بسم الله الرحمن الرحيم

DECLARATION

I declare that this thesis entitled on "**Enhancing Image Steganography for Secure Communication**" is the result of my own research except as cited in the reference. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

DEDICATION

Dedications to **ALLAH SWT**

With blessings, love, and respect for those who helped us reach the level of excellence at which we are all now, we look forward to a bright future.
&

To our respected

PARENTS

&

respected

TEACHERS

For their unconditional support & encouragement & inspiration, that made us able

for this thesis work.

CERTIFICATE

This is to certify that Mr./ Miss_____D/o, S/o_____Roll No:_____Finalyear student of Bachelor of Science Information Technology) has completed the Partial requirement of the Project / Thesis during session, 2023-24. The Title of the project is "Enhancing Image Steganography for Secure Communication" and it is submitted to the Quaid-e-Awam University of Engineering. Science & Technology Nawab Shah for the Degree of Bachelor of Science, Information Technology Department.

Supervisor

Dr. Saima Siraj Soomro

Department of Information Technology

Chairman

Prof. Dr. Mukhtiar Ahmed Memon

Department of Information Technology

External Examiner

ACKNOWLEDGEMENT

We are deeply grateful to our supervisor **Dr. Saima Siraj Soomro** for her continuous support in the selection of our project topic. Her guidance and encouragement helped us make decisions throughout our project idea selection and led us to a successful idea for our project. We thank our supervisor at Quaid-E-Awam University of Engineering, Science and Technology Nawab Shah for staying with us, helping us, and guiding us with our FYP. Also, we would like to thank our supervisor Dr. Saima Siraj Soomro for her support and guidance at various stages, from the research proposal to project idea selection.

Table of Contents

DECLARATION	(III)
DEDICATION	(IV)
CERTIFICATE	(V)
ACKNOWLEGMENT	(VI)
TABLE OF CONTENTS	(VII)
CHAPTERS	(VIII)
LIST OF TABLES	(XII)
LIST OF FIGURES	(XIII)
ABSTRACT	(XV)

CHAPTER NO.01 INTRODUCTION **1**

1.1 INTRODUCTION TO IMAGE STEGANOGRAPHY 1

1.2 Image Stenography Basics 7

1.3 Encoding and Decoding Functions 8

1.3.1 Image Selection 9

1.3.2 Message Input 9

1.3.3 Encoding Option 10

1.3.4 Decoding Option 10

1.4 Problem Statement 12

1.5 Objective 12

1.6 Structure of the Thesis 12

CHAPTER NO.02: LITERATURE REVIEW 14

2.1 Introduction 14

2.2 Historical Background 14

2.3 Early Methods 14

2.3.1 Ancient Greece and Rome 15

2.3.2 Wooden Tablets and Wax 15

2.3.3 Invisible Ink 16

2.3.4 Cipher Codes 17

2.4 Existing Stenography Technique 19

2.4.1 Least Significant Bit (LSB 19

2.4.2 Discrete Cosine Transform (DCT) 21

2.4.3 Spread Spectrum 23

2.4.4 Phase Coding 24

2.5 Comparative Analysis- Strengths 26

2.5.1 Least Significant Bit (LSB) 26

2.5.2 Discrete Cosine Transform (DCT) 27

2.5.3 Spread Spectrum 27

2.5.4 Phase Coding 27

2.6 Comparative Analysis 28

2.7 Review of Significant Research Papers 29

2.7.1 Enhancing Security with Compression and Encryption 29

2.7.2 Watermarking in the Frequency Domain 29

2.7.3 Detecting LSB Steganography 30

2.7.4 Robustness of Spread Spectrum Techniques 30

2.7.5 Use of Wavelet Transforms 30

CHAPTER NO.03 RESEARCH METHODOLOGY 32

3.1 Introduction 32

3.2 Requirement Gathering and Analysis 34

3.3 Design 34

3.4 Overview of the Steganography Workflow 36

3.4.1 Data Hiding Process 36

3.4.1.1. User Authentication 36

3.4.1.2 Data Encryption 36

3.4.1.3 Cover Image Selection 37

3.2.4.4 Steganography Algorithm Application 37

3.2.4.5 Stego Image Creation 38
3.4.2 Data Retrieving Process 38
3.4.2.1 Stego Image Input 38
3.4.2.2 Secret Key Utilization 38
3.4.2.3 Data Extraction 39
3.4.2.4 Decryption 39
3.3 Development 40
3.4 Testing 42
3.5 Deployment 42
3.6 User Feedback and Maintenance 43
3.7 Proposed Algorithm 43
3.8 Data Hiding Process 44
3.9 Data Retrieval Process 44
3.10 Security Features 44

CHAPTER NO.4 RESULTS AND DISCUSSIONS 46

4.1 Encode Functionality 46
4.1.1 Choose Image 47
4.1.2 Select Secret Key 48
4.1.3 Enter Message 49
4.1.4 Encoding Process 50
4.1.5 Output Image 51
4.2 Decode 52
4.2.1 User Interface Overview 52
4.2.2 Choose Image 53

4.2.3 Input Secret Key 54

4.2.4 Decoding Process 55

4.2.5 Displaying the Hidden Message 55

4.3 Analysis and Discussion 55

4.3.1 Security Considerations 55

4.3.2 Usability and Performance 56

4.3.3 Limitation 56

4.4 Conclusion 56

CHAPTER NO.05 CONCLUSION AND FUTURE WORK 57

5.1 Conclusion 57

5.2 Future Work 58

LIST OF TABLES

Table No 1.1 :	The Diff: Between Steganography And Cryptography	04
Table No 1.2 :	Functionality For Encoding and Decoding	11
Table No 2.1 :	Methods of Stenography	18
Table No 2.2 :	Existing Stenography Techniques	25
Table No 2.3 :	Comparative Analysis Table	28
Table No 2.4 :	Review of significant research paper	31
Table No 3.1 :	Proposed Algorithm	45

LIST OF FIGURES

Figure 1.1:	Image Steganography [31]	02
Figure 1.2:	Cryptography [32]	06
Figure 1.3:	Encoding and Decoding Functions [33]	08
Figure 1.4:	Encoding and Decoding Options [34]	10
Figure 2.1:	Invisible Ink [35]	16
Figure 2.2:	Cipher Codes [36]	17
Figure 2.3:	Least Significant Bit [37]	20
Figure 2.4:	Discrete Cosine Transform [38]	22
Figure 3.1:	Workflow of the Novel Steganography Algorithm [39]	33
Figure 3.2:	Algorithm for embedding data inside image [40]	35
Figure 3.3:	Algorithm for extracting data from stego image [41]	35
Figure 3.4	The main interface for SIS [42]	41
Figure 3.5	The secret key is required for SIS [43]	41
Figure 3.6	(a) Original image (b) Stego image [44]	42
Figure 3.7	(a) Original image (b) Stego image [45]	42
Figure 4.1:	Encode and Decode Functionality [46]	46
Figure 4.2:	Choose Image [47]	47

Figure 4.3:	Secret Key [48]	48
Figure 4.4:	Enter Message [49]	49
Figure 4.5:	Encoding Process [50]	50
Figure 4.6:	Decode Functionality [51]	52
Figure 4.7:	Choose Image [52]	53
Figure 4.8:	Decode Secret Key [53]	54

ABSTRACT

Steganography, the process of concealing a secret message within a larger, seemingly innocuous one, plays a critical role in information security by ensuring that the existence of the hidden message remains undetectable. Unlike encryption, which obscures the content of a message, steganography masks the very presence of communication. This thesis focuses on the application of steganography in digital images to unintended observers.

The research investigates the advantages of steganographic techniques, particularly their ability to provide a simple yet effective security mechanism. Since the hidden message is seamlessly integrated within an ordinary digital image. This characteristic makes steganography a valuable tool for secure communication, digital watermarking, and copyright protection.

This thesis provides a comprehensive analysis of current steganographic methods, comparing their effectiveness in terms of data embedding capacity, image quality preservation, and resistance to detection. Moreover, novel enhancements to existing algorithms are proposed, aiming to improve the robustness and efficiency of data concealment.