, E89-A, pp. 2933-2937.
- Bech, S., and Zacharov, N., 2006. The Perceptual Audio Evaluation: Theory, Method and Application. Wiley Blackwell.
- Bender, W., Gruhl, D., Morimoto, N., and Lu, A., 1996. Techniques for data hiding, IBM Syst. J., 35, pp.313-336.

- Bennett, K., 2004. Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text, Purdue University, CERIAS Tech.
- Bensaad Lahcen, and Yagoubi Bachir, 2011. High capacity diacritics-based method for information hiding in Arabic text, International Conference on Innovations in Information Technology, pp. 433–436.
- Böhme, R. and Westfeld, A., 2005. Exploiting preserved statistics for steganalysis, Proceedings of 6th International Workshop Information Hiding, Toronto, Canada, Lecture Notes in Computer Science, Springer, pp.82-96.
- Bors ,A. G. and Pitas, I. Median, Radial basis function neural network, IEEE Trans. Neural Networks, 7, pp. 1351-1364.
- Brassil, J. T., Low, S. and Maxemchuk, N. F. 1999. Copyright protection for the electronic distribution of text documents, Proc. of the IEEE 87(7), pp. 1181-1196.
- Cachin, C., 1998. An Information-Theoretic Model for Steganography, The Second International Workshop on Information Hiding, IH'98, 1525, pp 306-318.
- Chan, Chi-Kwong., and Cheng, L. M. 2004. Hiding data in images by simple LSB substitution. Pattern Recognition, 37, pp. 469-474.
- Chan, Chi-Kwong., and Cheng, L. M., 2001. Improved Hiding Data in Images by Optimal Moderately-Significant-Bit Replacement, IEE Eelectronics letters, 37(16), pp. 1017-1018.
- Chang Chin-Chen, Chan Chi-Shiang, and Fan Yi-Hsuan, 2006. Image Hiding Scheme with Modulus Function and Dynamic Programming Strategy on Partitioned Pixels, Pattern Recognition, 39(6) pp. 1155-1167.
- Chang, C.C., Lin, M. H., and Hu, Y. C., 2002. A fast and secure image hiding scheme based on lsb substitution,” International Journal of Pattern Recognition and Artificial Intelligence, 16(4), pp. 399-416.
- Chang, Chin-Chen., Hsiao, Ju-Yuan., and Chan, Chi-Shiang, 2003. Finding Optimal Least-Significant-Bit Substitution in Image Hiding By Dynamic Programming Strategy, Pattern Recognition, 36, pp.1538-1595.
- Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P., 2010. Digital image steganography: Survey and analysis of current methods, Signal Process., 90, pp. 727-752.
- Chen Hongyuan, and Zhu Yuesheng., 2012. A robust watermarking algorithm based on QR factorization and DCT using quantization index modulation technique, Journal of Zhejiang University-science C-computer and Electronics, 13(8), pp. 573-584.

- Chen, W., Chang, C., and Le, T., 2010. High Payload Steganography Mechanism Using Hybrid Edge Detector, *Expert Systems with applications*, 37, pp. 3292-3301.
- Chen, Yi-Hui., Pei-Yu, Lin, Eric, Jui-Lin Lu and Ping, Jung Chen, 2013. Secret Hiding Mechanism Using QR Barcode”, *International Conference on Signal-Image Technology and Internet-Based Systems*.
- Chow, C.K., and Kaneko, T., 1972. Automatic detection of the left ventricle from cineangiograms, *Computer. Biomed. Res.*, 5, pp. 388–410.
- Cole, E., 2003, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, Indiana, John Wiley and Sons Inc. *Communications of the ACM*, 47, pp. 76-82.
- Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J. and Kalker, T., 2008. *Digital Watermarking and Steganography-Second Edition*, Burlington, MA, USA, Elsevier Inc.
- Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T.G., 1997. Secure spread spectrum watermarking for multimedia, *IEEE Trans on Image Processing*, 6(12), pp.1673-1687.
- Currie, D.L. and Irvine, C.E., 1996. Surmounting the effects of lossy compression on steganography, *Proceedings of the National Information System Security Conference*, pp.194-201.
- Fard, A. M., Akbarzadeh-T, M.-R., and Varasteh-a, F., 2006. A New Genetic Algorithm Approach for Secure JPEG Steganography. 2006 *IEEE International Conference on Engineering of Intelligent Systems, ICEIS*, pp.1-6.
- Fridrich, J., 2010. *Steganography in digital media – Principles, Algorithms, and Applications*, Cambridge University Press, ISBN 978-0-521-19019-0.
- Fridrich, J., Goljan, M., and Hogeia, D, 2003. *New Methodology for Breaking Steganographic Techniques for JPEGs*, *Electronic Imaging, Security and Watermarking of Multimedia Contents*, Santa Clara, California.
- Grgic, S., Grgic, M. and Mrak, M. (2004) Reliability of objective picture quality measures, *Journal of electrical engineering*, 55, pp. 3-10.
- Gutub, A. and Fattani, M., 2007. A Novel Arabic Text Steganography Method Using Letter Points and Extensions, *WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE)*, Vienna, Austria, pp 25-27.

- Gutub, A., Al-Qahtani, A., and Tabakh, A., 2009. Triple-A: Secure RGB Image Steganography Based on Randomization, Proceedings of IEEE/ACS International Conference on Computer Systems and Applications (AICCSA, 2009), Rabat, Morocco, pp.400-403.
- Gutub, A., Ankeer M., Abu-Ghalioun M., Shaheen A., and Alvi A., 2008. Pixel Indicator high capacity Technique for RGB image Based Steganography, Proceedings of 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E.
- Hamid, A.M., Kiah L.M., Madhloom, H.T., Zaidan, B.B, and Zaidan, A.A, 2009. Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis, International Journal of Engineering and Technology (IJET),1 (2), PP. 63-69.
- Hassan, H., Sima'an, K., and Way, A., 2009. Lexicalized Semi-Incremental Dependency Parsing, Proceedings of the Conference on Recent Advances in Natural Language Processing (RANLP-2009), Borovets, Bulgaria.
- Hevner AR; March ST; Park J & Ram S., 2004. Design science in information systems research. MIS quarterly, 28 (1),pp. 75–105.
- Hsu, Fu-Hau, Min-Hao, Wu, Shiuh-Jeng, WANG, 2012. Dual-watermarking by QR-code Applications in Image Processing, 9th International Conference on Ubiquitous Intelligence and Computing.  
<http://www.sans.org/reading-room/whitepapers/steganography/steganography-steganalysis-overview-553> Accessed: July 10, 2014,
- Huang, D. and H. Yan, 2001. Interword Distance Changes Represented by Sine Waves for Watermarking Text Images, IEEE Transactions on Circuits and Systems for Video Technology, 11(12), pp. 1237-1245.
- Huang, J. Y. Q. Shi, and Shi, Y., 2000. Embedding image watermarks in DC component, IEEE Trans. Circuits Syst.: Video Technol., 10(6), pp.974 -979 .
- Huang, L. K. and Wang, M. J. J., 1995. Image thresholding by minimizing the measures of fuzziness, Pattern Recogn. 28,pp. 41–51.
- Hussain, M., and Hussain, M., 2011. Embedding data in edge boundaries with high PSNR, Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6.
- Iso-Dis, 1992. Digital Compression and Coding of Continuous-Tone Still Images - Requirements and Guidelines, CCITT Recommendation T.81.

- ITU-R-BT.500-11, 2002. Methodology for the subjective assessment of the quality of television pictures. International Telecommunication Union/ITU Radio communication Sector.
- Japanese Industrial Standards, 2004. Two Dimensional Symbol-QR-Code Basic Specification JIS X 0510.
- Jianquan, X., Qing, X., and Dazu, H., 2009. A Robust High Capacity Information Hiding Algorithm Based on DCT High Frequency Domain, Proc. Computer Network and Multimedia Technology, CNMT-2009, pp. 1-4.
- Johnson, N.F and Jajodia, S., 1998. Exploring Steganography: Seeing the Unseen, IEEE Computer, 31(2), pp.26-34.
- Jung, Ki-Hyun., Ha, Kyeong-Ju., and Yoo, Kee-Young., 2008. Image Data Hiding Method Based on Multi-Pixel Differencing and LSB Substitution Methods, In Proc., International Conference on Convergence and Hybrid Information Technology (ICHIT '08). Daejeon (Korea), pp. 355-358.
- Kahn, D., 1996. The History of Steganography, The First Workshop on Information Hiding, 1174, pp 1-5.
- Katzenbeisser, S. and Petitcolas, F., 2000. Information Hiding Techniques for Steganography and Digital Watermarking, Artech House.
- Ker, A., 2004. Improved Detection of LSB Steganography in Grayscale Images, Proc. 6th International Workshop. Toronto (Canada), Springer LNCS, 3200, pp. 97–115.
- Ker, A., 2005. Steganalysis of LSB Matching in Grey scale Images, IEEE Signal Process Letter, 12(6), pp. 441– 444.
- Kipper, G., 2003. Investigator's guide to steganography. Auerbach Publishers.
- Koch, E. and Zhao, J., 1995. Towards Robust And Hidden Image Copyright Labelling, Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Halkidiki, Greece, pp. 452–455.
- Kuhn, T., 1996. The Structure of Scientific Revolutions, Chicago: University of Chicago Press.
- Lawless, H. T., and Heymann, H., 1998. Sensory Evaluation of Food: Principles and Practices. Chapman and Hall, New York, NY, pp. 606–608.
- Lee, Y. K., and Chen, L. H., 2000. High Capacity Image Steganographic Model, IEEE Proc., Vis. Image Signal Process, 147( 3), pp. 288-294.



- Lewis, W and Allnatt J.A, 1965. Subjective quality of television pictures with multiple impairment, *Electronic Letters*, 1, pp.187-189.
- Lie Wen-Nung, and Chang Li-Chun, 1999. Data hiding in images with adaptive numbers of least significant bits based on the human visual system. *IEEE Int. Conf., Image Processing*. Kobe (Japan), pp 286-290.
- Lind, A. D., Marchal, A. W., and Wathen, A. S., *Statistical Technique in Business and Economics*, 13th Edition, 539.
- Liu Jen-Chang, and Shih Ming-Hong, 2008. Generalizations of Pixel Value Differencing Steganography For Data Hiding In Images, *Fundamental Informatics*, 83(3), pp. 319-335.
- Liu Shao-Hui, Chen Tian-Hang, Yao Hong-Xun, and Gao Wen., 2004. A Variable Depth LSB Data Hiding Technique in Images. *International Conference on Machine Learning and Cybernetics*. Shanghai (China), 7, pp. 3990-3994.
- Lou, D.-C. and Liu, J.-L., 2002. Steganographic Method for Secure Communications, *Computers and Security*, pp.449-460.
- Low, S.H., Maxemchuk, N.F., Brassil, J.T., and L. O'Gorman, 1995. Document marking and identification using both line and word shifting. *Proceedings of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies*, IEEEExplore Press, Boston, MA, USA, pp 853-860.
- Mandal ,J. K. and Debashis Das, 2012. Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain, *International Journal of Information Sciences and Techniques (IJIST)*, 2(4), pp
- Mamta, Juneja and Parvinder, S.Sandhu, 2013. An Analysis of Image Steganography Techniques in Spatial Domain, *International Journal of Computer Science and Electronics Engineering (IJCSEE)*, 1(3), pp.454-459
- March, S. T., and Smith, G. F., 1995. Design and natural science research on information technology, *Decision Support Systems*, 15(4), pp. 251–266.
- Marini, E., Autrusseau, F., Callet, P. L. and Campisi, P., 2007. Evaluation of standard watermarking techniques *Security, Steganography, and Watermarking of Multimedia Contents IX*, 6505, pp. 1-10.
- Marvel, L.M., Boncelet, C.G. and Retter, C.T., 1999. Spread spectrum image steganography, *IEEE Transactions on Image Processing*, 8(8),pp.1075-1083.
- Memon, J.A., Khowaja, K., and Kazi, H, 2005. Evaluation of Steganography for Urdu/Arabic Text, *Journal of Theoretical and Applied Information Technology*.

- Mielikainen Jarno, 2006. LSB Matching Revisited, *IEEE Signal Processing Letters*, 13(5), pp. 285-287.
- Moulin, P. and O'Sullivan A., 2003. Information-theoretic Analysis of Information Hiding, *IEEE Transactions on Information Theory* 49(3), pp.563 –593.
- Naderahmadian ,Yashar and Khayat, Saied Hosseini., 2010. Fast Watermarking Based on QR Decomposition in Wavelet Domain, *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, iih-msp, pp.127-130.
- Nakagawa, Y. and Rosenfeld, A., 1979. Some experiments on variable thresholding, *Pattern Recogn.* 11(3), 191–204.
- Niblack, W., 1986. *An Introduction to Image Processing*, Prentice-Hall, Englewood Cliffs, NJ, pp. 115–116.
- Nyman, G., Radun, J., Leisti, T., Oja, J., Ojanen, H., Olives, J.-L., Vuori, T. and Häkkinen, J., 2006. What do users really perceive - probing the subjective image quality. *Image Quality and System Performance III*, 6059-605902, pp.1-7.
- Ouaviani, E.P, Bottazzi, A.M., Brunelli, E., Caselli, F., and Guerrero, M., 1999. A common image processing framework for 2-D barcode reading, *Proc. 7th Int. Conf. Image Processing and its Applications*, 2, pp. 652–655.
- Owen, C. 1997. Design Research: Building the Knowledge Base, *Journal of the Japanese Society for the Science of Design*, 5 (2), pp.36-45.
- Owens, M. 2002. A discussion of covert channels and steganography, SANS Institute, Information Security Reading Room.
- Patton, M. Q. 2002. *Qualitative research and evaluation methods* (3 edition). Thousand Oaks, CA: Sage Publications.
- Pavlidis, T. 2000. A New Paper/Computer Interface: Two- Dimensional Symbologies, *IEEE Computer*, 2, pp. 145-151.
- Pinson, M. H. and Wolf, S., 2003. Comparing subjective video quality testing methodologies *Visual Communications and Image Processing*, 5150, pp.573-582.
- Provos, N. 2001. Defending Against Statistical Steganalysis. The 10th conference on USENIX Security Symposium.
- Provos, N. and Honeyman, P., 2003. Hide and Seek: An Introduction to Steganography. *IEEE Security and Privacy Magazine*, 1, pp. 32-44.

- Provos, N. and Honeyman, P., (2001) Detecting Steganographic Content on the Internet, CITI Technical Report, pp. 03–11.
- Rabah, K., 2004. Steganography- The Art of Hiding Data, *Information Technology Journal*, 3, pp 245-269.
- Sallee, P., 2004. Model-Based Steganography, In: Kalker, T., et al. (eds.): *International Workshop on Digital Watermarking*, LNCS 2939, Springer-Verlag, Berlin Heidelberg, pp. 154–167.
- Sauvola J. and Pietaksinen, M., 2000. Adaptive document image binarization, *Pattern Recogn.* 33, pp.225–236.
- Schneider, G.M. and Gersting, J.L., 2004. *Invitation to computer science. Course Technology.*
- Sezgin, M., and Sankur, B., 2004. Survey over image thresholding techniques and quantitative performance evaluation, *Journal of Electronic Imaging*, 13 (1), 146-165.
- Sheikh, H. R., Sabir, M. F. and Bovik, A. C., 2006. A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms. *IEEE Transactions on Image Processing*, 15, pp. 3440-3451.
- Shirali-Shahreza, M. H. and Shirali-Shahreza S., 2006. Persian/Arabic Text Font Estimation Using Dots," *Proceedings of the 6th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2006)*, Vancouver, Canada, pp. 420-425.
- Shirali-Shahreza, M. H. and Shirali-Shahreza, S., 2008. A New Synonym Text Steganography, *The 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1524-1526.
- Shirali-Shahreza, M., 2008. Text Steganography by Changing Words Spelling. *10th International Conference on Advanced Communication Technology*, pp.1912-1913.
- Silman, J. (2001). *Steganography and steganalysis: an overview.*
- Simmons, G. J., 1983. The Prisoners' Problem and the Subliminal Channel. *CRYPTO'83*, pp 51-67.
- Simone, F. D., Goldmann, L., Baroncini, V. and Ebrahimi, T., 2009. Subjective evaluation of JPEG XR image compression Applications of Digital Image Processing XXXII, 7443-744301, pp. 1-12

- Soo, T. J., 2008. QR Code, *Synthesis Journal*, pp.59-78.
- Stanley, C.A., 2005. Pairs of Values and the Chi-squared Attack, in *CiteSteer*, pp. 1-45.
- Stoica, A., Vertan, C. and Fernandez-Maloigne, C., 2003. Objective and subjective color image quality evaluation for JPEG 2000 compressed images, *International Symposium on Signals, Circuits and Systems*, pp. 137-140.
- Swanson, M. D. Zhu, B. and Tewfik, A. H., 1996. Robust data hiding for images, in *Proc. IEEE Digital Signal Processing Workshop*, Loen, Norway, pp. 37-40.
- Swanson, M. Zhu, B. and Tewfik, A., 1996. Transparent robust image watermarking, *IEEE International Conference on Image Processing*. Piscataway, NJ: IEEE Press, 3, pp. 211-214.
- T. Liang and F. Zhi-jun, (2008) An adaptive middle frequency embedded digital watermark algorithm based on the dct domain, *Pattern Recognition*, vol. 40, pp. 2408 - 2417.
- Thien, C. C., and Lin, J. C., 2003, A Simple and High-Hiding Capacity Method for Hiding Digit-By-Digit Data in Images Based On Modulus Function, *Pattern Recognition*, 36, pp. 2875-2881.
- Vaishnavi, V. and Kuechler, W., 2009. *Design Science Research in Information Systems*. DESRIST.org. Available at: <http://desrist.org/desrist>.
- Van Aken, J.E., 2005. Management research as a design science: Articulating the research products of mode 2 know edge production in management. *British Journal of Management*, 16, pp.19-36.
- Venkatraman, S., Abraham, A. and Paprzycki, M., 2004. Significance of Steganography on Data Security, *The International Conference on Information Technology: Coding and Computing (ITCC)*, 2, pp.347-351.
- Wakahara, Toshihiko; Yamamoto, Noriyasu, 2011. Image Processing of 2 Dimensional Barcode, *14th International Conference on Network-Based Information Systems*.
- Wallace, G.K., 1991. The JPEG Still Picture Compression Standard. *Communications of the ACM*, 34, pp. 30-44.
- Wang Ran-Zan, Lin Chi-Fang, and Lin Ja-Chen, 2000. Hiding Data in Images by Optimal Moderately Significant Bit Replacement, *IET Electronics Letters*, 36(25), pp. 2069-2070.
- Wang Ran-Zan, Lin Chi-Fang, Lin Ja-Chen, 2001. Image Hiding by Optimal LSB Substitution And Genetic Algorithm, *Pattern Recognition*, 34, pp. 671-683.

- Wang, H. and Wang, S., 2004. Cyber Warfare: Steganography vs. Steganalysis.
- Wang, Z. A., Bovik, C., Sheikh, H. R., and Simoncelli, E. P., 2004 Image quality assessment: From error measurement to structural similarity, *IEEE Trans. Image Processing*, 13( 4), pp.59-78.
- Wang, Z., Bovik, A. C. and Lu, L. 2002a. Why is image quality assessment so difficult? *IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '02)*, 4, pp. 3313-3316.
- Wang, Z., Sheikh, H. R. & Bovik, A. C. 2002b. No-reference perceptual quality assessment of JPEG compressed images. *Proceedings of the International Conference on Image Processing*, 1, pp.477-480.
- Wayner, P., 2002. *Disappearing Cryptography, Information Hiding: Steganography and Watermarking-Second Edition*, San Francisco, CA, USA, Elsevier Science.
- Weiss, M, 2009. Principles of Steganography. <http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf>  
Accessed: July 10, 2014
- Westfeld, A. and Pfitzmann, A., 2000. Attacks on steganographic systems, in *Information Hiding: 3rd International Workshop, IH'99 Dresden, Germany*, Springer-Verlag, Berlin Heidelberg LNCS 1768, pp. 61–76.
- Westfeld, A., 2001. High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm). In: Moskowitz, I.S. (eds.): *Information Hiding. 4th International Workshop. Lecture Notes in Computer Science*, Springer-Verlag, Berlin Heidelberg New York, 21(7), pp. 289-302.
- White ,J. M. and Rohrer, G. D., 1983. Image thresholding for optical character recognition and other applications requiring character image extraction, *IBM Journal of Research and Development* 27, pp. 400–411.
- Wu, D.C. and Tsai, W. H., 2003. A Steganographic Method for Images by Pixel-Value Differencing, *Pattern Recognition Letter*, 24 (10), pp. 1613–1626.
- Wu, H. R. and Rao, K. R., 2006. *Digital Video Image Quality and Perceptual Coding*, CRC Press.
- Wu, H.C., Wu, N.I., Tsai, C.-S., Hwang, M.S 2005, Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods, *IEE Proceedings-Vision, Image and Signal Processing*, 152 (5), pp. 611-615.

- Wu, N.-I. and Hwang, M.-S., 2007. Data Hiding: Current Status and Key Issues. *International Journal of Network Security*, 4, pp. 1-9.
- Yang, C. H., Weng, C. Y., 2006. A Steganographic Method for Digital Images by Multi-Pixel Differencing. In *Proc. International Computer Symposium*. Taipei (Taiwan), pp. 831-836.
- Yang, Cheng-Hsing., Weng Chi-Yao., Wang, Shiuh-Jeng., and Sun, Hung-Min., 2008. Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems, *IEEE Transactions on Information Forensics and Security*, 3(3), pp. 488-497.
- Yu, Y.-H., Chang, C.-C. & Hu, Y.-C., 2005. Hiding Secret Data in Images via Predictive Coding. *Pattern Recognition*, 38, pp. 691-705.
- Yung-Chen Chou, Chin-Chen Chang, and Kuan-Ming Li, 2008. A Large Payload Data Embedding Technique for Color Images, *Fundamental Informatics*, 88 (2), pp47-61.

**Error! Reference source not found.**