HYBRID DOCUMENT COPYRIGHT PROTECTION

NOR FATIN SHAZWANI BINTI ADNAN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: HYBRID DOCUMENT COPYRIGHT PROTECTION

SESI PENGAJIAN: 2020 / 2021

Saya: NOR FATIN SHAZWANI BINTI ADNAN

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (✓)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
_____	TIDAK TERHAD	

(TANDATANGAN PELAJAR)

Alamat tetap:

NO.33 JALAN DATO AHMAD RAZALI 21A/KS13, KG TELUK NIPAH, 42920, KLANG, SELANGOR

Tarikh: 8 September 2021

(TANDATANGAN PENYELIA)

PM TS DR. SITI RAHAYU BINTI SELAMAT
Nama Penyelia

Tarikh: 11 September 2021

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

HYBRID DOCUMENT COPYRIGHT PROTECTION

NOR FATIN SHAZWANI BINTI ADNAN

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Security) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2021

DECLARATION

I hereby declare that this project report entitled

HYBRID DOCUMENT COPYRIGHT PROTECTION

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : NOR FATIN SHAZWANI BINTI ADNAN DATE : 8 SEPT 2021

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of Computer Science (Computer Security) with Honours.

DEDICATION

This research is dedicated to my beloved father, who taught me to keep learning even in a difficult situation as long as there is a chance because knowledge is something precious we can have. It is also dedicated to my dearest mother, who taught me to never give up on what I am currently doing. She taught me that even the smallest progress is still considered progress and with the smallest progress I will be able to complete the task.

ACKNOWLEDGEMENTS

All praises to Allah with His Permission and Grace, I am able to complete this final year project report.

First of all, I would like to express my deepest gratitude to my supervisor, Prof. Madya TS Dr. Siti Rahayu Binti Selamat for her guidance, advice, encouragement, and supportive comments throughout the process of completing this project. Without my supervisor's help, I might not be able to complete this report and project successfully.

In addition, my utmost appreciation goes to my beloved parents, Mr. Adnan Bin Husain and Mrs. Norasila Binti Sanip, who have been giving me continuous support and motivation throughout my project. Indeed, without their ongoing support and encouragement, I would not be here.

Lastly, I would also like to take this opportunity to thank all my friends for lending hands every time I need it. Especially, Muhammad Hafiz Bin Jamil, Wan Nurin Jazmina Binti Wan Omar, and Amirah Nadhirah Binti Kamarulzaman, thank you for all the reminders, encouragement, care, guidance, and support. Thank you for inspiring me to finish this project. Words cannot express my gratitude for all your love and support.

ABSTRACT

The E-Learning system has made it easier for lecturers to share their digital lecture notes with the students. Students can access them from their lecturers anywhere and anytime. However, these digital lecture notes are vulnerable to illegal copy and unauthorized distribution because they do not have copyright protection. Therefore, to solve the problem, a QR code technology and a steganography technique have been applied as a mechanism of document protection. In this implementation, the information of the owner's file and the person who downloaded the file are stored and hidden in the QR Code and steganography image. In addition, a UTeM logo also was embedded as a watermark to provide multiple protection to the digital lecture notes. With this information, if the digital lecture notes are misused or distributed on a public platform without the permission of their lecturer, the user who distributed the files can be identified by scanning the QR code contained in that particular file. With that information, the owner of the digital lecture notes also can be proven.

ABSTRAK

Sistem *E-Learning* memudahkan pensyarah berkongsi nota kuliah digital mereka dengan pelajar. Pelajar boleh mendapatkannya dari pensyarah di mana sahaja dan pada bila-bila masa. Walau bagaimanapun, nota kuliah digital ini terdedah kepada salinan haram dan pengedaran yang tidak dibenarkan kerana mereka tidak mempunyai perlindungan hak cipta. Oleh itu, untuk menyelesaikan masalah ini, teknologi Kod QR dan teknik steganografi telah digunakan sebagai mekanisme perlindungan dokumen. Dalam pelaksanaan ini, maklumat fail pemilik dan orang yang memuat turun fail disimpan dan tersembunyi dalam Kod QR dan imej steganografi. Di samping itu, logo UTeM juga dimasukkan sebagai tera air untuk memberi perlindungan berganda kepada nota kuliah digital. Dengan maklumat ini, jika nota kuliah digital disalahgunakan atau diedarkan di platform awam tanpa kebenaran pensyarah mereka, pengguna yang mengedarkan fail boleh dikenal pasti dengan mengimbas kod QR yang terkandung dalam fail tersebut. Dengan maklumat itu, pemilik nota kuliah digital juga boleh dibuktikan.

TABLE OF CONTENTS

DECLARATION ..... **ii**
DEDICATION ..... **iii**
ACKNOWLEDGEMENTS ..... **iv**
ABSTRACT ..... **v**
ABSTRAK ..... **vi**
LIST OF TABLES ..... **xi**
LIST OF FIGURES ..... **xiv**
LIST OF ABBREVIATIONS ..... **xviii**
CHAPTER 1: INTRODUCTION **1**
1.1. Introduction 1
1.2 Project Background 1
1.3 Problem Statement (PS) 2
1.4 Project Question (PQ) 2
1.5 Project Objective (PO) 2
1.6 Project Scope 3
1.7 Project Contribution 3
1.8 Report Organization 4
1.9 Summary 5
CHAPTER 2: LITERATURE REVIEW **6**
2.1 Introduction 6
2.2 Digital Document 7
2.3 Protection Technique 8
2.3.1 Watermarking Technique 10
2.3.2 Steganography Technique 11
2.4 Basic of QR Code 12
2.5 Analysis of QR Code Applications in Information Security Perspective ... 16
2.6 Proposed solution 23
2.7 Summary 23
CHAPTER 3: PROJECT METHODOLOGY **24**

3.1 Introduction 24
3.2 Methodology 24
3.2.1 Literature Review 25
3.2.2 Analysis 25
3.2.3 Formulate Hybrid Protection Technique 25
3.2.4 Embedded Protection Techniques into document 26
3.2.5 Implementation 26
3.2.6 Testing 26
3.3 Project Schedule and Milestone 27
3.3.1 Gantt Chart 27
3.3.2 Milestone 30
3.4 Summary 31
CHAPTER 4: ANALYSIS AND DESIGN 32
4.1 Introduction 32
4.2 Requirement 32
4.2.1 Software Requirement 32
4.2.2 Hardware Requirement 33
4.3 System Architecture Design 34
4.4 QR Code Generator Design 37
4.4.1 Data Input 38
4.4.2 Analyzing Input Data 39
4.4.3 Data Encoding 40
4.4.4 Creating Error Correction Codewords 46
4.4.5 Structuring Final Data 47
4.4.6 Converting Block into QR Matrix 47
4.4.7 Apply Mask Pattern 48
4.4.8 Apply Version and Format Information 48
4.5 Steganography Image Generator Design 48
4.5.1 Determine data and image 49
4.5.2 Data Encoding 49
4.5.3 Determine Image Properties 50
4.5.4 Extract RGB color from the image 50
4.5.5 Inject data to image 51
4.6 Design for Embedding Images into Document 51

4.6.1 Import Document 51
4.6.2 Determine Document Page to Insert The Images 52
4.6.3 Import Images 52
4.6.4 Embed The Images Into Document 53
4.7 Summary 53
CHAPTER 5: IMPLEMENTATION 54
5.1 Introduction 54
5.2 Software Development Environment Setup 54
5.2.1 Web Application Manager 54
5.2.2 Database Manager 55
5.2.3 Visual Studio Code (VS Code) Setup 55
5.3 Implementation 57
5.3.1 QR code Generator 58
5.3.2 Steganography Image Generator 71
5.3.3 Embedding The Images into Document 76
5.4 Summary 88
CHAPTER 6: TESTING 89
6.1 Introduction 89
6.2 QR Code Generator Testing 89
6.3 Steganography Image Generator Testing 96
6.4 Embed Image into Document Testing 101
6.5 QR Code Image Testing 106
6.5.1 Completeness of data 107
6.5.2 Usability 109
6.6 Steganography image Testing 114
6.6.1 Completeness of data 114
6.6.2 Imperceptibility 117
6.7 Summary 119
CHAPTER 7: PROJECT CONCLUSION 120
7.1 Introduction 120
7.2 Project summarization 120
7.3 Project contribution 121
7.4 Project limitation 121
7.5 Future works 122

7.6 Summary 122
REFERENCES 124

LIST OF TABLES

PAGE

Table 1. 1: Summary of problem statement 2
Table 1. 2: Summary of project question 2
Table 1. 3: Summary of the project objective 3
Table 1. 4: Summary of the project contribution 3
Table 2. 1: Digital document protection technique 8
Table 2. 2: Data capacity of QR code (Espejel-Trujillo et al., 2012) 13
Table 2. 3: Summary of the QR code application in information security perspective 20
Table 3. 1: Gantt chart 27
Table 3. 2: Project Milestone 30
Table 4. 1: The list of software used with the description 33
Table 4. 2: The list of hardware used with the description 33
Table 4. 3 : Pseudocode for inserting required information into the QR code .. 39
Table 4. 4: Alphanumeric table 39
Table 4. 5: ECC level (Denso Wave Incorporated, 2021) 41
Table 4. 6: QR code version with maximum allowable capacity (Denso wave Incorporated, 2021) 41
Table 4. 7: Indicator mode for respective data type (Denso wave Incorporated, 2021) 42
Table 4. 8: Character count indicator according to the version and data type (Thonky, 2021) 43
Table 4. 9: Break phrase into pairs 43
Table 4. 10: Data encoding based on respective data type 44
Table 4. 11: Current bit string of the example 44
Table 4. 12: Error correction codewords (Thonky, 2021) 44

Table 4. 13: Terminator is added **45**
Table 4. 14: Arranged encoded data **45**
Table 4. 15: Required bytes for the example **46**
Table 4. 16: Encoded data in decimal and polynomial **47**
Table 4. 17: ASCII Table **49**
Table 4. 18: Example to encode data **50**
Table 5. 1: Pseudocode for Data Input Process **59**
Table 5. 2: Pseudocode for Analyzing Alphanumeric Data type **60**
Table 5. 3: Pseudocode for Alphanumeric Encoding **60**
Table 5. 4: Pseudocode for creating error correction codewords **61**
Table 5. 5: Pseudocode to structure final data in a block **63**
Table 5. 6: Pseudocode placement of finder pattern and separator **64**
Table 5. 7: Pseudocode to place timing pattern and alignment pattern **65**
Table 5. 8: Pseudocode to mask data **66**
Table 5. 9: Pseudocode to apply version and format information **67**
Table 5. 10: Pseudocode resizing logo image and set logo image transparency . **69**
Table 5. 11: Pseudocode for determine data and image **72**
Table 5. 12: Pseudocode for encoding message **73**
Table 5. 13: Pseudocode to reset image properties **73**
Table 5. 14: Pseudocode for extract rgb color of image inject data to image **75**
Table 5. 15: Javascript Pseudocode to pass material and user id **79**
Table 5. 16: Pseudocode to obtain user id and material location **80**
Table 5. 17: Pseudocode to check the file information **80**
Table 5. 18: Pseudocode for determining page to insert the images **81**
Table 5. 19: Pseudocode for passing QR code image path and the resizing value **82**
Table 5. 20: Pseudocode for checking image file type **82**
Table 5. 21: Pseudocode for checking image file **83**
Table 5. 22: Pseudocode to read png image stream **84**
Table 5. 23: Pseudocode to determine color type of the image **85**
Table 5. 24: Pseudocode define path for embedded document **87**
Table 5. 25: Pseudocode for calling Output() function **87**
Table 5. 26: Pseudocode to return output as pdf document to a new window ... **87**

Table 6. 1: Properties for data completeness 107
Table 6. 2: Data completeness of QR code analysis 109
Table 6. 3: User Usability Testing 110
Table 6. 4: Analysis of user usability testing on QR code 113
Table 6. 5: Data completeness properties 114
Table 6. 6: Data completeness of steganography image analysis 117
Table 6. 7: Visibility Testing Analysis 118

LIST OF FIGURES

PAGE

Figure 2. 1: Overview of literature review 6
Figure 2. 2: Classification of Watermarking Technique (Tiwari & Sharmila, 2017) 11
Figure 2. 3: Component of QR code (Pal & Kumar, 2021) 13
Figure 2. 4: Overview of QR code process (Tiwari, 2016) 14
Figure 2. 5: Encoding step (Tiwari, 2016) 14
Figure 2. 6: Decoding step (Tiwari, 2016) 15
Figure 3. 1: Methodology 24
Figure 4. 1: System Architecture 34
Figure 4. 2: Flowchart of the main module 35
Figure 4. 3: User interface of view student assignment submission 35
Figure 4. 4: User interface of student assignment submission 36
Figure 4. 5: User interface that contains lecture note and lab sheet 36
Figure 4. 6: ERD of the system 37
Figure 4. 7: QR code generator design 38
Figure 4. 8: Inject data into image design 48
Figure 4. 9: Embed images with document design 51
Figure 5. 1: Laragon setting 54
Figure 5. 2: Add phpMyAdmin folder to Laragon File 55
Figure 5. 3: VS Code extensions 56
Figure 5. 4: Setup Database Connection in VS Code 56
Figure 5. 5: Established Database Connection in VS Code 57
Figure 5. 6: System architecture 57
Figure 5. 7: Flowchart main process for the QR code generation 58
Figure 5. 8: Data module is structured in QR matrix 66

Figure 5. 9: Generated QR code 69
Figure 5. 10: QR code image with UTeM logo 71
Figure 5. 11: Flowchart of steganography image generation..... 71
Figure 5. 12: Flowchart for Embedding the images into a document 76
Figure 5. 13: Student user interface to download lecture note 77
Figure 5. 14: Student user interface to download lab material and submit assignment..... 77
Figure 5. 15: Lecturer user interface to manage their material 78
Figure 5. 16: Lecturer user interface to review open submission..... 78
Figure 5. 17: Lecturer user interface to review student submission 79
Figure 5. 18: Downloaded file 88
Figure 6. 1: QR code generator testing process.....89
Figure 6. 2: Download lecture note from the student side 90
Figure 6. 3: Generated QR code for lecture note (student)..... 90
Figure 6. 4: Generated QR code with UTeM's logo for lecture note (student) .. 90
Figure 6. 5: Download Lab document from the student side..... 91
Figure 6. 6: Generated QR code for lab document (student)..... 91
Figure 6. 7: Generated QR code with UTeM's logo for lab document (student)91
Figure 6. 8: Download student submission document from the student side 92
Figure 6. 9:Generated QR code for student submission document (student) 92
Figure 6. 10: Generated QR code with UTeM's logo for student submission document (student) 92
Figure 6. 11: Download lecture note from lecturer side 93
Figure 6. 12: Generated QR code for lecture note (lecturer)..... 93
Figure 6. 13: Generated QR code with UTeM's logo for lecture note (lecturer) 93
Figure 6. 14: Download Lab document from lecturer side 94
Figure 6. 15: Generated QR code for lab document (lecturer)..... 94
Figure 6. 16: Generated QR code with UTeM's logo for lab document (lecturer) 94
Figure 6. 17: Download student submission document from lecturer side..... 95
Figure 6. 18: Generated QR code for student submission document (lecturer). 95
Figure 6. 19: Generated QR code with UTeM's logo for student submission document (lecturer)..... 95
Figure 6. 20: Steganography image generator testing process 96

Figure 6. 21: UTeM's logo used as a container of hidden information 96
Figure 6. 22: Downloadable lecture note document UI from student's perspective 97
Figure 6. 23: Generated steganography image for lecture note document from student's perspective 97
Figure 6. 24: Downloadable lab document UI from student's perspective 97
Figure 6. 25: Generated steganography image for lab document from student's perspective 98
Figure 6. 26: Downloadable student's assignment document UI from student's perspective 98
Figure 6. 27: Generated steganography image for student's assignment document from student's perspective 98
Figure 6. 28: Downloadable lecture note document UI from lecturer's perspective 99
Figure 6. 29: Generated steganography image for lecture note document from lecturer's perspective 99
Figure 6. 30: Downloadable lab document UI from lecturer's perspective 99
Figure 6. 31: Generated steganography image for lab document from lecturer's perspective 100
Figure 6. 32: Downloadable student's assignment document UI from lecturer's perspective 100
Figure 6. 33: Generated steganography image for student's assignment document from lecturer's perspective 100
Figure 6. 34: Embed QR code image and steganography image into document testing process 101
Figure 6. 35: The user interface for a lecture note document that can be downloaded from the student's viewpoint 101
Figure 6. 36: Lecture note document with QR code image, watermark image, and steganography image embedded within it from the student's viewpoint .. 102
Figure 6. 37: The user interface for a lab document that can be downloaded from the student's viewpoint 102
Figure 6. 38: Lab document with QR code image, watermark image, and steganography image embedded within it from the student's viewpoint 103

Figure 6. 39: The user interface for student's submission document that can be downloaded from the student's viewpoint 103
Figure 6. 40: Student's submission document with QR code image, watermark image, and steganography image embedded within it from the student's viewpoint 104
Figure 6. 41: The user interface for a lecture note document that can be downloaded 104
Figure 6. 42: Lecture note document with QR code image, watermark image, and steganography image embedded within it from the Lecturer's viewpoint 104
Figure 6. 43: The user interface for a lab document that can be downloaded from the lecturer's viewpoint 105
Figure 6. 44: Lab document with QR code image, watermark image and steganography image embedded within it from the lecturer's viewpoint..... 105
Figure 6. 45: The user interface for a student's assignment document that can be downloaded from the lecturer's viewpoint 106
Figure 6. 46: Student's assignment document with QR code image, watermark image, and steganography image embedded within it from the lecturer's viewpoint 106
Figure 6. 47: Information of 'Adlina Kadir' from Database..... 107
Figure 6. 48: Information of owner file and submission date from System 108
Figure 6. 49: Information of source file 108
Figure 6. 50: Student submission document named 'assignment_adlina.pdf'' 108
Figure 6. 51: Result after scan the QR code 109
Figure 6. 52: User interface for message extraction..... 114
Figure 6. 53: Information of lecturer 'Nor Azman Abu' from Database..... 115
Figure 6. 54: File owner and submission date information from System 115
Figure 6. 55: The file source information..... 115
Figure 6. 56: The student's submission document named 'assignment_adlina.pdf' 116
Figure 6. 57: Outcome of the QR code scanning 116
Figure 6. 58: Steganography Image..... 116
Figure 6. 59: Extraction of message in steganography image 117
Figure 6. 60: Zoom in document 118

LIST OF ABBREVIATIONS

UTeM	**-**	**Universiti Teknikal Malaysia Melaka**
UiTM	**-**	**Universiti Teknologi Mara**
Covid-19	**-**	**Coronavirus Disease 2019**
QR-code	**-**	**Quick Response Code**
LSB	**-**	**Least Significant Bits**
ISO/IEC	**-**	**International Organization For Standardization/International Electrotechnical Commission**
2D code	**-**	**2 Dimensional Code**
RSA	**-**	**Rivest-Shamir-Adleman Encryption**
VSS	**-**	**Visual Secret Sharing**
DWT	**-**	**Discrete Wavelet Transform**
HH	**-**	**Higher Highs**
HL	**-**	**Higher Lows**
LH	**-**	**Lower Highs**
LL	**-**	**Lower Lows**
DCT	**-**	**Discrete Cosine Transform**
HE	**-**	**Histogram Attack**
JPEG	**-**	**Joint Photographic Experts Group**
SVD	**-**	**Singular Value Decomposition**
ID	**-**	**Identification**
ERD	**-**	**Entity Relationship Diagram**
PHP	**-**	**Personal Home Page**
SQL	**-**	**Structured Query Language**
RAM	**-**	**Random Access Memory**

LCD	**-**	**Liquid Crystal Display**
IPS	**-**	**In-Plane Switching**
GHz	**-**	**Gigahertz**
PnP	**-**	**Plug and Play**
ECC	**-**	**Error Correction Capability**
Char	**-**	**Character**
RGB	**-**	**Red, Blue, Green**

CHAPTER 1: INTRODUCTION

1.1. Introduction

Nowadays, online learning is a common way used by the educational industry to deliver their contents to their students because all the country has been hit by the Covid-19 Pandemic. Therefore, all universities have their own online learning platform. For example, U-Learn and i-Learn are the online platforms used by UTeM and UiTM respectively. With the online learning platform, lecturers can upload their material to be used by their students to be accessed anywhere and anytime. This also provides a convenient environment for both of them. However, several issues should be considered to ensure the materials provided are protected and not misused by the students. Therefore, this project is proposed to protect the materials provided by lecturers from any misuse by their students. Hence, this chapter will explain the background, problem, objectives, and significance of the project.

1.2 Project Background

Online learning has long been practiced by many universities, but its uses have increased since the hit of Covid-19 Pandemic. As a result, teaching and learning have been done digitally and using an online learning platform. According to Abdul Rahman et al. (2020), the implementation of teaching and learning activities online can help reduce the risk of Covid-19 infection because it is carried out virtually. As such, the use of digital documents has also increased as it is facilitating the teaching and learning process. However, although the use of digital documents in an online learning platform facilitates all parties, some issues can occur, such as copyright issues and misuse of the lecturer's teaching materials. Therefore, it is important to digitally secure those digital documents from these issues. In the meantime, this project will use a QR code and a steganography image to store information about who download the

document, the owner of the document, and the source of the document as it is simple and reliable just for academic purposes.

1.3 Problem Statement (PS)

Since the Covid-19 pandemic, teaching and learning have been done online. So, all notes and study materials from the lecturer have been uploaded to the online learning platform to make it easier for students to download and study in their respective places. However, the possibility for cases such as misuse of the lecturer's material by distributing it on the public platform without the permission of their lecturer can occur. Nowadays, there are also many public online platforms to share assignments and notes like Coursehero, Quizlet, and Quizizz. Apart from that, some of the lecturers also less consent about the copyright issue because they trust if the material is shared in that platform (such as U-Learn), it will be just between the student only, not with other people. The problem here is, we do not know who is the real person that shares the lecturer's material, where it might cause some problem for the lecturers later. For example, someone can publish a book using the lecturer's study material content.

Table 1. 1: Summary of problem statement

PS	Problem Statement
PS1	Current online learning situation is causing the misused of the lecturer's material and do not know who is behind it.

1.4 Project Question (PQ)

Based on the problem statements listed in Table 1.1, three project question (PQ) are constructed as shown in Table 1.2.

Table 1. 2: Summary of project question

PQ	Project Question
PQ1	What copyright protection technique can be used for documents?
PQ2	How to protect the digital documents from any illegal activities?
PQ3	How to measure the effectiveness of the proposed protection technique?

1.5 Project Objective (PO)

The aim of this project is to secure the lecturer's material. Therefore, to be able to

solve the problem identified in Table 1.1 and to achieve the aim of this project, three project objectives (PO) are derived as shown in Table 1.3.

Table 1. 3: Summary of the project objective

PQ	PO	Project Objective
PQ1	**PO1**	To analyze copyright protection techniques for documents
PQ2	**PO2**	To formulate hybrid copyright protection technique
PQ3	**PO3**	To evaluate the effectiveness of the proposed protection technique

1.6 Project Scope

The main purpose of this project is to generate a QR code and a steganography image that contains information about the user that downloads the document and embeds it into the lecturer material in order to find out who holds that document in case the document is misused by someone. The document also will be embedded with UTeM's logo as a watermark. A system has been developed for the testing part. The document supported to upload to the system is digital materials and the format of the document is .pdf. This project is targeting students and lecturers as this system is an online learning platform. This project will focus on how to solve the problem as stated in the problem statement with the use of QR code technology, steganography, and watermarking technique.

1.7 Project Contribution

Based on the problem statement, project question, and project objectives listed in Table 1.1, Table 1.2, and Table 1.3 respectively, three project contributions (PC) are constructed as shown in Table 1.4.

Table 1. 4: Summary of the project contribution

PS	PQ	PO	PC	Project Contribution
PS1	**PQ1**	**PO1**	**PC1**	Techniques to protect the digital documents from illegal activities or misuse activities
	PQ2	**PO2**	**PC2**	A protected document that embedded with QR code, watermark image and steganography image
	PQ3	**PO3**	**PC3**	The identity of the document's ownership