

**UNIVERSITI TEKNOLOGI MARA**

**DCT DOMAIN STEGASVM-SHIFTED  
LSB MODEL FOR HIGHLY  
IMPERCEPTIBLE AND ROBUST  
COVER-IMAGE**

**HANIZAN SHAKER HUSSAIN**

**PhD**

**August 2014**

## **AUTHOR'S DECLARATION**

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

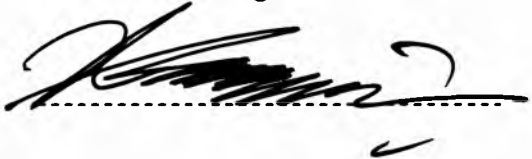
Name of Student : Hanizan Shaker Hussain

Student I.D. No. : 2008763271

Programme : Philosophy of Doctorate (IT)

Faculty : Computer and Mathematical Sciences

Thesis Title : DCT Domain StegaSVM-Shifted LSB  
Model for Highly Imperceptible and  
Robust Cover-image

Signature of Student : 

Date : August 2014

## ABSTRACT

The importance of information security in protecting data and information has increased due to the increased use of computers and the Internet. Similarly, with one of its exciting subfields i.e. information hiding. Information hiding is a technology where the secret-messages are hidden inside other files (e.g image files). One of the areas that are popular now applying this technology is digital image steganography (image steganography). In image steganography, the most popular and widely used techniques is the least significant bit (LSB) that hide data into a cover-image in a spatial and discrete cosine transform (DCT) domain as well. Beside the LSB technique, there is other technique that is also influential i.e support vector machine (SVM) normally used to strengthen the embedding algorithm. Whatever techniques used in the image steganography field, the main purpose is to keep the existence of the secret-message secret. But many of the techniques previously proposed have failed to attain this main purpose. The primary concern that contribute to this problem is the non-random changes on a cover-image that constantly occurred after the embedding process. Secondly, the non-robustness of embedding algorithm to image processing operation. Therefore in this research, the new model is proposed called StegaSVM-Shifted LSB model in DCT domain to preserve the imperceptibility and increase the robustness of stego-images. The StegaSVM-Shifted LSB model that has been proposed that utilize HVS and embedding technique through Shifted LSB showed a good performance. This can be seen when PSNR record high value, where it displays a good quality cover-image with 48.94dB while high quality robustness for secret-message with NC value is about 1.0. Therefore, StegaSVM-Shifted LSB model were acceptable in which it shows a higher quality steganography, thus enhancing the performance of existing works. In extracting process, by exploiting the SVM learning ability, the right secret-bits can be recovered.

## TABLE OF CONTENTS

	<b>Page</b>
<b>AUTHOR'S DECLARATION</b>	<b>ii</b>
<b>ABSTRACT</b>	<b>iii</b>
<b>ACKNOWLEDGEMENT</b>	<b>iv</b>
<b>TABLE OF CONTENTS</b>	<b>v</b>
<b>LIST OF TABLES</b>	<b>viii</b>
<b>LIST OF FIGURES</b>	<b>ix</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xii</b>
<b>LIST OF NOTATIONS</b>	<b>xiii</b>
<b>CHAPTER ONE: INTRODUCTION</b>	
1.1 Background of the Research	1
1.2 Statement of the Problem	3
1.3 Research Questions	7
1.4 Objectives of the Research	7
1.5 Scope of the Research	7
1.6 Significance of the Research	8
1.7 Research Approach	10
1.8 Organization of Thesis	11
<b>CHAPTER TWO: LITERATURE REVIEW</b>	
2.1 Introduction	13
2.2 Information Hiding	13
2.3 Steganographic Techniques	14
2.4 <i>Image Steganographic Domains</i>	16
2.5 <i>Image Steganographic Requirements</i>	17
2.6 <i>Image Steganographic Techniques</i>	19
2.7 Soft Computing (SC) in Information Hiding	25
2.8 Support Vector Machines (SVM)	30
2.9 SVM Works in Image Information Hiding	38

2.10	Attacks on Image Steganography	44
2.11	Image Steganography Evaluations	45
2.12	Summary	49
<b>CHAPTER THREE: RESEARCH METHODOLOGY</b>		
3.1	Introduction	51
3.2	Methodological Framework	51
3.3	Experimental Design	59
3.4	Summary	77
<b>CHAPTER FOUR: PROPOSED DESIGN</b>		
4.1	Introduction	78
4.2	Proposed Design Model	78
4.3	Summary	91
<b>CHAPTER FIVE: DEVELOPMENT</b>		
5.1	Introduction	92
5.2	StegaSVM Classification Stage	92
5.3	StegaSVM-Shifted LSB Embedding Stage	119
5.4	StegaSVM-Shifted LSB Extracting Stage	128
5.5	Summary	132
<b>CHAPTER SIX: RESULTS AND DISCUSSIONS</b>		
6.1	Introduction	133
6.2	Imperceptibility Requirement	133
6.3	Robustness Requirement	142
6.4	Summary	148
<b>CHAPTER SEVEN: CONCLUSIONS AND RECOMMENDATIONS</b>		
7.1	Conclusion	149
7.2	Contributions of the Research	151
7.3	Recommendation for the Extension of the Research	153