Bio-Inspired Optimization Algorithms for Image Steganographic and Cryptographic Applications

A thesis submitted

in fulfillment of the requirement for the award of degree

of

Doctor of Philosophy

Submitted by

Ajay Kumar

Registration Number: 901506016

Under the Supervision of

Dr. Alpana Agarwal

Professor, ECED

Dr. Abhijit Karmakar

Chief Scientific Officer
IIT, Jodhpur

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY, PATIALA-147004

December 2024

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "**Bio-Inspired Optimization Algorithms for Image Steganographic and Cryptographic Applications**", for the award of the degree of **Doctor of Philosophy** in Electronics and Communication Engineering Department (ECED), Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision and guidance of Dr. Alpana Agarwal, Professor, ECED, Thapar Institute of Engineering and Technology, Patiala, and Dr. Abhijit Karmakar, Chief Scientific Officer, IIT Jodhpur (Formerly Chief Scientist and Professor, CSIR-CEERI, Pilani).

The results presented in this thesis have not been submitted in part or in full to any other University or Institute for the award of any degree or diploma.

Ajay Kumar
901506016

This is to certify that the above statement made by the candidate is correct to the best of my knowledge and belief.

Dr. Alpana Agarwal
Professor, ECED
Thapar Institute of Engineering and Technology,
Patiala, India.

Dr. Abhijit Karmakar
Chief Scientific Officer
Indian Institute of Technology
Jodhpur, India.

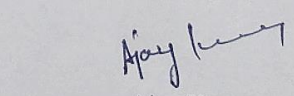
ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere, humble and deep sense of gratitude to my supervisors **Dr. Alpana Agarwal**, Professor, Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala and **Dr. Abhijit Karmakar**, Chief Scientific Offier, IIT Jodhpur (Formerly Chief Scientist, CSIR-CEERI, Pilani) for his support and motivation throughout the course of this research work. From last six years of research, I am unable to find any occasion when he could not spare time to discuss the problems related to my research. The enthusiastic supervision and beneficial remarks during inspiring discussions helped a lot to the accomplishment of this thesis.

I am highly grateful to **Dr. Manu Bansal,** Assistant Professor**, Dr. Anil Singh,** Assistant Professor for his continuous support and encouragement in my research work. Moreover, I am also grateful to my doctoral committee members **Dr. Sanjay Kumar**, Associate Professor, **Dr. Rishikesh Pandey**, Associate Professor in ECED, TIET, Patiala and **Dr. Anil Kumar Verma**, Professor, Department of Computer Science and Engineering, TIET, Patiala for their valuable suggestions during my entire research. I am also immensely thankful to my fellow researchers Vikas Thakur, Gurwinder Singh, Kiranjit Kaur, Rohit at Thapar Institute of Engineering and Technology, Patiala for helping me throughout my research.

I want to thank my parents for their love, affection, and support. It is only because of them I would able to face difficult times in my life. I am also extremely thankful to my wife Suman for understanding and providing me enough time to complete my research work.

This research work is supported by the Visvesvaraya PHD scheme for Electronics and IT, Ministry of Electronics and Information Technology, Government of India under Grant PhD-MLA/4(33)/2015-16/01. I would like to express my gratitude to the Ministry of Electronics and Information Technology for providing the financial support, without which it would not be possible for me to carry out this research work.



Ajay Kumar

ii

ABSTRACT

The multimedia data communication in the form of images is done in different applications, namely, healthcare, defense, and satellite. These images are prone to numerous attacks on the communication channel, such as statistical attacks and differential attacks. These attacks are overcome by adding the security layer to the multimedia data using steganography, encryption, and hybrid methods based on it. The steganography methods hide the secret data in the cover media, whereas encryption methods scramble the secret data using a random key. Further, in the hybrid methods, the secret data is encrypted and then hidden in the cover image. Hence, in this research, these security methods are investigated to find out the challenges of the existing algorithms and enhance them using the bio-inspired algorithms. In the literature, numerous authors used the bioinspired algorithm to enhance the security methods. However, in the literature, several bio-inspired algorithms are available, and selection of the most optimum algorithm is a challenging task. In this research, the most optimal bio-inspired algorithms, namely, Egyptian Vulture Optimization (EVO), Green Heron Optimization (GHO), and Black Widow Optimization (BWO), are chosen due to their better exploration rate, minimum parameter tuning, and better convergence rate. Based on these algorithms, security methods in the fields of steganography, encryption, and hybrid approaches based on them are designed in this research.

In this research work, two security methods are designed to enhance the security parameter known as imperceptibility for image steganography applications. In the first method, three parameters are determined before data hiding, such as optimal cover image index, block index, and secret data index, using the bio-inspired algorithms (EVO, GHO, and BWO), which were not claimed by other authors in the previous studies. On the other hand, in the second method, the secret data bits are matched with cover image LSB bits, and the matched index is determined. Thereafter, the matched index is hidden in the same cover image in the optimal way using the bio-inspired algorithm by finding the best starting index in the cover image and optimal secret data index. The bio-inspired algorithm searches the best indexes based on the objective function. In our work, the parameter mean square error (MSE) is taken as the objective function. Further, the benefit of the proposed image steganography method is that it is suitable for single- and multi-bit data embedding. The simulation evaluation of the image steganography method is done on the standard USC SIPI Image Database images. Further, for the evaluation purposes, several grayscale and color images are taken into consideration. Next, the evaluation is done based on subjective and objective analysis. In the subjective analysis, based on the visual quality, original cover images and their histograms are compared with the output images known as stego images. On the other hand, in the objective analysis, several performance parameters, namely, mean square error (MSE), root mean square error (RMSE), peak signal to noise ratio (PSNR), structure similarity index measure (SSIM), correlation coefficient (CC), entropy, university image quality (UIQ) index, image fidelity (IF), and normalized absolute error (NAE), are used to analyze the characteristics of the stego image with respect to the cover image. The result shows that the proposed image steganography method achieves high SSIM, CC, UIQI, IF near to one value, low MSE, RMSE, NAE near to

zero value, and approximates similar entropy between cover and stego image as required in the steganography. Besides that, the proposed method achieves better PSNR without degrading the payload capacity as compared to existing methods.

Two security methods are proposed next to overcome the statistical and differential attacks on the secret data for image encryption applications. In the first method, a random key of 512- bits is generated using the bio-inspired BWO algorithm for data encryption. The benefit of the BWO algorithm is that it searches for the best key among the *n* number of keys based on the objective function. Subsequently, this key is utilized in the image encryption method to perform substitution, permutation, and key scheduling steps. Besides that, the BWO mutation operation is performed in the permutation step. On the other hand, in the second method, the BWO algorithm searches the best parameter values of the chaotic logistic map for key generation based on the objective function. After that, an exclusive-OR operation is performed between the secret image pixel and the random key. Next, the encrypted matrix is randomly circularly shifted horizontally and vertically to achieve permutation. In both methods, entropy is taken as the objective function. The simulation evaluation is done in the standard USC SIPI image database. In the evaluation, several images are taken into consideration. The result shows that the encrypted image is found to be completely noisy from visual analysis, and its histograms are equally distributed. On the other hand, in the objective analysis, the proposed methods achieve high entropy (~7.999) close to the ideal value and also high number of pixels change rates (NPCR) (~99%) with a low correlation coefficient (near to zero value) and PSNR (near to 8-12 dB). Further, comparative analysis shows that the proposed method outperforms in terms of entropy and NPCR over the existing methods.

Next, a privacy-preserving method is designed by hybridizing the image encryption and steganography methods. The novelty of the proposed privacy-preserving method is that the same evolutionary BWO algorithm is used for key generation, for secret data encryption, and for optimized data hiding. The benefit of the proposed method comes from the fact that the cover image plane chosen to hide the encrypted data is not fixed, as it is determined based on the pixel intensity value. Moreover, in the proposed method, only sensitive information about the user is encrypted. The visual analysis shows that the input and output images are similar, and the objective analysis shows that the cover plane and optimal starting pixel index are not static, achieving better PSNR (in the range of 54.1579-54.3132 dB*)*, high CC, SSIM, IF, UIQI (near to 0.999 value), and similar entropy is obtained between input and output image. The proposed methods are useful for anyone who wants to communicate secret data in a more secure way.

LIST OF PUBLICATIONS

SCI/SCIE Journal Publications:

1. Ajay Kumar, Abhijit Karmakar, Alpana Agarwal, "Privacy-Preserving Method for Public Health Surveillance Data using Image Steganography," *Tobacco Regulatory Science*, vol. 7, no. 6-1, pp. 6814-6830, 2021.
2. Ajay Kumar, Abhijit Karmakar, Alpana Agarwal, "Improved Chaotic Logistic Map Algorithm based on Bio-Inspired Algorithm for Image Encryption," *Tobacco Regulatory Science*, vol. 8, no. 1, pp.1915-1928, 2022.

SCOPUS Journal Publication:

1. Ajay Kumar, Abhijit Karmakar, Alpana Agarwal, "Optimized Data Hiding Technique using Egyptian Vulture Optimization Algorithm for Image Steganography," *Design Engineering*, vol. 7, pp. 12525-12541, 2021.

LIST OF ABBREVIATIONS

ABC	Artificial Bee Colony
ACO	Ant Colony Optimization
AES	Advanced Encryption Standard
BBBCO	Big Bang Big Crunch Optimization
BBMO	Bumble Bee Mating Optimization
BI	Block Index
BIO	Bio-Inspired Optimization
BWO	Black Widow Optimization
CC	Correlation Coefficient
CI	Cover Index
CLM	Chaotic Logistic Map
CR	Cannibalism Rate
CRO	Chemical Reaction Optimization
CSO	Cat Swarm Optimization
DE	Differential Evolution
DES	Data Encryption Standard
DRPE	Double Random-Phase Encoding
EC	Evolutionary Computation
ECC	Elliptic Curve Cryptography
EVO	Egyptian Vulture Optimization
FN	Feistel Network
GA	Genetic Algorithm
GHO	Green Heron Optimization
GO	Grasshopper Optimization
GSA	Gravitational Search Algorithm
HS	Histogram Shifting
HVS	Human Visual System
LFSR	Linear Feedback Shift Register
LSB	Least Significant Bit
MD	Maximum Deviation
MR	Mutation Rate
MSE	Mean Square Error

NPCR	Number of Pixel Change Rate
PR	Procreate Rate
PRNG	Pseudorandom Random Key Generator
PSNR	Peak Signal to Noise Ratio
PSO	Particle Swarm Optimization
PVD	Pixel Value Difference
ROI	Region of Interest
SDI	Secret Data Index
SPN	Substitution-Permutation Network
TLBO	Teaching-Learning-Based Optimization
TRNG	True Random Number Generator

LIST OF SYMBOLS

N_{var}	Solution of the Optimization Problem
P_{red}	Pixel Value of Red
P_{green}	Pixel Value of Green
P_{blue}	Pixel Value of Blue
α	Alpha
P	Maximum Possible Intensity Value of a Pixel
O	Original Image
OI	Output Image
p	Probability of the Histogram
c	Histogram of the Encrypted Image
P_{mean}	Mean Value of the Original Image
E_{mean}	Mean Value of the Encrypted Image
D	Difference between Encrypted Image
χ^2	Chi Square Test

LIST OF FIGURES

Figure No.	Description of the Figure	Page No.
1.1	Block Diagram of Image Encryption and Decryption	4
1.2	Domains of Image Encryption	4
1.3	Block Diagram of Steganography	6
1.4	Properties of Steganography	7
1.5	Classification of Steganography	8
1.6	Block Diagram of the LSB Method	11
1.7	Block Diagram of the *k*-bits LSB Method	11
1.8	Stego Images for *k*-bit LSB Methods	11
1.9	Block Diagram of the Hybridization of Cryptography and Steganography	12
1.10	Flowchart of the Bio-Inspired Optimization Algorithm	14
1.11	Classification of Bio-Inspired Optimization Algorithm	15
2.1	Steps of Egyptian Vulture Optimization Algorithm	30
2.2	Flow Diagram for GHO Algorithm	31
2.3	Baiting Operation (a) Catch (b) Miss Catch (c) After False Catch	32
2.4	Change of Position Operation	32
2.5	Attracting Prey Swarms Operation (a) Original String (b) Left Circular Shifted the String by 5	32
2.6	Flowchart of Black Widow Optimization Algorithm	33
3.1	Flipped Secret Data Form	41
3.2	Swapped Secret Data Form	41
3.3	Circular Shift Secret Data Form	42
3.4	Block Diagram of Data Embedding using Swarm Intelligence Algorithms	43
3.5	Block Diagram of Data Extraction for Swarm Intelligence Algorithms	44
3.6	Flowchart of Data Embedding in Matching Method	67
3.7	Block Diagram of Data Extraction for Matching Method	70

4.1	*n* Number of Cover Images	87
4.2	(a) Cover Image Blocks (b) Rearrangement of the Cover Image Blocks	88
4.3	Flowchart of the Proposed Data Embedding Method using BWO Algorithm	88
4.4	Flowchart of the Data Extraction Method using BWO Algorithm	89
5.1	Flowchart of the Image Encryption using BWO Algorithm and its Operation	112
5.2	Block Diagram of Proposed Image Encryption Method based CLM Algorithm	121
6.1	Block Diagram of the Proposed Privacy-Preserving Method	133
6.2	Performance Evaluation of the Proposed Method based on CC, SSIM, IF, and UIQI Parameter	142
6.3	Performance Evaluation of the Proposed Method based on Input and Output Entropy	142
6.4	Performance Evaluation of the Proposed Method based on MSE, RMSE, NAE	143

LIST OF TABLES

Table No.	Description of the Table	Page No.
3.1	Initial Parameter Values of the EVO/GHO Algorithm for Determine Optimal Secret Data and Cover Image Index	45
3.2(a)	Subjective Analysis of the EVO Algorithm for the Proposed Data Hiding Method	46
3.2(b)	Subjective Analysis of the GHO Algorithm for the Proposed Data Hiding Method	47
3.3(a)	Subjective Analysis based on the Histogram of the EVO Algorithm (for Grey-Scale Images)	48
3.3(b)	Subjective Analysis based on the Histogram of the GHO Algorithm (for Grey-Scale Images)	49
3.3(c)	Subjective Analysis based on the Histogram of the EVO Algorithm (for Color Images)	50
3.3(d)	Subjective Analysis based on the Histogram of the GHO Algorithm (for Color Images)	51
3.4(a)	Objective Analysis of the EVO Algorithm (For Grey-Scale Images)	53
3.4 (b)	Objective Analysis of the GHO Algorithm (for Grey-Scale Images)	54
3.5 (a)	Objective Analysis of the EVO Algorithm (For Color Images)	55
3.5 (b)	Objective Analysis of the GHO Algorithm (For Color Images)	58
3.6(a)	Cover Index, Block Index, and Secret Data Index for EVO/GHO Algorithms (for Grey Scale Images)	61
3.6(b)	Cover Index, Block Index, and Secret Data Index for EVO/GHO Algorithms (for Color Images)	62
3.7	MSE and PSNR for Different Data Embedding	63
3.8(a)	Comparison of Proposed and Existing Algorithms [38] in terms of PSNR (in dB)	63
3.8(b)	Comparison of Proposed and Existing Algorithms [115] in terms of PSNR (in dB)	64
3.8(c)	Comparison of Proposed and Existing Algorithms [116] in terms of PSNR (in dB)	64
3.9	Performance Metrics for different Intentional/Non-Intentional Attacks on the Proposed Method	65

3.10	Initial Parameter Values of the EVO/GHO Algorithm for Matching Method	70
3.11	Subjective Analysis of the Matching Method for EVO/GHO Algorithm (for Grey-Scale Image)	71
3.12	Subjective Analysis of the Matching Method for EVO/GHO Algorithm (for Color Images)	73
3.13(a)	Objective Analysis of the Matching Method for EVO Algorithm (for Grey-Scale Images)	76
3.13(b)	Objective Analysis of the Matching Method for EVO Algorithm (for Color Images)	77
3.14(a)	Objective Analysis of the Matching Method for GHO Algorithm (for Grey-Scale Images)	80
3.14(b)	Objective Analysis of the Matching Method for GHO Algorithm (for Color Images)	81
3.15	Comparison of Proposed and Existing Algorithms in terms of PSNR (in dB)	84
4.1	Parameter Values of BWO Algorithm to Find the Optimal Cover Image, Block, and Secret Data Index	91
4.2	Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Grey-Scale Image)	92
4.3	Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Color Images)	93
4.4 (a)	Optimal Selected Cover Image, Block Order, and Secret Data Index based on BWO Algorithm (for Grey-Scale Image)	96
4.4 (b)	Optimal Selected Cover Image, Block Order, and Secret Data Index based on BWO Algorithm (for Color Image)	97
4.5 (a)	Objective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Grey-Scale Image)	98
4.5 (b)	Objective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Grey-Scale Image)	99
4.6	EC vs. PSNR for the Proposed Method	102
4.7 (a)	Comparative Analysis of the Proposed Image Steganography Method based on BWO Algorithm with the Existing Steganography Methods [38] based on PSNR Value	103
4.7 (b)	Comparison of Proposed and Existing Algorithms [115] in terms of PSNR (in dB)	103
4.7 (c)	Comparison of Proposed and Existing Algorithms [116] in terms of PSNR (in dB)	104

4.8	Performance Metrics for different Intentional/Non-Intentional Attacks	105
5.1	Parameter Values of BWO Algorithm for Key Generation and Encryption	113
5.2	Subjective Analysis of the Proposed Image Encryption Method based on BWO Algorithm	114
5.3(a-b)	Histogram Analysis of the Proposed Image Encryption Method based on BWO Algorithm	115
5.4	Chi-Square Test for the Proposed Image Encryption Method based on BWO Algorithm	117
5.5	Objective Analysis for the Proposed Image Encryption Method based on BWO Algorithm	118
5.6	Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on NPCR Value	119
5.7	Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on Entropy Value	119
5.8	Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on Correlation Coefficient Value	120
5.9	Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on Execution Time (in Seconds)	120
5.10	Parameter Values of BWO Algorithm for Determine Optimal Parameter Values of CLM Algorithm	123
5.11(a-d)	Subjective Analysis of the Image Encryption Method based CLM Algorithm	123
5.12	Objective Analysis for the Image Encryption Method based CLM Algorithm	128
5.13	Comparative Analysis of Proposed Image Encryption Method based on CLM Algorithm and Existing Methods based on based on Entropy Parameter	129
5.14	Comparative Analysis of Proposed Image Encryption Method based on CLM Algorithm and Existing Methods based on based on NPCR Parameter	129
6.1	Secret Data Index Value and its Description	135
6.2(a)	Parameter Values of BWO Algorithm in the Proposed Privacy-Preserving Method for Key Generation	136

6.2(b)	Parameter Values of BWO Algorithm in the Proposed Privacy-Preserving Method for Optimal Secret Data Index and Starting Pixel in the Cover Image	136
6.3	Selected Plane, Optimal Starting Pixel, and Secret Data Index for Proposed Privacy-Preserving Method	137
6.4(a-b)	Subjective Analysis of the Proposed Privacy-Preserving Method	138
6.5	Objective Analysis of the Proposed Privacy-Preserving Method	141
6.6	Comparative Analysis with the Proposed Privacy-Preserving Method	143

TABLE OF CONTENTS

Certificate……...i

Acknowledgments……..……..ii

Abstract……..…….……iii

List of Publications……...…….....v

List of Abbreviations……...……vi

List of Symbols…….……..viii

List of Figures…… ix

List of Tables……...……xi

Table of Contents……...……....xv

Chapter 1: Introduction……1-16

1.1 Background and Motivation……1

1.2 Image Cryptography……2

1.2.1 Image Encryption and Decryption…….....3

1.2.2 Domains of Image Encryption…….....4

1.3 Image Steganography……..5

1.3.1 Data Embedding and Extraction Procedure of Steganography……6

1.3.2 Properties of Steganography……7

1.3.3 Classification of Steganography……..8

1.3.4 Image Security Methods based on Steganography……..10

1.4 Hybridization of Cryptography and Steganography Methods……...12

1.5 Bio-Inspired Optimization……..13

1.5.1 Objective Function……..15

1.5.2 Selection Criteria for Bio-Inspired Optimization Algorithm……..16

1.6 Dissertation Outline……....16

Chapter 2: Literature Survey……...….19

2.1 Introduction……....19

2.2 Related Work on Image Encryption….……..19

2.3 Related Work on Image Steganography……21

2.4 Related Work on Hybrid the Cryptography and Steganography Methods……..22

2.5 Research Gaps……23

2.6 Objectives……..…….24

2.7 Dataset, Evaluation Platform and Performance Evaluation Parameters……..25
2.7.1 Standard Dataset……..25
2.7.2 Software Tools and Platforms……26
2.7.3 Performance Analysis Parameters……...26
2.8 Bio-Inspired Optimization Algorithms Utilized in this Research……29
2.8.1 EVO Algorithm……30
2.8.2 GHO Algorithm……...31
2.8.3 BWO Algorithm……..33
2.9 Contributions of the Research Work……..35
2.10 Chapter Summary……37
Chapter 3: Image Steganography Method based on Swarm Intelligence Algorithms….38
3.1 Introduction……38
3.2 Proposed Approaches of Image Steganography based on Swarm Intelligence Algorithms.39
3.3 Optimal Secret Data Index and Cover Index Finding Method……40
3.3.1 Optimal Secret Data Index……...40
3.3.2 Optimal Cover Image Index……42
3.3.3 Data Embedding and Extraction based on the Swarm Intelligence Algorithms……43
3.3.4 Results and Analysis……44
3.4 Data Matching Method & Hiding the Matched Index in an Optimal Way……66
3.4.1 Data Embedding and Extraction for the Data Matching Method……67
3.4.2 Results and Analysis for the Data Matching Method……70
3.5 Conclusion……..84
Chapter 4: Image Steganography method based on Evolutionary Algorithm……85
4.1 Introduction……..…….85
4.2 Proposed Image Steganography Method based on Evolutionary Algorithm…….……86
4.2.1 Secret Data Index…….……...87
4.2.2 Cover Image Index……..……87
4.2.3 Data Embedding and Extraction Method……..…..88
4.3 Results and Analysis……..…90
4.3.1 Subjective Analysis…….....90
4.3.2 Objective Analysis…….96

4.3.3 Embedding Capacity Vs. PSNR……....102

4.3.4 Comparative Analysis……102

4.3.5 Intentional/Non-Intentional Attacks……..104

4.4 Conclusion……105

Chapter 5: Evolutionary Algorithm based Key Generation for Image Encryption……107

5.1 Introduction……..……107

5.2 Proposed Methods based on BWO Algorithm……..109

5.3 Image Encryption Method based on BWO Algorithm and its Operation…….110

5.3.1 Results and Analysis……..112

5.3.2 Comparative Analysis with the Existing Image Encryption Methods……..119

5.4 Image Encryption using Chaotic Map Algorithm……121

5.4.1 Determination of Optimal Parameter Values using BWO Algorithm……122

5.4.2 Results and Analysis for the Chaotic Logistic Map Algorithm…….122

5.4.3 Comparative Analysis of the Proposed Image Encryption Method based on Chaotic Logistic Map Algorithm with the Existing Encryption Methods……..129

5.5 Conclusion……130

Chapter 6: Privacy-Preserving Method based on Hybridization of Cryptography and Steganography Algorithms…….……131

6.1 Introduction…….…….131

6.2 Cover Image Plane Selection……131

6.3 Proposed Privacy-Preserving Method……..132

6.3.1 Key Generation using BWO Algorithm……134

6.3.2 Optimal Secret Data Index and Starting Pixel in the Cover Image using BWO Algorithm……...…134

6.4 Results and Analysis……135

6.5 Conclusion……....144

Chapter 7: Conclusions ……...145

7.1 Key Contributions and Findings……..145

7.2 Limitations of the Work……147

7.3 Scope for Future Work…….147

References…….149

Chapter 1

Introduction

1.1 Background and Motivation

The internet is the most preferred communication medium for transmission and reception of data such as in the form text, speech, image, or video, from one place to another. Due to the advancement of technology, the amount of data communication on the internet has increased exponentially. This has resulted in large amount of information of common people being transmitted on the internet. The data contains sensitive information such as, health care parameters, financial transactions, and vital identification parameters of individuals. This information is accessed by a number of authenticated parties or business enterprises such as by telecom, e-commerce, and transportation companies for specific purposes. In many cases, the personal information of the people is accessed by various parties, whether required or not. Further, the information shared is breached, quite often, on the internet and is prone to numerous attacks, leading to data tampering, unauthorized use or further misuse.

The two important security measures that are used to ensure data confidentiality, data authenticity and data integrity are cryptography and steganography. The cryptography algorithms encrypt the data using a private key, whereas the steganography algorithms hide the data in the cover media to make it imperceptible to the attacker [1-2]. The security of a cryptography algorithm depends on the encryption algorithm and the private key. In the earlier times, various conventional cryptography algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Blowfish were deployed for data encryption. These algorithms are superior for encrypting text information [3-5]. On the other hand, images contain some inherent features such as huge number of data pixels, strong correlation between adjacent pixels, and high redundancy between pixels [6]. Also, this is to be noted that in the current scenario, data communication is done, majorly, in the form of images or videos rather than in text. Thus, the deployment of conventional cryptography algorithms provides inferior quality of security. Besides that, private keys are generated using conventional algorithms such as linear and non-linear feedback shift registers, RSA, and Fibonacci series in the literature [7-

10]. However, these algorithms generate non-random keys if the input parameters are not chosen appropriately and the output key remains fixed.

On the other hand, in steganography, the most popular data-hiding algorithm is the least significant bit (LSB) method. The LSB algorithm substitutes the least significant bit of the cover media with the secret data bit [11]. Further, a *k*-bit LSB algorithm is proposed in which *k*-bits of the LSB of the cover medium are substituted with secret data bits. The *k*-bit LSB algorithm provides better data hiding capacity than the LSB algorithm; but it provides higher variability that negatively impacts the imperceptibility parameter [12]. Besides that, the cover media scanning order and starting pixel of the data hiding are fixed. In addition, the secret data order is also fixed. Thus, it is easy for the attacker to break the steganography algorithm.

To overcome these limitations of image cryptography and steganography, bio-inspired optimization algorithms are being used for these data security applications [13-14]. The biologically-motivated optimization algorithms are inspired by the living organisms for their survival purposes, and have been employed in several applications [15]. The characteristics are studied by researchers, based on which the optimization methods have been developed that are known as bio-inspired optimization algorithms. Further, in recent years, bio-inspired optimization algorithms have gained in popularity over traditional optimization methods any complex problem can be optimized according to the desired requirements. The bio-inspired algorithms are differentiated from each other based on their search process, number of parameters required and their tuning [16].

In our work, we have tried to obtain a set of optimal bio-inspired algorithms and incorporate them for image cryptography and steganography applications that quickly explore the search space to find the optimal solution based on the chosen objective function with minimum number of parameters.

1.2 Image Cryptography

The use of cryptography in writing can be traced back to at least 1900 BC, when an Egyptian scribe employed a non-standard form of the hieroglyphic alphabet to convey information. Experts disagreed on when exactly cryptography first originated, but mostly agreed that it was developed for use in everything from diplomatic letters to military strategy documents after the invention of writing. When computers and the internet became widely usable for

communication, it was natural that new cryptographic techniques would emerge. Cryptography is important in the data and communications fields whenever data is sent over a medium that can't be trusted, like the Internet and other networks. To ensure the safety of any data exchanged between programs, there are some essential conditions that must be met [17].

- **Confidentiality:** Confidentiality is defined as the protection of the sender's privacy and the contents of the message from anyone other than the recipient.
- **Authentication:** Proof of one's identification is called "authentication." Name-based or address-based authentication are now the most common methods of host-to-host authentication on the Internet, however, they are both extremely insecure.
- **Integrity:** It makes sure that the recipient gets a copy of the message that hasn't been changed from the original.
- **Non-repudiation:** It ensures the original sender cannot deny sending the communication.

Thus, not only the main data is safeguarded from theft or tampering, but cryptography might also be employed for the authentication process. The following sections cover the three main categories of cryptographic systems used for these purposes, namely, “hash functions”, “secret-key cryptography”, and “public-key cryptography”. The original, unencrypted data is always called "plaintext." The information is encrypted into ciphertext and then decrypted back into plaintext.

1.2.1 Image Encryption and Decryption

Image encryption and decryption methods are used to securely transmit the secret image over the internet and retrieve it in its original form on the receiver side. The block diagram of image encryption and decryption is shown in Figure 1.1. Initially, the secret image and key are read and given to the encryption method. The encryption method performs various operations on the secret image, such as substitution and permutation, and gives the encrypted image as the output. The encrypted image is communicated on the communication channel through the internet. On the receiver side, the encryption image along with the key are given to the decryption method. The decryption method performs inverse operations on the encrypted image that were performed on the encryption method and gives the original secret image at the output [18].

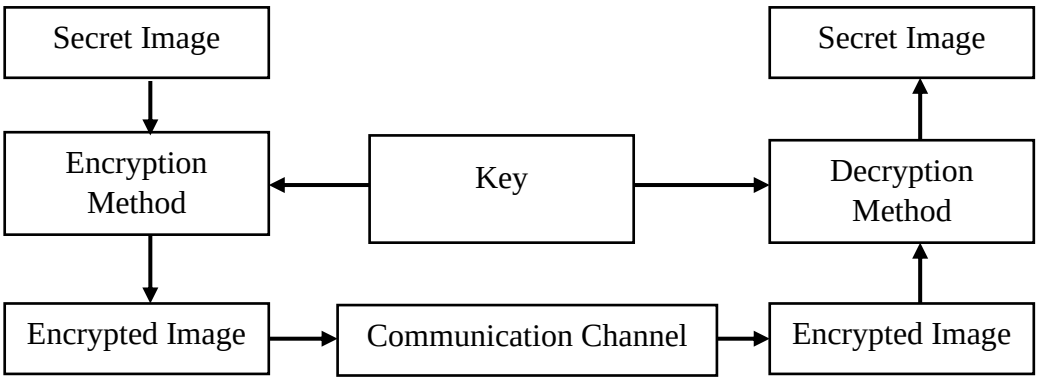


Figure 1.1: Block Diagram of Image Encryption and Decryption (Adapted from [18])

1.2.2 Domains of Image Encryption

The image encryption methods are classified into four types based on domains. These domains are spatial, transform, optimal, and compressive sensing, as shown in Figure 1.2. These domains are described below.

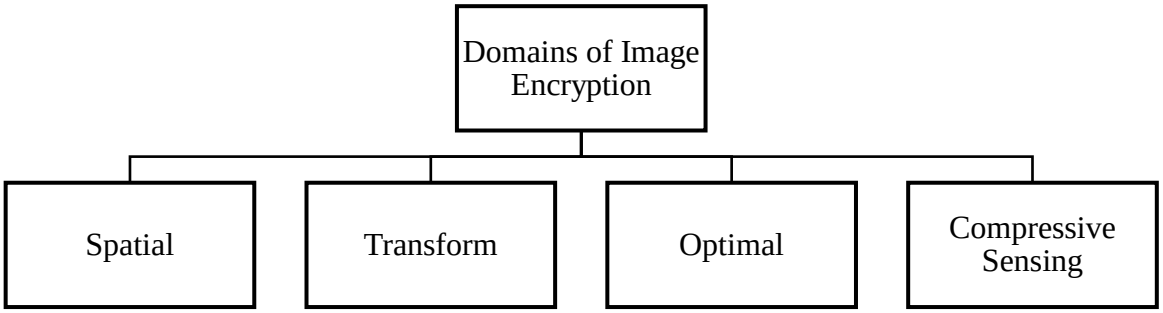


Figure 1.2: Domains of Image Encryption (Adapted from [18])

- **Spatial Domain:** In the spatial domain, the secret image pixels are operated directly for encryption purposes. In most of the image encryption methods, while encrypting an image, the secret image pixel the exclusive-OR is performed with a random key. For example, chaotic function-based image encryption methods. This domain-based image encryption is faster, less complex, and easier to understand than the other domain based image encryption methods. Due to these advantages, in this work, the spatial domain is chosen for image encryption.
- **Transform Domain:** In the transform domain, the secret image pixels are transformed from the spatial domain into the frequency domain. To achieve this goal, any of the frequency technique is used. After performing the encryption in the transform domain,

it is inverse transform to get the encrypted image. This domain-based image encryption method is complex, requires understanding of frequency techniques, and requires more computation time for image encryption over the spatial domain.

- **Optical:** In the optimal domain, the secret image is transformed into stationary white noise. To achieve this goal, a double random-phase encoding (DRPE) approach is used. Specifically, it uses a pair of random phase masks, one in the input plane and the other in the Fourier plane. In DRPE, these randomized phase masks serve as the "key." This domain-based image encryption method is faster due to good computation speed and parallel processing.
- **Compressive Sensing:** In the compressive sensing domain, secret images are compressed as well as encrypted. The compression is achieved using any compression method before encryption. The most popular image compression methods are lossless predictive coding and DRACO [19]. This domain method takes longer to compute because data compression and encryption need to be performed. Besides that, more information is communicated when compared to other domain-based image encryption methods.

1.3 Image Steganography

The word "steganography" has been derived from two words, "stegano" and "graphia," whose meaning is "cover writing." In this method, the secret information is written in some form of cover media, so it gives no attention to the attacker [2]. Steganography has been used since ancient times for secure communication, as explained below.

- In the fifth century, Histaiacus used this method to send a secret message by designing a message on the skull of his slave, and the slave moved that message with growing hair.
- Nearly, 50 decades ago, an Italian mathematician, Jerome Carden rescued a method of secret message writing that had been adopted by the Chinese in ancient times. In this method, a sheet of paper was used as a mask by making grid holes in it and writing a hidden message by placing it on a blank sheet of paper. This mask was then shared between the sender and the receiver. Once the grid mask is placed, the unwritten blank paper is filled, which turns out to be harmless text.

- During the First World War, the Germans used unused magazine material to create multiple stages of microdot technology. Various techniques were used to write a secret message, including “open coded messages”, “the Enigma machine”, “different null ciphers”, and using invisible ink during the Second World War.
- In Saudi Arabia, a king started a project at Abdulaziz City of Science and Technology, the information for secret writing and a detailed description of their project were found in a twelve-hundred-year-old manuscript.

Further, in the last 20 years, steganography has been transformed into digital processing-based steganography methods due to advancements in the technology of wireless communication, digital cameras, data digitalization, and the internet. In the current scenario, secret data in any form, namely, text, audio, video, and images, is hidden in the cover media. Furthermore, digital steganography methods cover a variety of media types, including text, audio, images, and video.

1.3.1 Data Embedding and Extraction Procedure of Steganography

The block diagram of the data embedding and extraction for steganography is shown in Figure 1.3. Initially, cover media, secret data, and a key are read and given to the data embedding algorithm. The key parameter is optimal in the steganography.

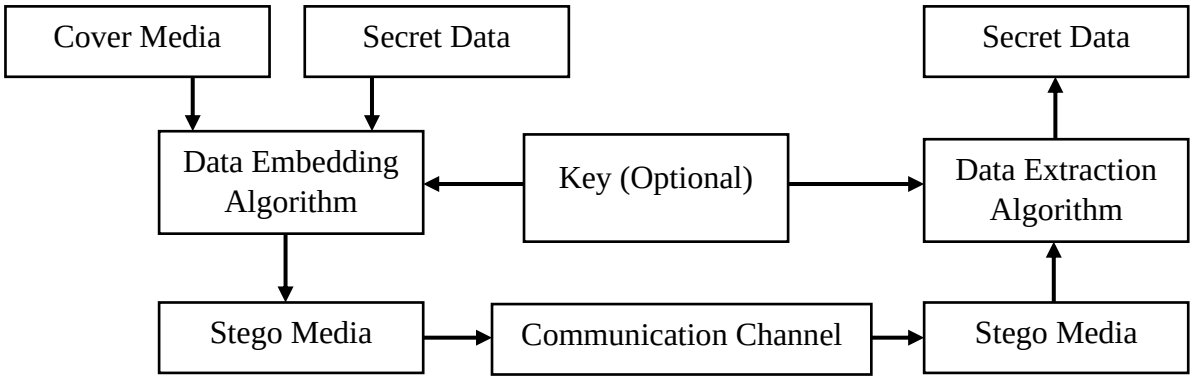


Figure 1.3: Block Diagram of Steganography (Adapted from [20])

Internally, the data embedding algorithm performs three operations. In the first operation, processing is done on the least significant bit (LSB) of the cover media and logical operations are performed on it to make it suitable for data substitution. The second operation involves the splitting of secret data into 1-bit chunks. In the third operation, the secret data bits are substituted in the LSB bit of the cover media. The data embedding algorithm outputs stego

media, which is communicated to the receiver for data extraction. On the receiver side, the stego media and key are read and given to the data extraction algorithm. This algorithm processes the LSB bits of the STEGO medium and extracts the least significant bit of it. The extracted LSB bits are processed to reconstruct the secret data on the receiver side.

1.3.2 Properties of Steganography

Steganography methods provide confidentiality for the secret data. Therefore, the properties that are taken into consideration when designing steganography methods are explained in this section. These properties are imperceptibility, payload capacity, and robustness (as shown in Figure 1.4), and their explanation follows [21].

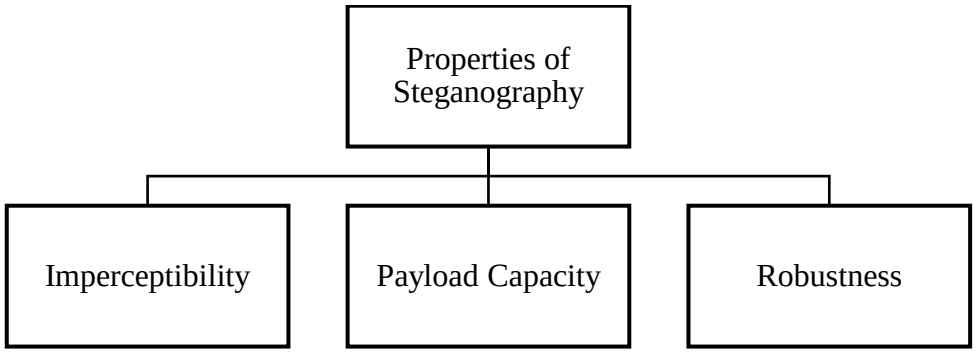


Figure 1.4: Properties of Steganography (Adapted from [21])

- **Imperceptibility:** The imperceptibility parameter defines how much distortion is generated in the cover media due to the data hiding process. In the ideal case, minimum distortion is required so it gives no attention to the attacker. Thus, imperceptibility is the most important security parameter of steganography. In the literature, several authors work to enhance this parameter by applying various operations to the secret data or cover image.
- **Payload Capacity:** This parameter defines how much information is hidden in the cover media. The payload capacity depends on the size of the cover media and how many bits are hidden per cover media pixel. In the literature, some of the researchers, pre-process the secret data using data compression methods such as Huffman coding, arithmetic coding to enhance the payload capacity. On the other hand, some of the researchers are hiding more bits per pixel of the cover media to enhance payload capacity, but this negatively impacts the imperceptibility parameter because hiding more bits per pixel generates extreme distortion in the cover media. Thus, there is an inverse relationship between payload capacity and imperceptibility.

- **Robustness:** The robustness parameter defines how much the steganography method is robust to attacks on the communication channel. The most popular statistical attacks on the stego medium are noise addition, rotation, zooming, and scaling. In order to overcome these attacks, the researchers in the literature, pre-process the secret image and add the error correction code to it, such as the Hamming code. On the other hand, the addition of error correction code in the secret data, negatively impacts the payload capacity parameter.

In this work, we have enhanced the imperceptibility parameter without impacting the embedding capacity parameter.

1.3.3 Classification of Steganography

The steganography methods are classified into three types, namely, based on the cover media, hiding domain and based on retrieval process, as shown in Figure 1.5 [2]. The detailed explanation of these types is given below.

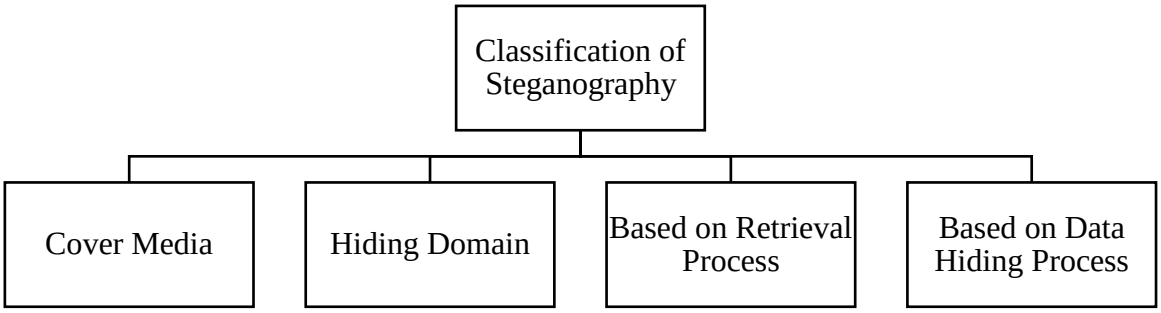


Figure 1.5: Classification of Steganography (Adapted from [2])

- **Cover Media:** The cover media is important in steganography because the secret data is substituted in it in such a way that the attacker cannot detect it. In the literature, four types of cover media are available: text, image, video, and audio. In text steganography, text data is used as a cover medium to hide the secret data. Further, in image and video steganography, image pixels and video frame pixels are taken as cover media to hide the secret data, respectively. Finally, in audio steganography, audio samples are used as a cover media to conceal the secret data. Out of these media, image steganography is most popular because it provides better payload capacity due to the large number of pixels in it. Further, the variability is generated in the cover image due to the data embedding process, and it does not draw attention to the attacker because it is recognizable in the cover image. In video steganography, one frame is equivalent to

one image. Therefore, the same embedding and extraction process of image steganography is applicable to video steganography. In this research work, we have chosen images as the cover medium to hide the secret images.

- **Hiding Domain:** The image steganography is classified into two types based on the hiding domain. These are spatial domains and transform domains. In the spatial domain, the cover image pixels are directly manipulated for data hiding, whereas in the transform domain, the image pixels are transformed into the frequency domain using frequency techniques. Some of the most popular frequency domain techniques in the literature are discrete Fourier, cosine, and wavelet transforms and their various types, such as integer based, complex wavelet, and dual-tree complex wavelet transforms. After that, data hiding is performed on the transformed pixels, and an inversed transform is conducted using the frequency method before communicating the stego image. Further, when comparison is based on the embedding capacity, the spatial domain is superior to the transform domain because all pixels can be manipulated for data hiding, whereas in the transform domain, either low, high, or dc coefficients are used for data hiding purposes. Next, the spatial domain provides less complexity than the transform domain because no conversion needs to be performed on the cover image. Due to these advantages of the spatial domain, in our work, the spatial domain is used for hiding the secret images. In the literature, several spatial domain-based data hiding methods are available for data hiding, such as least significant bit (LSB), histogram shifting (HS), pattern based, pixel value difference (PVD), multiple bit plane, and palette based. Out of these data hiding methods, the LSB method is most preferred in the spatial domain due to its simple structure and process of data hiding.
- **Retrieval Process:** The retrieval process of the steganography method defines whether the cover image and secret data are retrieved on the receiver's side or not. It is divided into reversible and irreversible steganography methods based on the retrieval process. The reversible steganography method retrieves both information (the cover image and secret data). This category includes the histogram shifting method. On the other hand, in the irreversible steganography method, only secret data is retrieved on the receiver side because, in this method, the cover image LSB bits are manipulated due to the data hiding process. The LSB method falls under this category.
- **Data Hiding Process:** In the data hiding process, either data is hidden in the entire cover medium in a consecutive manner or a region of interest (ROI) is found to be hiding the secret data. In the literature, pre-processing on the cover media is done before

the data hiding process. Some researchers, for example, identified the region of interest in the cover image and then performed data hiding on it. Further, some researchers split the cover image into a smooth region and an edge region, hiding less information in the smooth region because of high redundancy between pixels, whereas hiding more information in the edge region because low redundancy exists between pixels. Next, some scholars worked on cover images, in which RGB planes are available and plane selection is done based on the human visual system's (HVS) characteristics for data hiding. In the HVS characteristic, the researchers define that eyes are more sensitive to green color than blue. Therefore, blue is chosen for data hiding. In our work, data hiding is done in a consecutive manner. Furthermore, the challenges of HVS characteristics in steganography are considered when selecting the optimal plane. The challenges of HVS characteristics-based plane selection are that it is a fixed data hiding plane, and if the blue plane is the more dominant plane in the steganography, then it negatively impacts the imperceptibility parameter.

1.3.4 Image Security Methods based on Steganography

In this section, we have studied and analysed the image security methods based on steganography.

- Least Significant Bit (LSB) Method: The basic structure of the least significant bit (LSB) method is shown in Figure 1.6. Initially, a secret image is read. The secret image is split into 1-bit chunks [11]. After that, the cover image and 1-bit chunks of data about the secret image are given to the data embedding method. The data embedding method performs two operations. In the first operation, the least significant bit of the cover image pixel makes it "0." After that, in the second operation, the 1-bit chunks of information of the secret image in the cover image are substituted, resulting in a stego image in the output.

  Further, numerous researchers have designed *k*-bit LSB methods. The block diagram of the *k*-bit LSB method is shown in Figure 1.7. In these methods, secret image bits are split into *k*-bit chunks. After that, the *k*-least significant bit of the cover image is concealed with secret image bit chunks. Figure 1.8 shows the stego images obtained from k-bit LSB methods. There is a clear degradation in stego image quality when the number of bits per pixel is raised, as seen by the stego images.

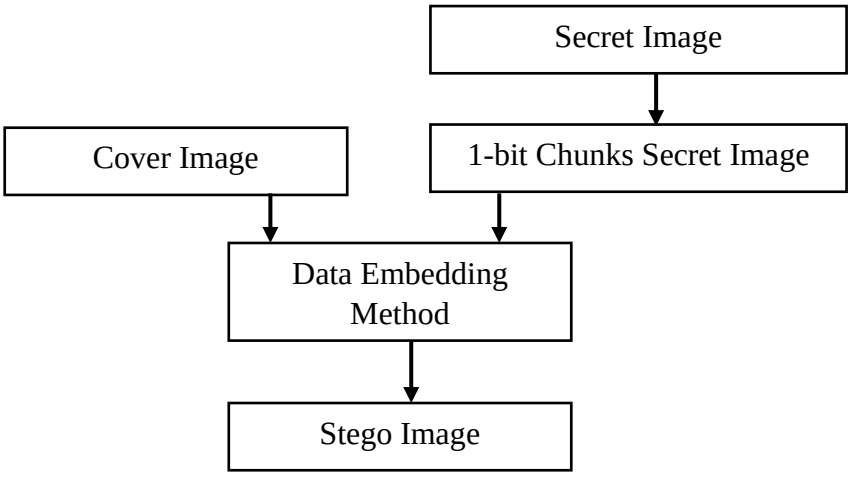


Figure 1.6: Block Diagram of the LSB Method

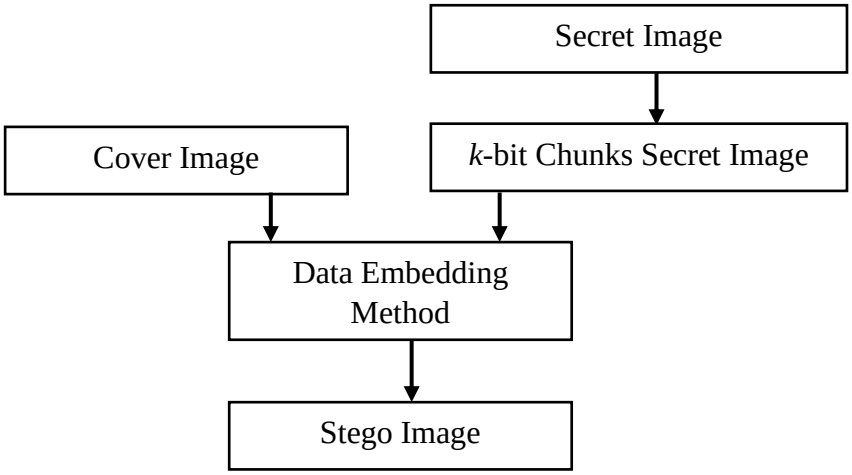


Figure 1.7: Block Diagram of the *k*-bits LSB Method

Figure 1.8: Stego Images for *k*-bit LSB Methods [22]

The mathematical model for LSB method for data embedding and extraction is given below.

$$S' = C - C \; mod \; 2^n + d \tag{1.1}$$

$$d = S' mod \; 2^n \tag{1.2}$$

In Eq. (1.1), C, S' denotes the cover and stego image pixel value whereas n specifies the number of bits replacement in the cover image pixel. Further, d denotes the secret message.

In the proposed steganography methods, LSB method is taken under consideration to hide the optimal secret data in the cover image to enhance the imperceptibility parameter.

1.4 Hybridization of Cryptography and Steganography Methods

The hybridization of cryptography and steganography methods is done to add a number of layers to the secret data, known as a "multi-layer security system [23]." In this method, one layer of security is added to the secret data by performing the encryption process. After that, a second layer of security is added by hiding it in the cover media. The block diagram for it is shown in Figure 1.9. Initially, the secret data is encrypted using a secret key in the encryption method. Following that, encrypted data and cover media are fed into the data embedding method, which returns stego media in the output after data hiding. On the receiver side, the data extraction method gives the encrypted data after extracting the data bits from the stego media. Furthermore, the encrypted data along with the key is forwarded to the decryption method. The decryption method performs the inverse functions that are performed in the encryption method and gives the original secret data at the output. In the literature, the encryption method uses advanced encryption standard (AES), IDEA, chaotic mapping, and exclusive-or operations, whereas the LSB method is used for data hiding [23-27].

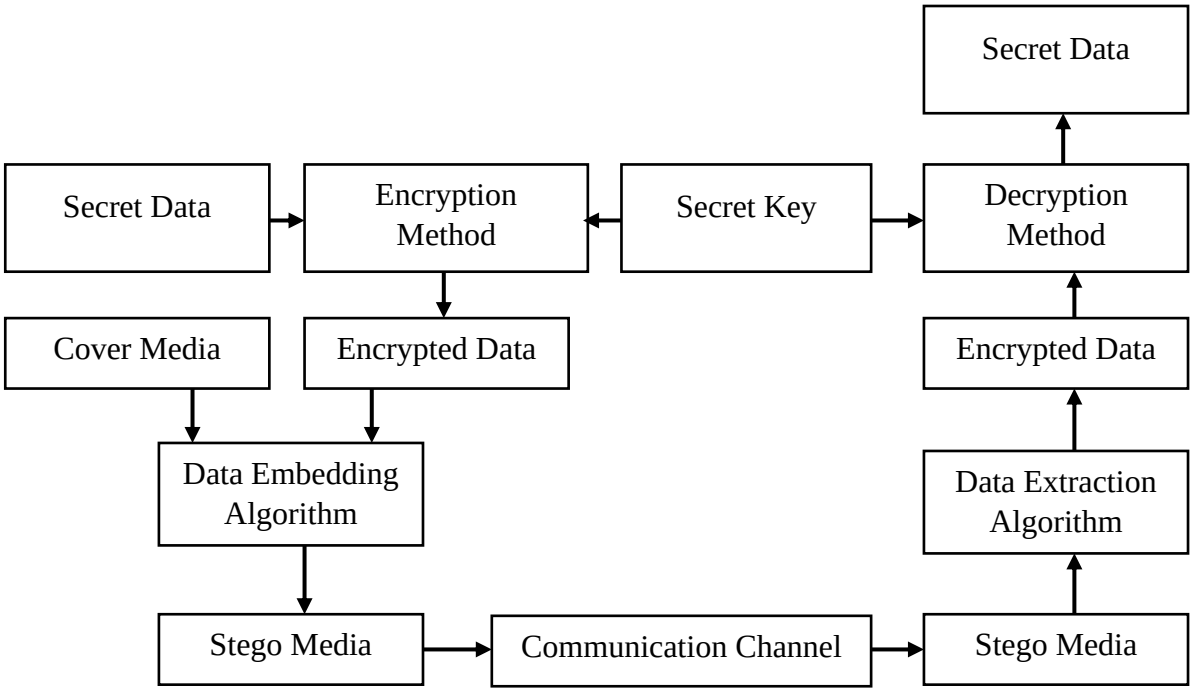


Figure 1.9: Block Diagram of the Hybridization of Cryptography and Steganography (Adapted from [2])

However, the hybridization of cryptography and steganography methods increases the overall execution time because the entire secret data is encrypted and then hidden in the cover media. Besides that, all parties need to have access to the secret key to retrieve the secret data. Instead of encrypting the entire secret data, we only encrypt the sensitive parts of the secret data, which reduces the overall execution time. Further, only the required parties need to have access to the secret key instead of all parties, which enhances the security of the proposed method.

1.5 Bio-Inspired Optimization

Optimization algorithms have gained popularity in different engineering disciplines to solve various mathematical problems. The main motive of the optimization algorithms is to find the optimal or near-optimal solution to the chosen problem [28]. Further, optimization algorithms are classified into types, namely, "deterministic" and "stochastic." In deterministic algorithms, the algorithm gives the same output, whereas in stochastic algorithms, there is ambiguity related to the output according to the input constraint [29]. The traditional optimization algorithms that are preferred in the earlier stages to solve mathematical problems require massive computation efforts, are not applicable to all problems, and fail to find an optimal solution when the problem is complex. These limitations give us the motivation to explore bio-inspired optimization algorithms, which require less computation effort and cover a broader range of complex problems than traditional optimization algorithms. It is an iterative process that searches for the optimal or near optimal solution according to the given problem. The optimization of the solution is done based on the objective function. Thus, according to the given problem, the objective function is either maximized or minimized.

Next, we have explained the workings of the bio-inspired optimization algorithm to understand how it works. The flowchart of the bio-inspired optimization algorithm is shown in Figure 1.10.

As we know, the main motive of the bio-inspired algorithm is to provide an optimal or near optimal solution. As a result, the initial population is initialized randomly in the lower and upper limits based on the required solution because the solution space contains hundreds of solutions and searching each solution in consecutive ways requires significant computation effort. Further, the dimension of each population depends on the problem. In the next step, the fitness evaluation is performed for each population based on the objective function. As a result, the objective function is important in the bio-inspired algorithm, and its proper selection improves the optimal solution to the given problem. In most of the problem constraints, its

value is either maximized or minimized. Based on the fitness evaluation, the best population is determined, which gives the superior solution over the other populations. The bio-inspired algorithm is then iteratively executed until either the required solution is not achieved or a fixed number of iterations is reached. In this iterative process, the bio-inspired optimization algorithm operations are performed on the initial population to generate a new population in order to explore solution space.

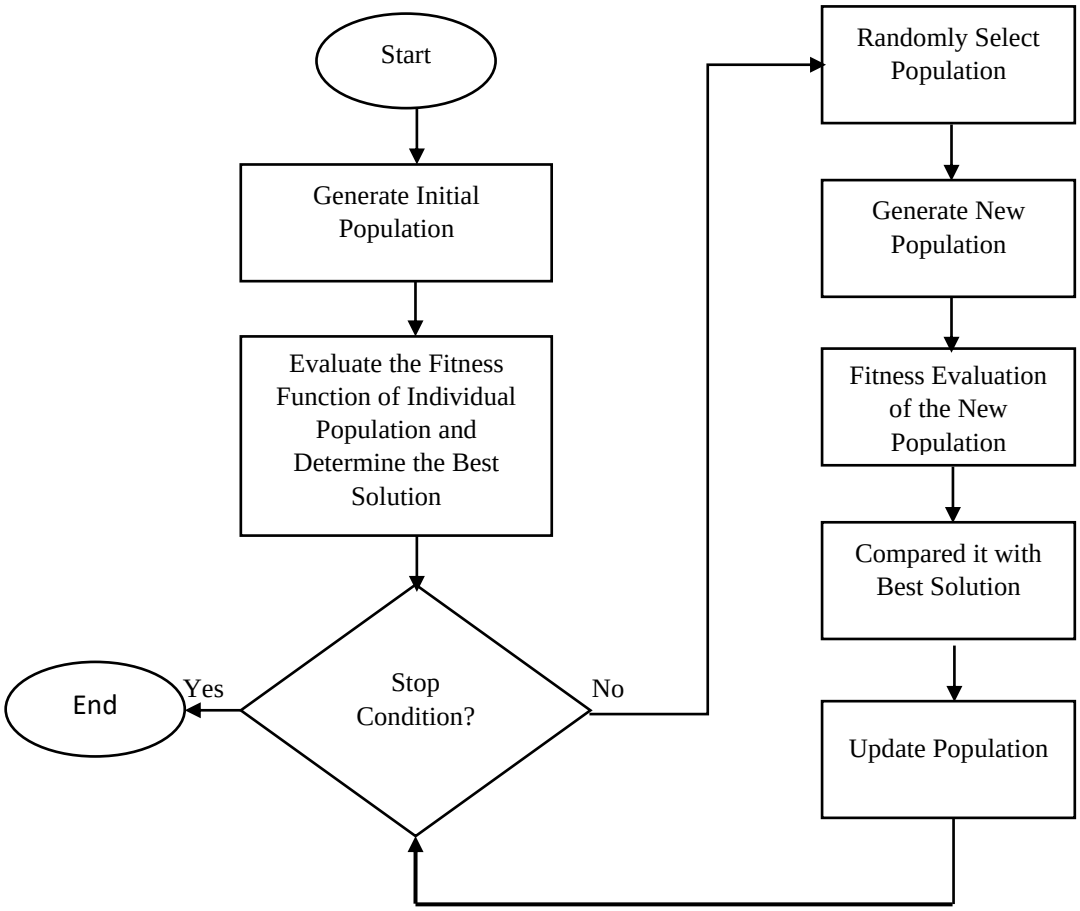


Figure 1.10: Flowchart of the Bio-Inspired Optimization Algorithm (Adapted from [30])

For example, the GA algorithm performs "crossover" and "mutation" on the initial population, whereas the EVO algorithm performs "hit with a pebble," "rolling with twigs," and "change of angle" on the initial population to generate a new population. The new population is evaluated in the same way as the initial population. Thus, the new population chooses the superior solution over the best solution in the earlier phase, and the best solution is then updated.

Further, bio-inspired algorithms are classified into four types namely, swarm intelligence, evolutionary, physical based, and chemical based, as shown in Figure 1.11.

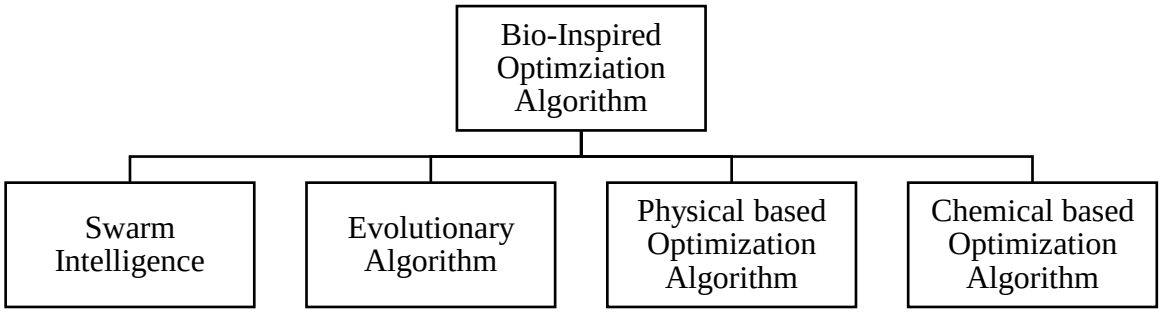


Figure 1.11: Classification of Bio-Inspired Optimization Algorithm (Adapted from [31])

The swarm intelligence algorithms are based on the food searching behavior of the living organisms. The well-known swarm intelligence algorithms are "particle swarm optimization" (PSO), "ant colony optimization" (ACO), "cat swarm optimization" (CSO), "Egyptian vulture optimization" (EVO), and "green heron optimization" (GHO). On the other hand, the evolutionary algorithm is based on the mating process of living organisms. The most popular evolutionary algorithms are the genetic algorithm (GA), black widow optimization (BWO), and bumble bee mating optimization (BBMO). Next, physical and chemical optimization algorithms are based on the physical and chemical properties [32]. Gravitational search algorithms, big bang big crunch optimization, and chemical reaction optimization are some of the most popular optimization algorithms. The most efficient algorithms based on these optimizations are swarm intelligence and evolutionary algorithms. Therefore, in our research, these algorithms are taken into consideration.

1.5.1 Objective Function

Objective function plays a vital role in the BIO algorithm. According to the problem, the objective function is either maximized or minimized [33]. For example, in cryptography, the objective function such as entropy is maximized for best encryption; whereas in steganography, the objective function such as mean square error is minimized for enhancing the imperceptibility parameter. Further, single- or multi-objective function concepts are given by researchers. In the single objective function, single characteristics of the given problem are boosted, whereas in the multi-objective function, multiple characteristics of the given problem are enhanced. In the last step, the optimal selection of the objective function reduces the algorithm complexity based on the population and the number of iterations (number of times the objective function is evaluated in the bio-inspired optimization algorithm).

1.5.2 Selection Criteria for Bio-Inspired Optimization Algorithm

A huge number of BIO algorithms are available in the literature, and a good number of them are deployed frequently for cryptography and steganography applications. Thus, selecting the most optimal bio-inspired algorithm for these algorithms is a challenging task. Therefore, this section explains how these optimization algorithms are differentiated from each other and selected for the search of the optimal solution in these applications.

- **Exploration and Exploitation Rate:** The main components of the bio-inspired algorithms are exploration and exploitation rate, or intensification and diversification. Generating a large number of potentially appropriate answers is the meaning when talking about "diversification," with the ultimate goal of broadening our search. Intensification is the process of narrowing a search to a smaller geographical area, taking advantage of the knowledge that a good solution is already located there. In conjunction with picking the top options, this is what happens. The diversity of the solutions is increased through randomness, and the selection of the best alternatives guarantees that they might converge on optimality. In most cases, success in achieving global optimality can be guaranteed through careful coordination of these two primary factors. In our work, these components are taken into consideration while choosing the bio-inspired algorithm for designing encryption and steganography methods [34].
- **Convergence Rate:** The convergence rate defines the count of iterations; a bio-inspired algorithm is used to find the solution [35]. The convergence rate is a graph plotted between iterations and the fitness function. It depends on the exploration and exploitation rates of the algorithm.
- **Total Number of Input Parameters:** This parameter defines the total number of input parameters required for the bio-inspired optimization algorithm to determine the optimal solution.

1.6 Dissertation Outline

The main aim of this dissertation is to enhance the security of the image steganography and encryption methods using the bio-inspired algorithms. In this section, the organization of the dissertation is explained. The dissertation is organized into seven chapters.

Chapter 1 provides a background and motivation for this research work. Following that, a detailed description of cryptography is provided, which includes an examination of image

encryption and decryption method and its domains. Further, spatial domain methods are studied in detail because they are taken into consideration in this research. Next, a detailed description of steganography is given, in which, data embedding and extraction procedure, its various properties, classification, and the most popular data hiding methods are studied. Following, the hybridization of cryptography and steganography, bio-inspired algorithms, and their types are studied. In this study, swarm intelligence and bio-inspired evolutionary algorithms are considered. As a result, a thorough investigation was conducted. Based on the study, important terms like "objective function" and how bio-inspired algorithms are selected. Finally, outline of the dissertation outline is discussed in this chapter.

Chapter 2 presents the review of the literature. In this chapter, initially, a literature review is conducted for image encryption, image steganography, and hybrid approaches based on it. After that, based on the literature survey, research gaps and objectives for the thesis work are defined. Further, datasets, evaluation platforms, and performance metrics for encryption and steganography are defined to understand the research methodology. Next, in this chapter, a detailed description of the swarm intelligence algorithms, namely, Egyptian Vulture Optimization (EVO), Green Heron Optimization (GHO), and evolutionary algorithm black widow optimization are taken into consideration in our work for optimizing data hiding and encryption is explained. In the last section, the research contributions are defined.

Chapter 3 presents the proposed optimized image steganography methods that are developed using the swarm intelligence algorithms in order to enhance the imperceptibility parameter. In this work, EVO and GHO algorithms are taken into consideration due to better exploration of solution space over other swarm intelligence algorithms. We, next, explain the proposed approaches for the image steganography method. In the first approach, the swarm intelligence algorithms search the best cover image, optimal block order, and optimal secret data index before data hiding to enhance the imperceptibility, whereas in the second approach, a matching method is proposed in which swarm intelligence operations and their optimization are used for hiding the data in an optimal way. The result analysis is performed based on the subjective and objective analyses and are compared with the existing methods based on them.

In **Chapter 4,** we have developed an optimized image steganography method by considering the evolutionary (Black Widow Optimization) algorithm. Initially, in this chapter, the reasons for choosing an evolutionary algorithm such as Black Widow Optimization (BWO) in our work, is explained over existing evolutionary algorithms. Next, the proposed image

steganography method based on is explained, including how the BWO algorithm searches for the optimal secret data and cover image index in order to enhance the imperceptibility parameter. Following that, subjective and objective analysis is performed on the standard dataset in the result and analysis section to validate its performance over the existing method.

In **Chapter 5**, we have presented two key generation methods based on evolutionary BWO algorithm for image encryption. Initially, we start with the explanation how bio-inspired algorithms are used for key generation for image encryption. After that, two approaches are explained for the proposed image encryption method. In the first approach, how the evolutionary BWO algorithm is used for random key generation and its operation deployed for image encryption is explained, whereas in the second approach, random key generation is done using the chaotic logistic map algorithm and its performance is enhanced by determining the best initial parameter value using the evolutionary BWO algorithm. After that, its deployment for image encryption is explained. Furthermore, the proposed methods' results are analyzed in terms of simulation setup configurations of the BWO algorithm, followed by subjective and objective analysis. The final section includes a comparative analysis.

In Chapter 6, a privacy-preserving method is proposed by combining the image encryption and steganography algorithms and optimizing their performance using the evolutionary BWO algorithm. Initially, in this chapter, the need for a privacy-preserving method and the challenges of the existing methods are defined. After that, how the optimal cover image plane is chosen for data hiding by pre-processing the cover image is explained. Next, the proposed privacy-preserving method is explained, in which encryption is performed on the sensitive data and optimized data hiding is done in the cover image plane using the BWO algorithm. The simulation evaluation is also explained in detail, including the simulation setup configuration of the BWO algorithm and a subjective and objective analysis of the proposed method. In the last section, the comparative analysis is done with the existing methods based on the various performance metrics.

In **Chapter 7**, conclusions are drawn. Initially, in this chapter, key contributions and findings are explained. After that, limitations and future scope of the work are discussed.

Chapter 2

Literature Survey

2.1 Introduction

The main theme of the research work in this thesis is to study and explore bio-inspired optimization (BIO) algorithms and employ them to optimize the performance of image encryption and steganography methods for secure communication of digital images on the internet. In this chapter, a survey of related literature is provided on image cryptography and steganography methods, followed by hybrid approaches. Based on this survey, the research gaps and objectives have been elaborated in this chapter. The standard image dataset employed for evaluation of the performance matrices for the proposed methods, along with the software tools and platforms, are also discussed in this chapter. Next, an overview of the bio-inspired algorithms is given which are considered in this research. Finally, research contributions are defined.

2.2 Related Work on Image Encryption

In this section, some important related work is provided for image encryption methods to understand how bio-inspired optimization algorithms are deployed for image security. The main motive of the image encryption methods is to secure the digital images on the internet by encrypting them [36]. In encryption, the encryption method and random key play an important role. In the literature, numerous encryption methods such as chaotic function, Advanced Encryption Standard (AES) [37], DNA [38], elliptic curve cryptography (ECC) [39], and bio-inspired based methods are used for image encryption. In recent years, bio-inspired based methods have gained in popularity over other encryption methods because they encrypt the secret images by analyzing their characteristics. Therefore, we have studied and analyzed the bio-inspired-based image encryption methods proposed by various researchers.

In [40], the authors generated *n* number of encrypted images using the original image and chaotic function. After that, encrypted images used a population in the genetic algorithm to determine the best encrypted image that provided high entropy and a low correlation coefficient. In [41], the authors designed a two-stage step to maximize entropy and minimize the correlation coefficient using a dynamic harmony search algorithm. In [42], authors

optimized a chaos-based image encryption scheme using teaching-learning-based optimization (TLBO) and a gravitational search algorithm (GSA). The TLBO provides superior results over gravitational search algorithms. In [43], authors deployed the genetic algorithm for chaotic functions. Furthermore, single, and multi-objective functions are designed. The hybrid combination of entropy and correlation coefficient as an objective function provides superior results over other combinations of objective functions. In [44], authors have hybridized the linear feedback shift register (LFSR), chaotic functions such as tent and logistic map algorithms for key generation. After that, process the original image in fixed block size. Furthermore, perform XOR and genetic operations to get the encrypted image in the output. In [45], authors used the keccak, henon map, DNA encoding, and genetic operations to achieve image encryption. In [46], authors determined the optimal parameter values of a chaotic logistic map using the grasshopper optimization (GO) algorithm and used the entropy as an objective function.

On the other hand, the random key plays an important role in the image encryption method because, in most of the image encryption methods, an exclusive-or operation is performed between the image pixel and the random key [47]. In the literature, various conventional key generation methods such as RSA, elliptic curve cryptography (ECC), and linear and non-linear feedback shift registers are used for encryption purposes [7-10,48]. Out of these, RSA and ECC-based methods are used for key generation for software applications. These algorithms require modular, multiplication, and exponent functions [9,48]. As a result, key generation takes a long time. On the other hand, linear and non-linear feedback shift register methods are used for key generation for hardware applications [7-8]. These algorithms generate 1 bit per cycle and require a number of shift registers and logical operators. Besides that, in conventional key generation methods, the random key is fixed and easy to cryptanalyze if the input parameters are known by the attacker. To overcome these limitations, researchers have proposed bio-inspired-based key generation methods. These methods, instead of generating the random key, explore the optimal key from n numbers of keys based on key characteristics such as probability of 0s and 1s, transition between 0s and 1s, and other characteristics of the key. Following that, we investigated and analyzed the use of bio-inspired algorithms for key generation.

For key generation, in [49], authors used the particle swarm and ant colony optimization algorithms. Further, authors [50] took into consideration the different evolutionary algorithms such as genetic algorithms, differential evolution, improved modified harmony search, and

hybrid combinations of improved modified harmony search and differential evolution for key generation for stream ciphers. They have designed the bi-objective function to maximize the entropy parameter and the intersection between random keys and secret data.

2.3 Related Work on Image Steganography

The central idea of the image steganography method is to substitute the secret data in the cover image in such a way that minimum distortion is generated in the output image, known as a stego image [2]. A minimum distortion in the stego image gives the least imperceptibility to the attacker when data substitution is performed on it. In the conventional substitution method, in order to conceal secret information in the cover image, the LSB of the cover image pixel is replaced with a secret data bit. This method is known as the "least significant bit" (LSB) in steganography [11]. However, due to the substitution procedure, a distortion in the output image is generated when the cover image LSB bit is not matched with the secret data bit, which adversely impacts the imperceptibility parameter. Thus, determination of the optimal secret data or cover image before data substitution enhances the imperceptibility parameter [51-58]. To achieve this goal, rearrangement of the secret data or cover image is done, and determination of the optimal form is a very challenging task because a number of combinations are available. Further, exploring all the combinations is almost a difficult task. Hence, to overcome this issue, bio-inspired optimization algorithms are taken into consideration by various researchers in the literature. Next, we studied and analyzed how the bio-inspired optimization algorithms are used for image steganography.

In [51], authors used the genetic algorithm to search for the optimal pixel scanning order in the cover image and secret data form. In [52], authors determined the optimal secret data matrix by performing swapping, data direction, and data polarity. To achieve this goal, they have employed the genetic algorithm. Further, authors [53] have deployed the PSO algorithm to search the optimal pixels in the cover image for data embedding. However, the data embedding capacity is reduced because only a subset of the cover image can be hidden rather than the entire image. In [54], authors used cat swarm optimization to find the best substitution secret data matrix. This method outperforms the exhaustive LSB substitution method because it uses all substitution matrices to find the best stego image. As a result, the computation time is increased. In [55], authors searched for the optimal cover image scanning direction and optimal secret form. The scanning direction is divided into two states: horizontal and vertical, and the optimal secret data form is determined by flipping, transposing, and shifting operations. In

2018, authors [56] did the pre-processing on the cover image by splitting it into blocks. After that, determine the optimal block order using the artificial bee colony algorithm. Further, authors [57], say that if the restriction is done to the same cover image, then the best results are not always obtained. Therefore, they have designed a method that searches for the optimal cover image from a set of cover images using a genetic algorithm. Next, in [59], authors used the genetic algorithm to rearrange the secret data before data embedding in the cover image. However, the genetic algorithm has low convergence rate. Finally, in [60], authors designed n-bit optimized LSB data hiding method using the Harris Hawks optimization method to determine the encoded form of secret data based on the objective function. In their work, PSNR is taken as the objective function.

Further, some researchers designed a matching method for image steganography to enhance the imperceptibility parameter. In [58], authors designed a method that identifies the suitable location to hide the secret data in each pixel. The identification process generates the coefficient matrix corresponding to the location of the match. Furthermore, they have deployed the genetic algorithm to hide the coefficient matrix in the cover image in the optimal way. The hiding capacity is less because only one quarter of the cover image is used for identifying the suitable locations and the remaining matrix is used for hiding the coefficient matrix. In [61], authors designed a complemented or non-complemented method that matches the complemented or non-complemented form of secret data bits with the cover image LSB bits and determines the optimally matched form. The advantage of their method is that it provides better embedding capacity, but variability is generated in their method due to hiding the optimally matched form using the LSB method. In [62], authors designed an optimized data hiding method in which the cover image is split into smooth and edge regions. The smooth region LSB bits are matched with secret data bits, whereas edge region pixels are used to hide the matched index. The embedding capacity is not fixed, and data extraction is feasible only if the same number of edges are recovered while hiding the data.

2.4 Related Work on Hybrid the Cryptography and Steganography Methods

The hybridization of cryptography and steganography methods is done to achieve multi-layer security on the secret image. In these methods, the secret image is encrypted using image encryption methods [63]. After that, the encrypted image is hidden in the cover image using steganography methods. In this section, we have studied and analyzed the various methods proposed by the hybridization of cryptography and steganography.

In [64], the authors safeguard the users' private and sensitive data on the IoT network using the chaotic function. After that, utilized the steganography method to hide the information. In [65], authors employed the RSA and neural network-based steganography approach to safeguard the personal and confidential information in the medical photographs. The authors of [66] created an approach to protecting user privacy by combining the Advanced Encryption Standard (AES) and the LSB algorithm. In [67], the authors, hybrid the AES, ECC and LSB algorithm in which data encryption is done using AES algorithm, secure the private key of AES algorithm using ECC, then hiding the encrypted key using LSB algorithm. The hybridization is done with the conventional encryption method which takes longer computation time (for example in RSA, exponent, modular needs to perform for data encryption) for data encryption and consumes more resources (for example look-up tables are required in AES for substitution and mix column layer). Besides that, entire information is encrypted then hidden in the cover media using data hiding method which takes long execution time.

2.5 Research Gaps

In this section, the research gaps are defined based on the literature survey.

- In image steganography, either optimal secret data or a cover image is determined using the bio-inspired optimization algorithm before data substitution [52-58]. The most popular bio-inspired optimization algorithm is the genetic algorithm. The genetic algorithm selects the population randomly to generate the offspring. The population is randomly selected, and if the selected population is of inferior quality, then the superior offspring will not be generated from it [68]. Thus, the exploration rate of genetic algorithms is slower, and they provide a low rate of convergence.

- In the matching method of image steganography, the secret data bits are matched with the cover image pixels and optimal matching indexes are determined [58,61-62]. After that these indexes are hidden in the same cover image. Therefore, the embedding capacity is lower and it takes a longer execution time for data substitution if the data substitution is done for high resolution images.
- The pre-processing of the cover image is done to select the most optimal plane for data hiding. The optimal plane for data hiding is chosen in the literature based on the characteristics of the human visual system (HVS) [62]. Green is more sensitive to the human eye than blue, according to the HVS characteristic. Therefore, the blue plane is

chosen for data hiding. For these reasons, the data hiding plane is fixed, and its impact on the security parameter is negative. Furthermore, if the blue color is the most dominant color in the cover image, it will have a highly negative impact due to data concealment.

- Random keys play an important role in cryptography and steganography algorithms. Encryption and key generation methods are designed using bio-inspired algorithms while considering the characteristics of the input image and random key. In the literature on it, the conventional key generation methods are deployed for it. It takes a long execution time, generates a fixed key generation pattern, and is based on complex mathematical models [7-10, 48].
- In cryptography, chaotic functions are preferred over conventional cryptography algorithms because they are extremely sensitive to initial conditions and provide non-linearity, unpredictability, and ergodicity [69]. The inappropriate selection of initial condition parameters negatively impacts the security parameter. Therefore, bio-inspired optimization techniques such as the genetic algorithm, dynamic harmony search, teaching learning-based optimization (TLBO), gravitational search algorithm (GSA), and grasshopper optimization algorithms are deployed to determine the optimal parameter values based on the objective function [42-43, 46]. These algorithms provide a low convergence rate and require parameter tuning.
- Cryptography and steganography algorithms are hybridized to design multi-layer security systems [63]. In this system, the secret data is encrypted and then hidden in the cover image using the steganography algorithm. The hybridization methods take a longer execution time because the entire secret image is encrypted using cryptography.

2.6 Objectives

In this section, the research objectives are defined that are based on the literature survey and research gaps.

1. *To study and explore bio-inspired Cipher and Steganography Algorithms*

   The focus of the study is to first explore the limitations of traditional image cipher and steganography algorithms. Next, the suitability of bio-inspired algorithms are studied for deployment in cipher and steganography algorithms. The swarm intelligence and evolutionary algorithm based cipher and steganographic algorithms are studied in detail along with their challenges

2. *To propose bio-inspired cryptographic and steganographic algorithms for optimizing performance and high security*

Two swarm intelligence algorithms, namely, Egyptian vulture optimization and green heron optimization, and one evolutionary algorithm, namely, the black widow optimization algorithm, are employed for proposition of the image steganographic methods. These algorithms are utilized to search for the optimal form of secret data by performing various operations and determining the optimal scanning order in the cover image for optimized data hiding. These algorithms perform three operations in each iteration to explore the solution space and to search for the optimal solution.

3. Generation of reliable random key using bio-inspired algorithms

The objective is to propose the cryptographic key generation method based on bio-inspired black widow optimization algorithm. Firstly, a completely random key is generated using the BWO algorithm based by the minimization of the objective function. In the second approach, the optimal parameter values of the chaotic logistic map algorithm are determined using same algorithm. The random key is generated using it subsequently.

4. *To demonstrate the proposed algorithms in related applications.*

Here, the main objective is to design a privacy-preserving method using the hybridization of cryptography and steganography methods. In the proposed multi-layer security system secret data is encrypted and then hidden in the cover image using the steganography algorithm.

2.7 Dataset, Evaluation Platform and Performance Evaluation Parameters

2.7.1 Standard Dataset

Digital images are stored in the USC-SIPI picture database [70]. It is kept up mainly to help researchers in the fields of imaging science and computer vision. In 1977, the first USC-SIPI image database was made available to the public; since then, thousands more photographs have been uploaded. The database is broken up into collections called "volumes" that are based on the common themes seen in the images. Depending on the volume, images with resolutions of 256x256 pixels, 512x512 pixels, or 1024x1024 pixels can be found. Both the grayscale and color images are 8 bits/pixel in depth. Current database access includes the volumes, namely,

texture, aerials, miscellaneous, and sequences. Out of these, miscellaneous volume is maximally used in image encryption and steganography.

2.7.2 Software Tools and Platforms

The MATLAB program is used for the simulated examination of cryptography and steganography algorithms. Matrix Laboratory, or MATLAB for short, is a popular high-level language and interactive environment for doing numerical computation, visualising data, and writing computer programs. MathWorks creates MATLAB [71]. It's possible to work with matrices, plot data and functions graphically, construct methods, design user interfaces, communicate with other programs written in languages like C, C++, Java, and FORTRAN, and much more. Various mathematical instructions and functions are pre-installed to facilitate numerical procedures, plot generation, and other mathematical operations.

2.7.3 Performance Analysis Parameters

Performance analysis parameters are determined to evaluate the performance of the image encryption and steganography methods. These methods are analysed using subjective and objective analysis [2,44, 72], as explained below.

- **Subjective Analysis:** In the subjective analysis, the input and output images of image encryption and steganography methods are compared based on the visual parameter. In the image encryption, the output image should be completely noisy as required, whereas in steganography, the output image should be similar to the input image.

- **Objective Analysis:** In the objective analysis, various performance metrics are determined for image encryption and steganography methods. Some performance metrics are common to both methods (such as mean square error (MSE)), peak signal to noise ratio (PSNR), entropy, and correlation coefficient (CC)), whereas others are determined for encryption (such as NPCR, maximum deviation, and chi-square test) or steganography methods (payload capacity). The detailed description of these performance metrics is given below.
  1. **Peak Signal to Noise Ratio (PSNR):** The Peak Signal to Noise Ratio (PSNR) is the most preferred parameter to verify visual analysis. It is calculated using Eq. (2.1). It is measured in *dB*. A low value of PSNR represents the strong encryption whereas high value represents better image steganography method.

$$PSNR = \log_{10} \frac{P^2}{MSE} \quad (2.1)$$

In Eq. (2.1), P denotes the value of maximum possible intensity of a pixel in the original image (secret image in the image encryption/cover image in the steganography). MSE represents the mean square error between original and output image (encrypted image in the encryption/stego image in the steganography) and it is calculated using Eq. (2.2).

$$MSE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (O_{ij} - OI_{ij})^2}{M \times N} \quad (2.2)$$

Here, O, OI denote the original and output image whereas M, N denote the row and column of the image.

2. **Entropy:** This parameter defines the degree of uncertainties in the system. In the image encryption process, a higher value of entropy represents the high randomness in the encrypted image and is less prone to statistical attacks. On the other hand, in steganography, the similar entropy to the cover image is required. It is calculated using Eq. (2.3) as

$$E(c) = \sum_{m=1}^{2^N - 1} p(c_m) \times \log_2 \left[\frac{1}{p(c_m)} \right] \quad (2.3)$$

Here, p denotes the probability of histogram value, c denotes the histogram for the encrypted image/stego image, m represents the histogram value which varies between 0 and 255. The entropy value for an encrypted image is near to 8 value in an ideal case.

3. **Correlation Coefficient:** Correlation coefficient is computed using Eq. (2.4) as follows:

$$CC = \frac{\sum_i \sum_j (O_{ij} - O_{mean})(OI_{ij} - OI_{mean})}{\sqrt{(O_{ij} - O_{mean})^2 (OI_{ij} - OI_{mean})^2}} \quad (2.4)$$

where O, OI denote the original as well as output images. P_{mean}, E_{mean} denote the mean values for the original and output images respectively. Lastly, i, j denote the subscripted variables. The correlation coefficient value varies from -1 to 1. The 1 value represents the strong correlation between original and output image. In the cryptography, ideal value of 0 is required which represents the low correlation between original and encrypted image. On the other hand, in the steganography, high value of correlation

coefficient required which denotes the strong correlation between cover and stego image.

4. **Number of Pixel Change Rate (NPCR):** Cryptanalysts sometimes alter the original image/key slightly to test how the alteration impacts the encrypted image [44]. A robust encryption system that is resistant to differential attacks should be extremely sensitive to even minor changes in the original image/key. This sensitivity is analysed in cryptography using number of pixels change (NPCR) parameter. NPCR is computed using Eqn. (2.5).

$$NPCR = \frac{\sum_{m,n} D(m,n)}{R \times C} \times 100 \tag{2.5}$$

Here, D denotes the difference between encrypted images. Its value is 1 if encrypted image pixels are different else it is 0. On the other side, R, C denote the rows and columns of the images.

5. **Maximum Deviation (MD)**: Maximum deviation is the sum of the difference between the histograms of the plaintext image and the encrypted image [44]. The mathematical representation of maximum deviation is represented in Eq. (2.6).

$$D_{max} = \frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} di \tag{2.6}$$

6. **Chi-Square Test:** Chi-square test (χ^2) is performed to verify the histogram uniformity. It is determined for encrypted images using Eq. (2.7).

$$\chi^2 = \sum_{i=0}^{np} \left(\frac{(O_i - E_i)^2}{E_i} \right) \tag{2.7}$$

7. **Payload Capacity:** Payload capacity parameter defines how many bits per pixel is hidden in the image steganography.
8. **Structural Similarity Index Measure (SSIM):** SSIM measures the image quality based on original initial image which is free of compassion or distortion. SSIM index estimates perceived errors which mean that is consider image distortion as perceived alteration in structural information. It is based on estimating when the pixels have inter dependencies particularly when theses pixels are spatially close. Inter dependencies provides significant structure information of the objects in visual scene. SSIM can be mathematically calculated as given in 2.8.

$$SSIM(c, s) = \frac{(2\mu_c\mu_s + C_1)(2\sigma_{cs} + C_2)}{(\mu_c^2 + \mu_s^2 + C_1)(\sigma_c^2 + \sigma_s^2 + C_2)} \tag{2.8}$$

9. **Universal Image Quality Index (UIQI):** UQI is a Universal image quality index for measure the distortion between two input images. This approach based on configuring three factors which is luminance distortion, contrast distortion and structural comparisons. Despite this index is mathematically defined without considering the HVS, experimental results show that it reveals amazing reliability with subjective quality measurement. UQI performs better quality evaluation comparing with MSE and PSNR. Based on the above three comparison, UQI can be described as given in 2.9 and 2.10.

$$UQI(c,s) = L(c,s), C(c,s), S(c,s) \tag{2.9}$$

$$UIQI = \frac{4\mu_c\mu_s\mu_{cs}}{(\mu_c^2+\mu_s^2)(\sigma_s^2+\sigma_s^2)} \tag{2.10}$$

Where $\mu c, \mu s$ indicates the mean values of cover and stegoed images. And $\sigma c \sigma s$ indicates the standard deviation of cover and stegoed images, and μcs is the covariance of both images.

10. **Root Mean Square Error (RMSE):** The root mean square value is a standard way of measuring the error of a model in predicting quantitative data. Formally it is defined as follows:

$$RMSE = \sqrt{MSE} \tag{2.11}$$

11. **Image Fidelity (IF):** The image fidelity parameter measures the distortion in the stego image due to data hiding.

$$IF = 1 - \frac{\sum_{jk}(I_{jk}-O_{jk})^2}{\sum_{jk} I_{jk}\times O_{jk}} \tag{2.12}$$

In Eq. (2.12), I_{jk}, O_{jk} denotes the input and output image pixel value in the image steganography.

2.8 Bio-Inspired Optimization Algorithms Utilized in this Research

In the proposed methods, three bio-inspired algorithms, namely, Egyptian Vulture Optimization (EVO), Green Heron Optimization (GHO), and Black Widow Optimization (BWO) algorithm is taken into consideration. The detailed description of these algorithms is given below.

2.8.1 EVO Algorithm: The Egyptian vulture optimization (EVO) algorithm is based on the natural processes employed by Egyptian vulture for food acquisition [73-75]. The Egyptian vultures eat the eggs of the other birds as their food. To break the eggs, these vultures use activities, such as, tossing with pebbles, rolling with twigs, and change the angle of the eggs for searching the weak points. The steps for the EVOA are shown in Fig. 2.1. The details of the steps are explained below.

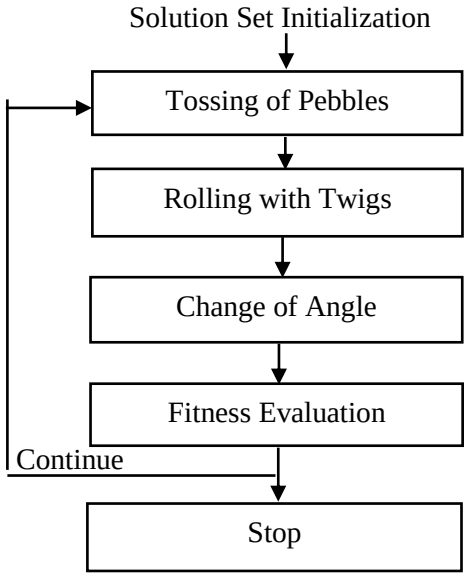


Figure 2.1: Steps of Egyptian Vulture Optimization Algorithm [73]

- *Solution Set Initialization:* The initialization of the parameters is done in the form of variables that represent initial solution sets. The refinement of variables is done to determine the superimposed conditions and constraints.
- *Tossing with Pebbles:* The Egyptian vulture uses the pebbles to break the eggs of other birds. The pebble works as a hammer, which is hit number of times on random position of the eggs to find the weak point and break the egg.
- *Rolling with Twigs:* The Egyptian vulture uses another astonishing skill, i.e., rolling with twigs to search the other weak points in the eggs. The rolling with twigs is performed when no suitable match is found, as a result of hit with pebbles.
- *Change of Angle:* The Egyptian vulture uses one more technique to increase the chances of breaking the eggs, by changing the angle of the eggs.
- *Fitness Evaluation:* The Egyptian vulture checks the condition of the egg after *hitting with pebble*, *rolling with twigs* and *change of angle* to evaluate the weak points that are formed on the eggs.

- *Check Condition to continue or to stop*: Based on the fitness evaluation and initialization parameters, the iteration is continued or stopped.

2.8.2 GHO Algorithm: The Green Heron optimization (GHO) algorithm is inspired by the technique used by Green Heron birds for food acquisition through their artistic skills, senses and intelligence [76]. The Green Heron birds reside in low-lying locations with abundant fish prey. The Green Heron optimization algorithm has previously been applied in several optimization problems such as travelling salesman problem [77], 0/1 Knapsack problem [78], and Quadratic Assignment problem [78]. The flow diagram of Green Heron algorithm is shown in Fig. 2.2.

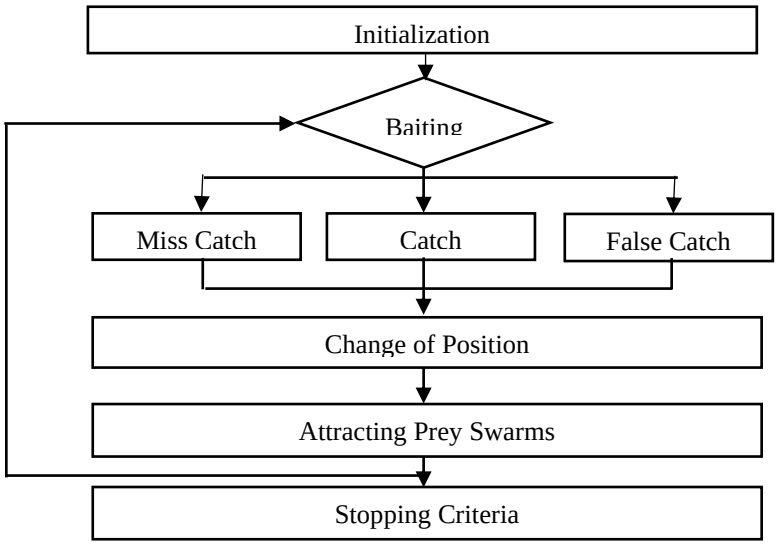


Figure 2.2: Flow Diagram for GHO Algorithm (Adapted from [76])

This algorithm has three main steps namely: *baiting, change of position, and attracting prey swarm.* The last step, namely, *Stopping Criteria* terminates the optimization search upon completion. The steps are as described below:

- *Baiting*: Initially, the Green Heron birds attract their prey with baits (feathers, earthworms, insects, bread crusts). In this step, the bird drops the bait in water and tries to catch the prey as shown in Figure 2.3. Here, there are three probable situations in view of catching prey namely, *Catch, Miss Catch, False Catch*. If the prey is caught with dropping bait in the water, it is known as *Catch* operation as shown in Figure 2.3(a) and if catch is missed then it is known as *Miss Catch* as shown in Figure 2.3(b). On the other hand, in *False Catch* the bird sits near the water and without bait tries to catch the prey in the water as shown in Figure 2.3(c).

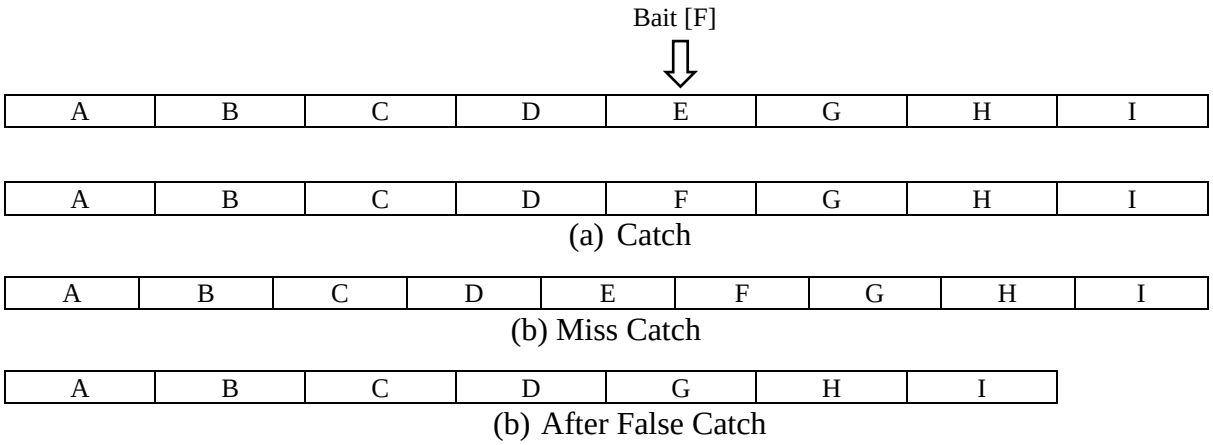


Figure 2.3: Baiting Operation (a) Catch (b) Miss Catch (c) After False Catch (Adapted From [76])

- *Change of Position:* Next, *Change of Position* is the local search strategy that is applied by birds to get maximum probability of catching the prey in short interval of time. In this step, if *Miss Catch* happens after dropping the bait in the water, the bird changes the position to get maximum probability of prey in quick interval of time as shown in Figure 2.4.

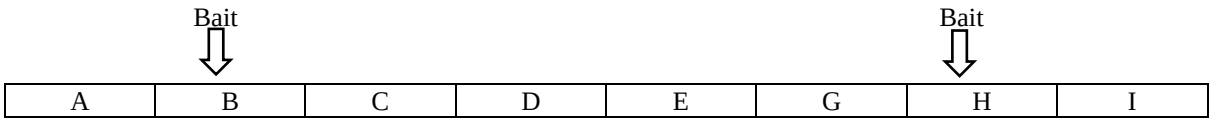


Figure 2.4: Change of Position Operation (Adapted From [76])

- *Attracting Prey Swarm:* In this step, the bird sits near water with bait and in place of dropping bait it attracts the prey to come near the surface. In this step, even after changing position there is *Miss Catch*, the bird sits near water and the string circularly shifts to get solution as shown in Figure 2.5 (a, b).
- *Stopping Criteria:* At last, based on the number of iterations, the operation of searching prey with bait continues or stops.

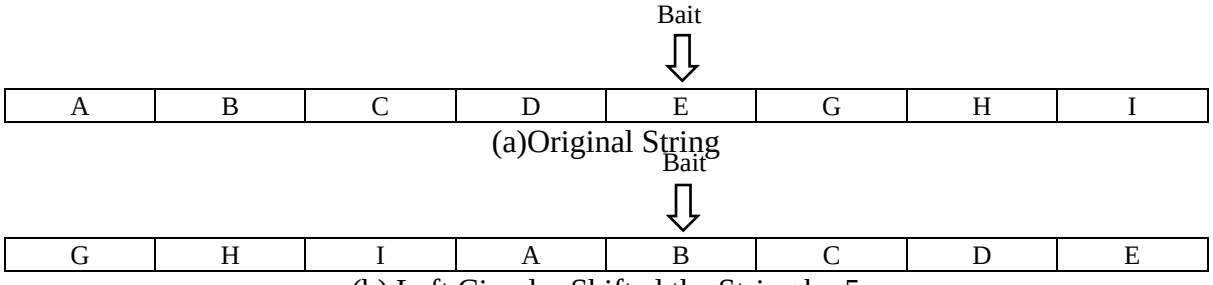


Fig.2.5 Attracting Prey Swarms Operation (a) Original String (b) Left Circular Shifted the String by 5 (Adapted From [76])

2.8.3 BWO Algorithm: The evolutionary black widow optimization (BWO) method is inspired by the mating habits of black widow spiders [79]. Figure 2.6 illustrates the flowchart of BWO algorithm. The steps of BWO are as follows:

- **Initialization of Population:** In order to find a workable solution to an optimization process, the numbers of the relevant variables need to take on a certain shape. In the terminology of PSO and GA, this structure is described as a chromosome; and in the terminology of PSO, it is referred to as a particle location. However, in the black widow optimization method (BWO), it is referred to as a widow.

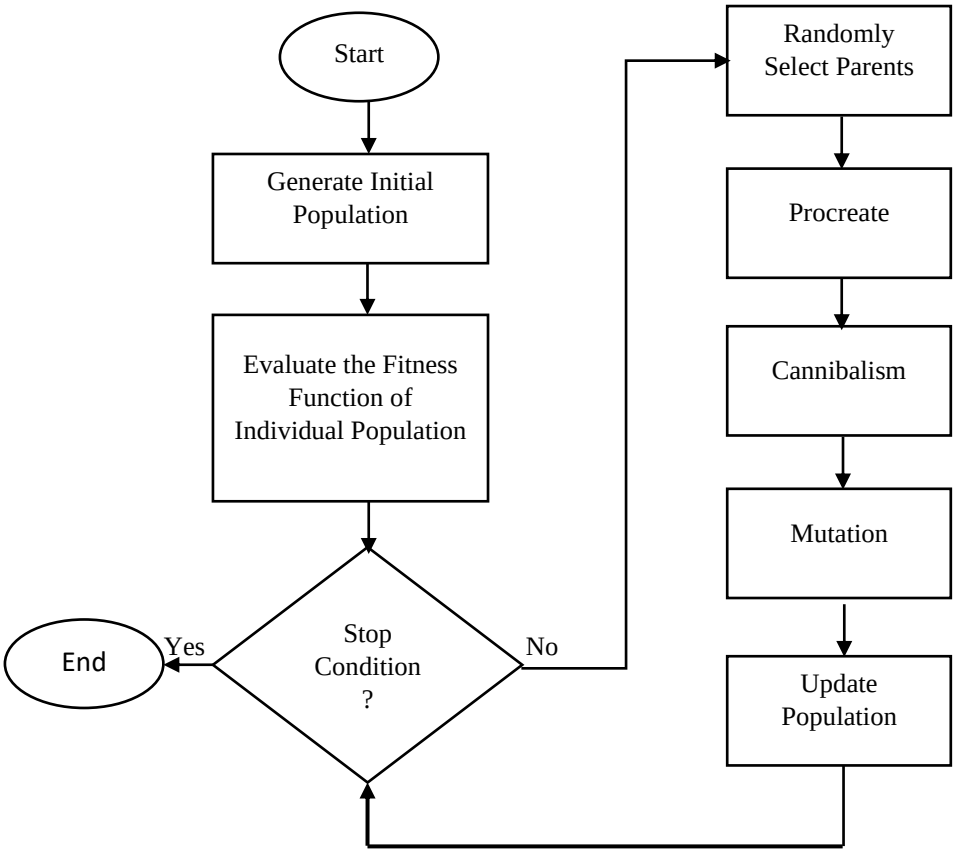


Figure 2.6: Flowchart of Black Widow Optimization Algorithm (Adapted from [79])

Each possible answer is compared to a Black Widow spider in the Black Widow Optimization (BWO) Algorithm. Black widow spiders represent the issue variables and their values. For the purposes of this work, the structure may be thought of as an array for the purposes of solving benchmark functions.

The solution to the optimization problem with N_{var} dimensions is represented as a widow, an array of size $1 \times N_{var}$. The following is the syntax for defining this array:

$$\text{widow} = [x_1, x_2 \dots \dots \dots \dots \dots x_{Nvar}] \quad (2.13)$$

Here, $[x_1, x_2 \ldots . . x_{Nvar}]$ denotes the widows. Further, evaluation of the widow is done based on the fitness function f.

$$\text{Fitness}=f(widow) = (x_1, x_2 \ldots \ldots \ldots \ldots \ldots x_{Nvar}) \quad (2.14)$$

First, a spider population, denoted by N_{pop}, is formed to populate a potential widow matrix, of size N_{var}. The next phase is to carry out the mating process for a randomly chosen set of parent couples, at the point which the female black widow will consume the male.

- **Procreate:** Because the couples are autonomous from one another, they begin to mate in order to generate a new generation simultaneously. This replicates how mating occurs in nature, where each pair does it in its own web, independently of the others. In the actual world, each successful mating results in the production of around one thousand eggs, but in the end, some of the spider infants survive to become stronger adults. Thus, in this reproducing technique, we need to first generate a widow array containing random values (named alpha), and then we use alpha in the following formula (equation1), where x_1 and x_2 are the parents, and y_1 and y_2 are the offspring.

$$\begin{cases} y_1 = \alpha \times x_1 + (1-\alpha) \times x_2 \\ y_2 = \alpha \times x_2 + (1-\alpha) \times x_1 \end{cases} \quad (2.15)$$

While carrying out this procedure $N_{var}/2$ times, one should take care to avoid duplicating any of the randomly chosen numbers. Cannibalism score is then used to choose some of the most fit people to add to the newly formed population. Afterwards, the offspring and the mother are placed to an array and ordered by their overall fitness value. These procedures are applicable to both sets.

- **Cannibalism:** Specifically, there are three distinct forms of cannibalism at action here. The first kind of cannibalism is known as sexual cannibalism, and it occurs when a female black widow consumes her husband while they are mating or shortly thereafter. The fitness scores were used to distinguish between male and female users of this method.

  Cannibalism can also occur within a species, such as when stronger spiderlings eat their weaker siblings. The number of survivors is calculated in this algorithm based on a cannibalism rating (CR) that we establish. It is not uncommon to see the third kind of cannibalism, in which the young spiders consume their mother. The fitness value is used to rank baby spiders on a scale of how healthy they are.

- **Mutation:** Mutation step is performed to alter the population randomly. This variation is performed very small in the population based on the mutation rate.

2.9 Contributions of the Research Work

In this dissertation, we have explored bio-inspired search-based optimization algorithms for their suitability in image data steganography and cryptography applications. We have proposed new image steganography methods based on two swarm-based optimization algorithms, that improve the imperceptibility of the data embedding. Subsequently, another bio-inspired optimization algorithm, namely, the evolutionary algorithm with better exploration rate is employed to implement image steganography. Next, a cryptographic key generation method is proposed based on bio-inspired evolutionary algorithm for better image encryption. Finally, a hybridization of cryptography and steganography is done for proposing privacy-preserving method of image data. The research contribution is further explained below:

- **Swarm Intelligence Algorithm based Image Steganography**

  Two swarm intelligence algorithms, namely, Egyptian vulture optimization (EVO) and green heron (GH) algorithms are used for optimized data hiding in image steganography. These algorithms search for the optimal form of secret data and cover image index by performing various operations on them for optimized data hiding. EVO and GH perform three operations in their iterative process, to explore the solution space and search for the optimal solution. EVO algorithm performs hit with a pebble, rolling with twigs, and change of angle operations, whereas the GH optimization algorithm performs baiting, changing of position, and attracting prey swarm operations. Due to these operations, the optimal form of secret data and cover image index becomes variable. Also, the scanning order for the data hiding in the cover image is varied from for different image data. The setup configuration of the EVO and GHO algorithms and complete subjective and objective analyses of the proposed image steganography are provided along with the comparative analysis is shown in Chapter 3.

- **Image Steganography Method based on Evolutionary Algorithm**

  An optimized image steganography method is proposed based on the black widow optimization (BWO) algorithm. The BWO algorithm searches the optimal cover image, block order, and secret data index to enhance the imperceptibility parameter by minimizing the objective function. The novelty of the method is that, instead of searching the optimal secret data index, it searches the optimal secret data and cover image indexes. The cover image indexes define the chosen cover image as well as the best block order for it. On the other hand, the secret data index defines what operation was performed on the secret data,

which gives the minimum variability. The objective analysis shows that the proposed method achieves low values of MSE; high values of PSNR and correlation coefficient; and comparable entropy between cover and stego image. The detailed description of image steganography method based on evolutionary algorithm is shown in Chapter 4.

- **Key Generation for Image Encryption based on Evolutionary Algorithm**

  We have proposed two image encryption methods by generating the random key based on the BWO algorithm. In the first method, the BWO algorithm is used for key generation based on the objective function. The "mutation" operation is used in the encryption process. The second method proposed is based on the chaotic function whose output is highly sensitive to the input parameter values. Thus the optimal selection of parameter values enhances the security of the image encryption method. Therefore, the BWO algorithm is used to determine the best values for the parameter based on the objective function. In the proposed method Entropy is taken as an objective function in both methods. Performance metrics are measured that make it robust against various attacks. The detailed description of key generation for image encryption method based on evolutionary algorithm is shown in Chapter 5.

- **Hybridization of Cryptography and Steganography Algorithms to achieve Privacy-Preserving Method**

  A privacy-preserving method is designed for public health surveillance data using a hybridized approach utilizing both the data security methods, namely, image steganography and cryptography. The proposed method provides better imperceptibility and security as compared to the existing methods. The optimal cover image plane is chosen based on the pixel intensity value and the data is split into sensitive and non-sensitive part. The sensitive part of the data is encrypted using black widow optimization algorithm. In the encryption process, exclusive OR operation is performed between data and random key and the data is hidden in the inferior plane in an optimal way. The comparative analysis shows that the proposed method provides superior performance over the existing methods. The detailed description of proposed privacy-preserving method based on evolutionary algorithm is shown in Chapter 6.

2.10 Conclusion

In this chapter, initially, we have analysed the related work is done in the steganography, cryptography, and their hybrid approaches. Based on the existing study, research gap and objectives are defined. Further, the details of the standard dataset utilized for our work is given along with the software platform and performance metrics to evaluate the performance of the proposed bio-inspired cryptography and steganography methods. Next, an overview of bio-inspired algorithms (EVO, GHO, and BWO) is given which is taken into consideration in this research. In the last, the research contribution is defined.

Chapter 3

Image Steganography Method based on Swarm Intelligence Algorithms

3.1 Introduction

The main motive of image steganography is to hide the secret data in the cover image in such a way that it is imperceptible to the attacker [2]. This goal can be accomplished if the distortion generated by the data hiding process in the cover image is kept to a minimum. In order to accomplish this goal, in the proposed image steganography methods, swarm intelligence algorithms are utilized. In this chapter, two swarm intelligence algorithms, namely, Egyptian Vulture Optimization (EVO) and Green Heron Optimization (GHO), are taken into consideration in the proposed method/s because these algorithms required the minimum input parameters to search the solution space and quickly explore the solution space due to better exploration and exploitation rates [73,76]. Due to these advantages, in the proposed method, two approaches are designed. In the first approach, an optimal secret data index and cover image index finding method is proposed for image steganography. The novelty of the first approach is that swarm intelligence algorithms search the optimal cover image index along with the secret data index based on the objective function, which was not claimed by other authors in the previous studies. The swarm intelligence algorithms search the best cover image among the *n* of cover images, followed by the optimal block index in the best cover image, and finally, the optimal secret data index. After determining these indexes, the data hiding is achieved in the best cover image using the least significant bit (LSB) algorithm. In the second approach, a matching method is proposed for image steganography. The novelty of the second approach is that the swarm intelligence operations are utilized for matching the secret data bits with the *k*-LSB bits of the cover image in place of the linear search process, which is done by other authors in the literature [58,61]. Followed by hiding the matching index in the same cover image in the optimal way using the swarm intelligence algorithms.

To elaborate on these approaches, the remaining chapter is divided into four parts. Section 3.2 defines the proposed approaches as being designed for image steganography based on swarm

intelligence algorithms. Section 3.3 explains the first approach designed for the image steganography method based on the swarm intelligence algorithm, in which the optimal secret data and cover image index are determined. This section also includes a detailed description of data embedding, extraction, and results. Section 3.4 explains the second approach, which is designed for image steganography and is based on matching the secret data bits with the cover image pixel and hiding the matched index in an optimal way using swarm intelligence algorithms. In the last, Section 3.5 concludes the proposed method.

3.2 Proposed Approaches of Image Steganography based on Swarm Intelligence Algorithms

The main motive of the proposed image steganography approaches is to enhance the security parameter known as imperceptibility, as elaborated in Section 3.1. Two optimized data hiding approaches are designed to achieve this goal. The optimal secret data and cover image index are determined using swarm intelligence algorithms in the first approach. To achieve this goal, *n* number of cover images and secret data are given to the swarm intelligence algorithm. Based on this information, the swarm intelligence algorithm performs various operations on the cover image and secret data, evaluates their fitness based on the objective function, and searches for the optimal index of cover image and secret data. The operations that are performed on the secret data or cover image are given an index value. Therefore, the initial population of the EVO and GHO algorithms is randomly initialized in the index value range. Following that, they perform operations on the index values to generate new indexes (such as hitting with a pebble, rolling with twigs, and changing angles in the EVO algorithm, whereas baiting, changing positions, and attracting prey swarms in the EVO algorithm). The benefit of the EVO and GHO algorithms is that instead of performing all operations in a sequential way, they perform them one after another only when the previous operation did not give the optimal index. Once the secret data and cover image index are obtained, based on them, the data is hidden in the cover image using the LSB algorithm.

In the second approach, a matching method is proposed in which secret data bits are matched with cover image pixels and the matched indexes are determined. After that, matched indexes are hidden in the same cover image in the optimal way. To accomplish this goal, the cover image was split into two parts. The first part of the cover image is matched with secret data bits. The matching is performed in the LSB bits of the cover image pixel because matching the

entire pixel of the cover image, requires more computation, and the matching index varies according to the pixel value. For example, in the grey-scale images, the pixel is 8 bits long. Therefore, the matching index varies from 0 to 7. Further, in place of matching the LSB bits in a consecutive manner based on EVO and GHO operations, the matching bit position of the pixel is determined. If the matching position is found, then the optimal matched index is determined; otherwise, LSB-based data hiding is performed and matched index 0 is defined. The LSB is the most optimal position for data hiding. Therefore, it is used for data hiding when matching cannot be achieved with the cover image. Next, the second part of the cover image, along with a matched index, is given to the swarm intelligence algorithms in this work. These algorithms based on the objective function determines the optimal starting pixel in the cover image. After determining the optimal starting pixel index, 2-bit LSB method-based data hiding is performed in the cover image. A complete explanation of these methods is given in the following sections.

3.3 Optimal Secret Data Index and Cover Index Finding Method

The main motive of this method is to determine the secret data and cover image index to enhance the imperceptibility parameter. To achieve this objective, the optimal secret data index is determined by performing various operations, such as flipping, shifting, and swapping, on the original secret data. The optimal cover index, on the other hand, is determined by selecting the best cover image from a large number of cover images. Further, finding the optimal block order index for the best cover image. Thus, optimal cover index provides two pieces of information: the selected cover image and the block index within it. A detailed description of secret data operations and cover index selection is given below.

3.3.1 Optimal Secret Data Index

Here, we have explained how various operations are performed on the secret data to determine the optimal secret data index. Figures 3.1–3.3 show the various secret data indexes and how they impact the variability parameter. Figure 3.1 explains the flipped secret data form. In this form, the secret data bits are flipped, for example, from 1-0 to 0-1 and vice versa. In Figure 3.1(c), the pixels are shown in red, which provides variability after substituting the original secret data form in the cover image pixel. Out of 8 pixels, 5 pixels provide variability. Next, Figure 3.1(d) shows the flipped form of secret data, and its substitution in the cover image pixels is shown in Figure 3.1(e). Further, the pixels that provide variability are highlighted in

red. It is observed that out of 8 pixels, only 3 pixels provide variability. This shows that the flipped form reduces the variability from 5 pixels to 3 pixels.

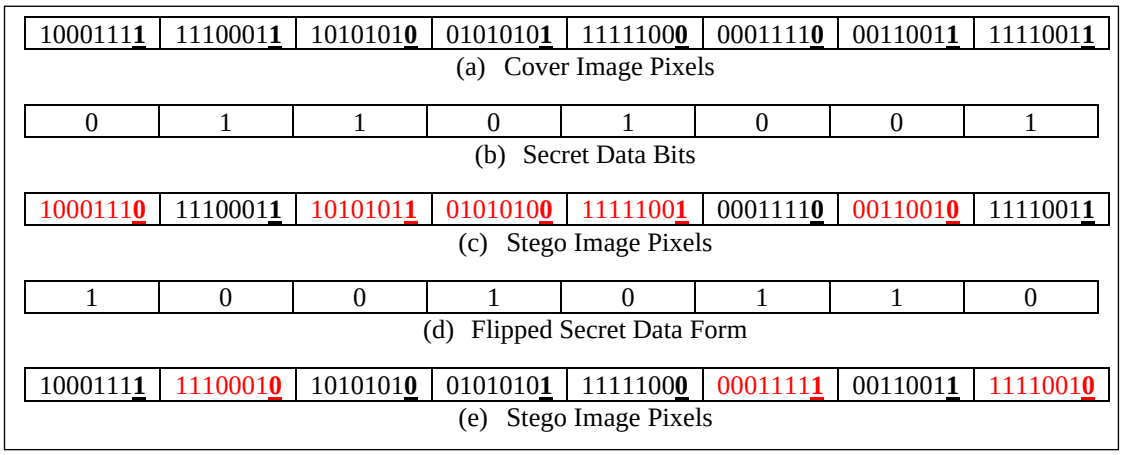


Figure 3.1: Flipped Secret Data Form

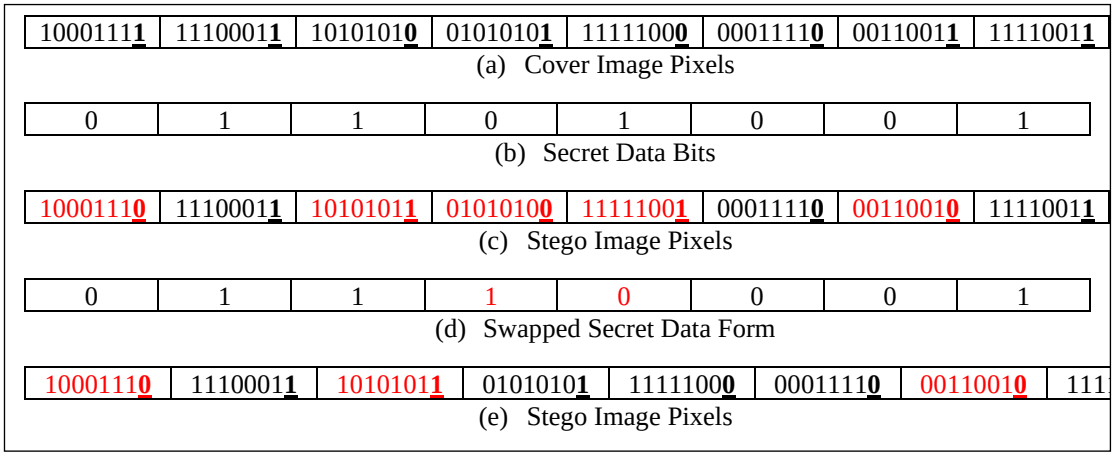


Figure 3.2: Swapped Secret Data Form

Figure 3.2 explains the swapped secret data form. In this form, the secret data bits are swapped. In Figure 3.2(c), the pixels are shown in red, which provides variability after substituting the original secret data form in the cover image pixel. Out of 8 pixels, 5 pixels provide variability. Next, Figure 3.2(d) shows the swapped form of secret data (the swapped bits are highlighted in red color), and its substitution in the cover image pixels is shown in Figure 3.2(e). Further, the pixels that provide variability are highlighted in red. It is to be noted that, here, out of 8 pixels, only 3 pixels provide variability. This demonstrates how swapped form reduces variability from 5 to 3 pixels.

Figure 3.3 explains the circular shift operation on the secret data. In this operation, the secret data bits are circularly shifted randomly. In Figure 3.3(c), the pixels are shown in red, which

provides variability after substituting the original secret data form in the cover image pixel. Here, out of 8 pixels, 5 pixels provide variability. Next, Figure 3.3(d) shows the 1-time left circular shift operation of secret data and its substitution in the cover image pixels, as shown in Figure 3.3(e). Additionally, the pixels that provide variation are highlighted in red. Out of 8 pixels, only 1 pixel provides variability. This shows that a circular shift operation reduces the variability from 5 pixels to 1 pixel.

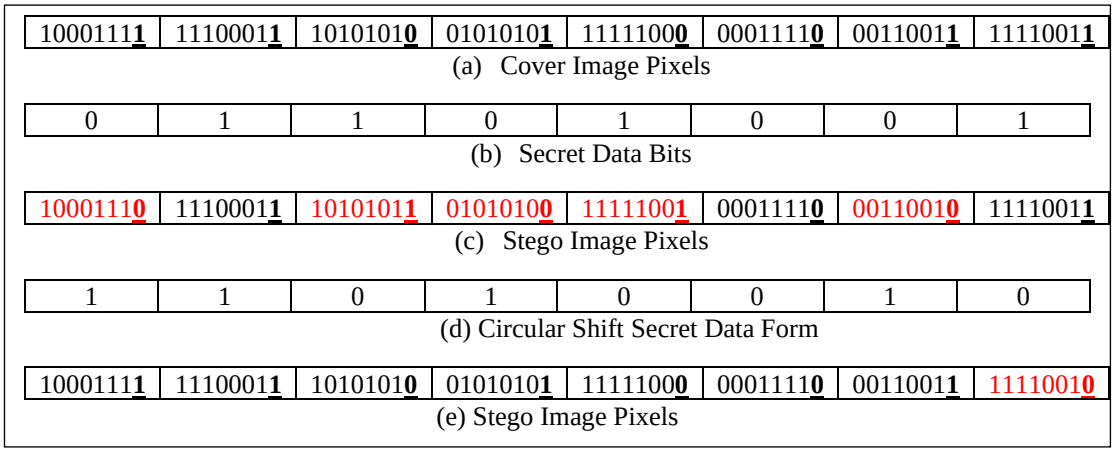


Figure 3.3: Circular Shift Secret Data Form

Finally, we have explained the how various forms of the secret data is generated using the Eq. (3.1-3.4). The original form is determined using Eq. (3.1), flipped form is determined using Eq. (3.2), circular shift form is determined using Eq. (3.3), and transpose form is determined using the Eq. (4), respectively.

Original $$D' = D \tag{3.1}$$

Flipped $$D' = D_{max} - D \tag{3.2}$$

Circular Shift $$D' = Circular\ Shift\ (D, SF) \qquad 1 \leq SF \leq D_{length} \tag{3.3}$$

Transpose $$D' = D^T \tag{3.4}$$

3.3.2 Optimal Cover Image Index

The main purpose of finding the optimal cover image is to determine which cover image gives the least variability after data hiding. To accomplish this aim, two processes are done on the cover image. In the first process, the best cover image is found, whereas in the second process, the optimum block order index is determined. Thus, optimal cover image index is a matrix with

two elements: the first defining the cover image index and the second defining the optimal block order index.

3.3.3 Data Embedding and Extraction based on the Swarm Intelligence Algorithms

The flowchart of the data embedding using swarm intelligence algorithms (Egyptian Vulture Optimization (EVO) & Green Heron (GH) algorithm) are shown in Figure 3.4.

Initially, *n* number of cover images and secret data are read and given to the swarm intelligence algorithm. The swarm intelligence algorithm determines the optimal secret data and cover image index. This index value, along with the cover image and secret data, is given to the data embedding algorithm.

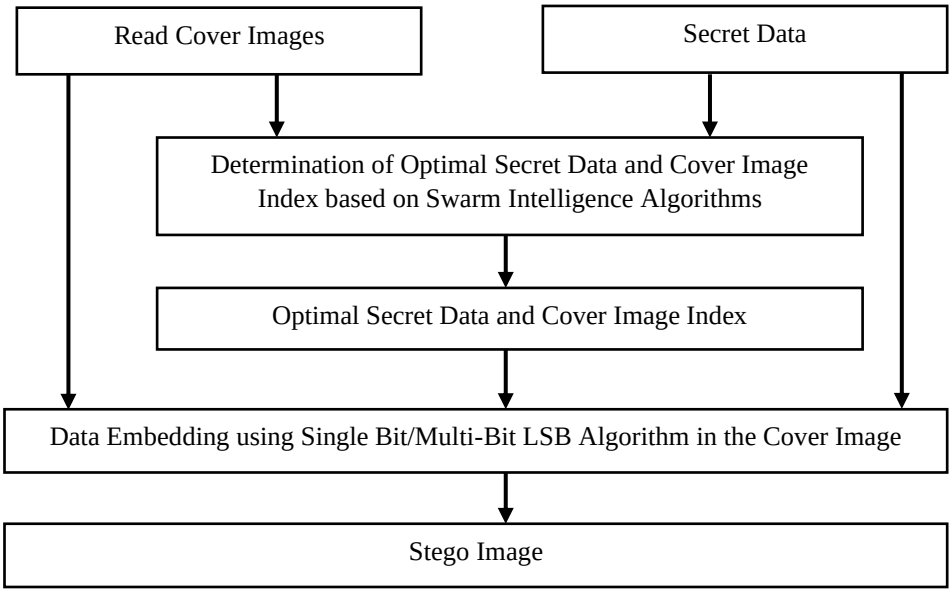


Figure 3.4: Block Diagram of Data Embedding using Swarm Intelligence Algorithms

Further, it performs the single-bit/multi-bit LSB-based data hiding in the cover image based on the given index values and gives the STEGO image in the output. The stego image, along with secret data and cover image index information, need to be communicated with the receiver. Next, we have explained the steps by which the EVO and GHO algorithms search for the optimal secret data and cover image index, as explained below:

- In the first step, the EVO/GHO algorithms' parameters are initialized in terms of population, dimension of each population, iterations, objective function, lower and upper limits of the cover image, block order, and secret data index.

- In the second step, the population array is randomly initialized at the lower and upper limits of the cover image, block order, and secret data index.
- The population fitness evaluation is performed in the third step based on the objective function to determine which population index provides the lowest MSE over the other population. The initial best population is the one with the lowest MSE among all populations.
- In the fourth step, one population is randomly chosen and its operations (for example, in EVO: hitting with a pebble, rolling with twigs, and changing angles, whereas in GHO: baiting, changing positions, and attracting a prey swarm) are performed to generate new indexes. These operations are performed one after another only when the previous operation's fitness is inferior to that of the best population. Besides that, the best population is updated if the superior population is found while performing these operations.
- Then, step 4^{th} repeated for a fixed number of iterations until the optimal secret data and cover image index are determined.

The block diagram of data extraction is shown in Figure 3.5. Initially, the stego image is read along with the information from the secret data and cover image index and given to the single/multi-bit LSB data extraction algorithm. The extraction algorithm extracts the secret data bits from the optimal blocks of the cover image based on the cover image index information. Next, based on the secret data index information, the inverse operations are performed on it to reconstruct the original secret data.

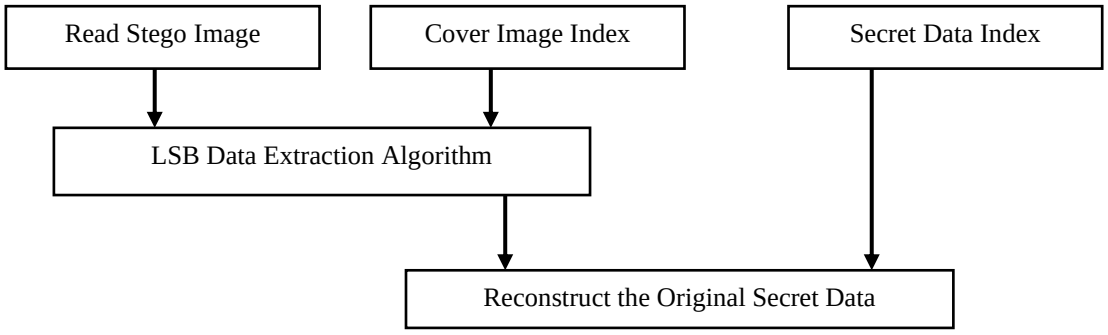


Figure 3.5: Block Diagram of Data Extraction for Swarm Intelligence Algorithms

3.3.4 Results and Analysis

In this section, the results and analysis are shown which is performed for proposed methods based on EVO/GHO algorithm. The ten grey-scale and color images are taken under

consideration are *Lena, Baboon, Barbara, Pepper, Boat, Cameraman, Airplane, Female, couple, house*. The proposed method searches the best cover images from it. Further, the proposed method is simulated thirty times for different secret data (fifteen times for grey-scale images and fifteen times for color images, respectively). Moreover, simulation results for single and multi-bit LSB data embedding are shown. The initial parameter value of the EVO/GHO algorithm for determine the optimal secret data and cover image index is given in Table 3.1.

Table 3.1: Initial Parameter Values of the EVO/GHO Algorithm for Determine Optimal Secret Data and Cover Image Index

Parameter	**Values**
Population	50
Dimension	3
Iterations	30
Objective Function	MSE
Secret Data Index	[0-3]
Cover Image Index	[1-15]
Total Blocks Index	[1-4]
Cover Image Size	$[256 \times 256]$

- **Subjective Analysis**

Table 3.2 (a-b) shows the subjective analysis of the swarm intelligence algorithms (EVO/GHO) for determine optimal secret data and cover image index for grey-scale and color images. In this analysis, original cover image and stego image are compared. The result shows that the images look indistinguishable for swarm intelligence algorithms. Further, the benefit of the proposed method is that the cover image is chosen for data hiding is not fixed because swarm intelligence algorithms choose the best cover image among the *n* number of images. Table 3.3 (a-d) shows the subjective analysis between original cover and stego image based on their histogram for EVO/GHO for grey-scale and color images. In the ideal case, the histogram distribution should be same for both images. The outcome demonstrates that the histograms of both the cover and stego images are very similar in appearance.

Table 3.2 (a): Subjective Analysis of the EVO Algorithm for the Proposed Data Hiding Method

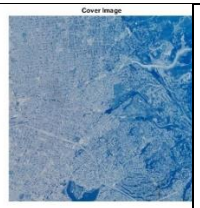
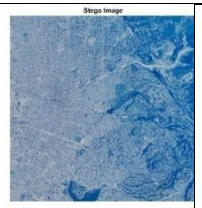
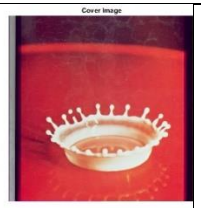
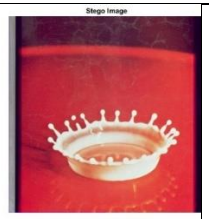
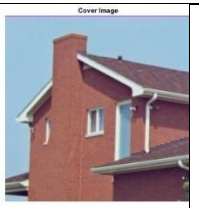
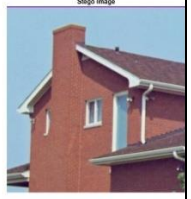
(for Grey-Scale Images)							
Cover Image	**Stego Image**	**Cover Image**	**Stego Image**	**Cover Image**	**Stego Image**	**Cover Image**	**Stego Image**
							
(For Color Images)							
							

Table 3.2 (b): Subjective Analysis of the GHO Algorithm for the Proposed Data Hiding Method

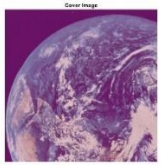
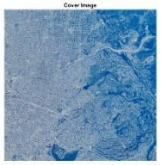
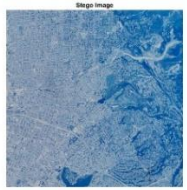
For Grey-Scale Images							
Cover Image	**Stego Image**	**Cover Image**	**Stego Image**	**Cover Image**	**Stego Image**	**Cover Image**	**Stego Image**
							
For Color Images							
							

Table 3.3 (a): Subjective Analysis based on the Histogram of the EVO Algorithm (for Grey-Scale Images)

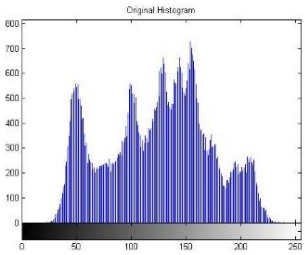
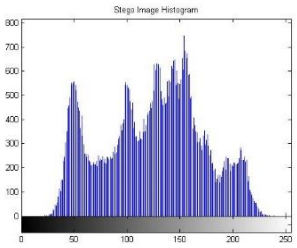
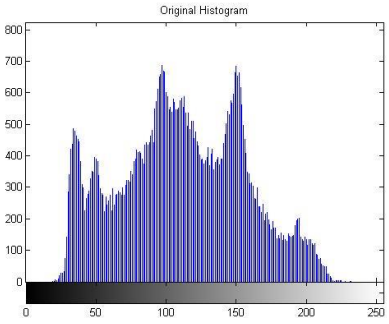
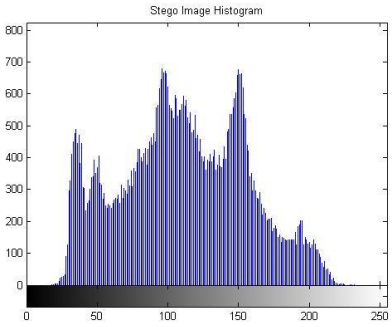
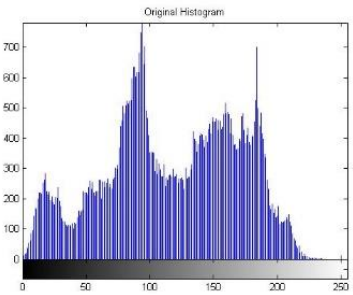
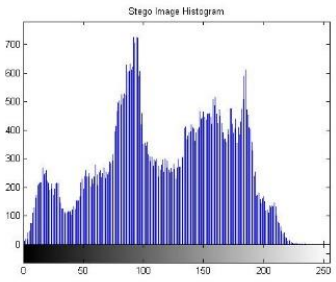
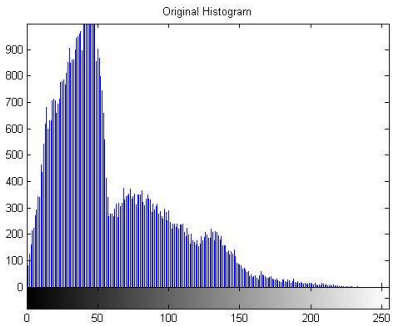
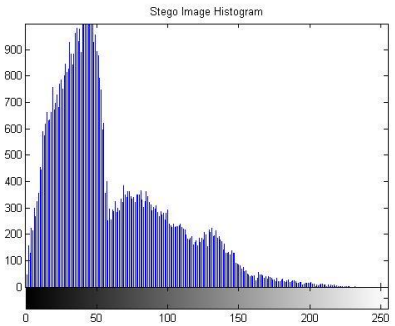
Secret Data1	**Cover Image**	**Stego Image**
1		
2		
3		
4		

Table 3.3 (b): Subjective Analysis based on the Histogram of the GHO Algorithm (for Grey-Scale Images)

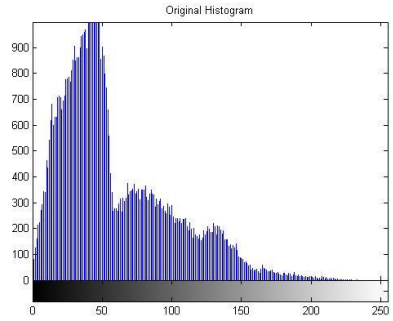
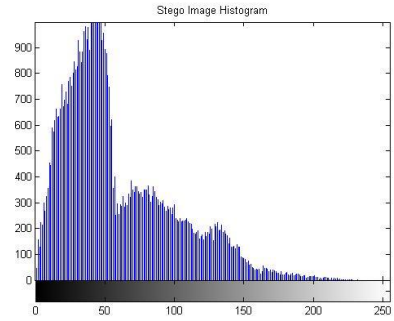
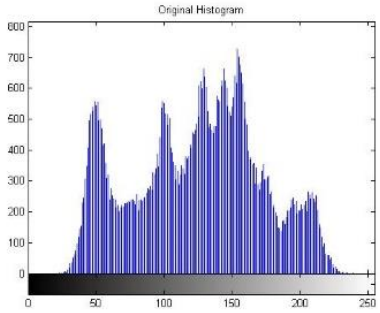
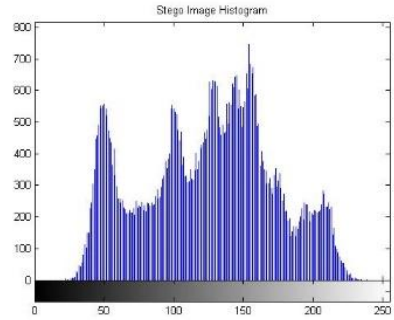
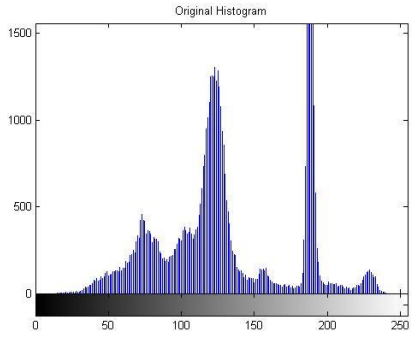
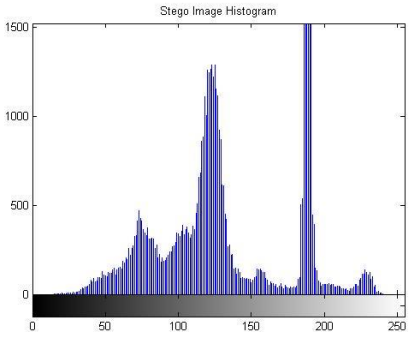
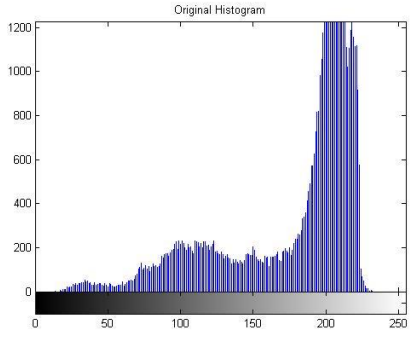
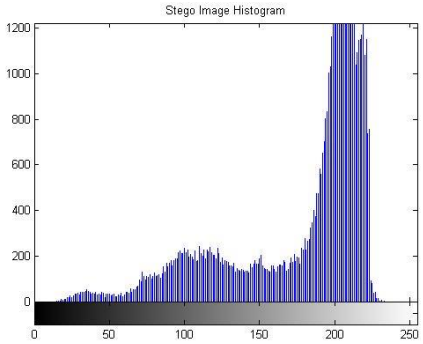
Selected Data	Cover Image	Stego Image
1		
2		
3		
4		

Table 3.3 (c): Subjective Analysis based on the Histogram of the EVO Algorithm (for Color Images)

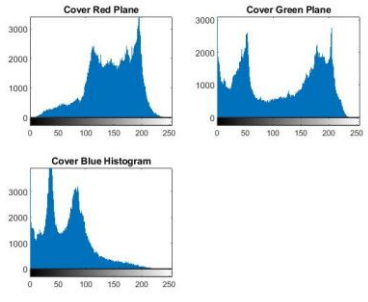
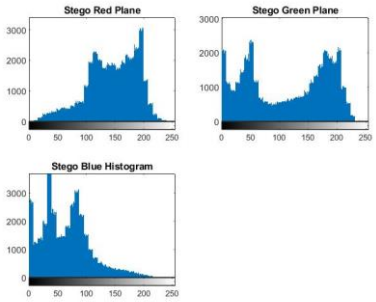
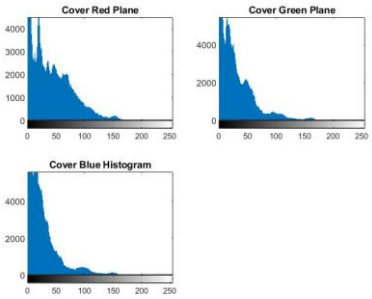
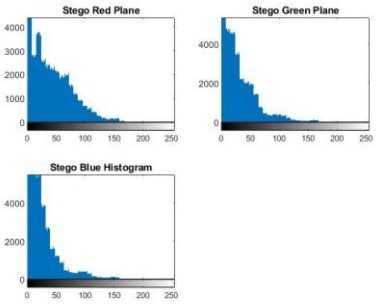
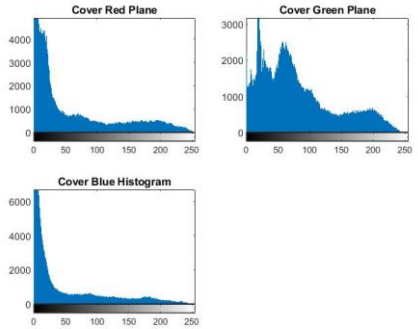
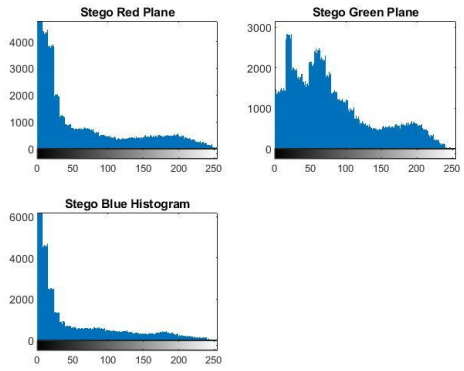
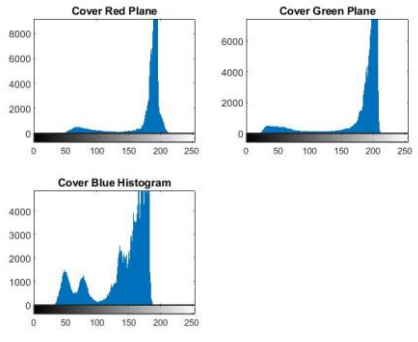
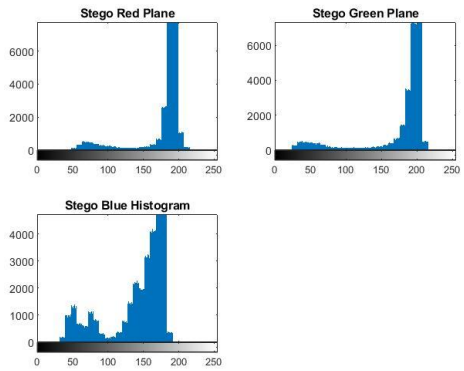
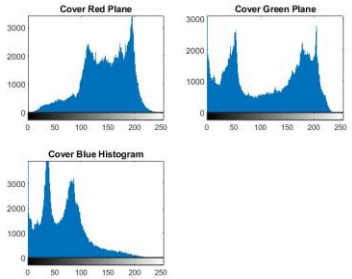
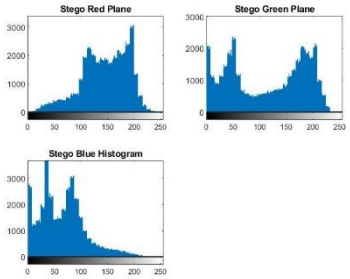
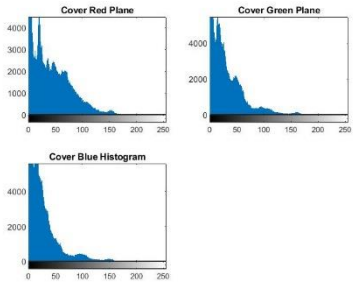
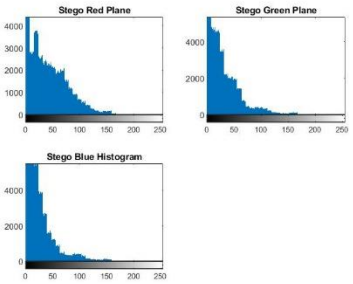
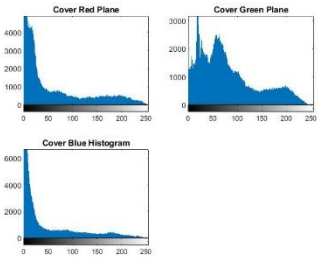
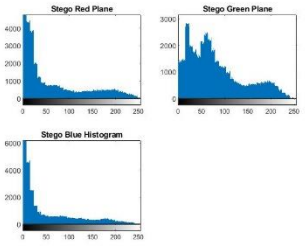
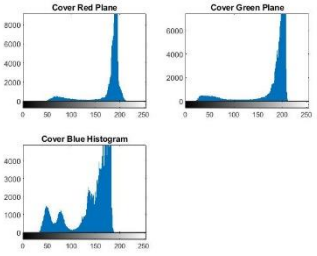
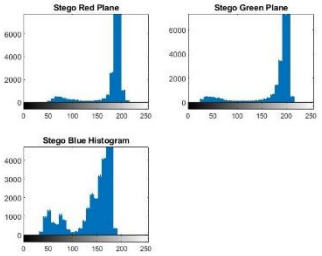
Selected Data	Cover Image	Stego Image
1		
2		
3		
4		

Table 3.3 (d): Subjective Analysis based on the Histogram of the GHO Algorithm (for Color Images)

Selected Data	Cover Image	Stego Image
1		
2		
3		
4		

- **Objective Analysis**

Table 3.4 shows the objective analysis of the matching method based on the various parameters for grayscale. The parameters taken under consideration are MSE, RMSE, PSNR, SSIM, CC, entropy, UIQ, IF, and NAE. Table 3.4 (a-b) shows the evaluation of the proposed method using the EVO and GHO algorithms for grayscale images for *the k-bit* LSB method. The result shows that the proposed method achieves a desirable PSNR value due to the lower error between cover and stego image. The error matrices are evaluated for the proposed method using the MSE, RMSE, and NAE parameters. Further, CC, SSIM, UIQI, and IF parameters show that the proposed method achieves a high value near to 1 value as required in the image steganography method. Next, the entropy analysis shows that the input and output entropy of the cover and stego image is approximate similar due to less variation in the pixel values. Finally, we have observed that both swarm intelligence algorithms give approximately similar results.

Next, the proposed method is evaluated for the color images for the EVO and GHO algorithms in Table 3.5 (a-b). In this approach, the data hiding is performed in the different planes of the color image. After that, average values of the parameters are reported in this table for *the k-bit* LSB method. The result shows that the proposed method achieves the high value for CC, SSIM, UIQI, and IF parameters. Followed by low values of MSE, RMSE, and NAE parameters. This reflects that the proposed method achieves the desired PSNR value for the k-bit LSB method. Finally, the entropy analysis shows that the proposed method achieves the similar values.

Table 3.4 (a): Objective Analysis of the EVO Algorithm (For Grey-Scale Images)

MSE	RMSE	PSNR	SSIM	CC	Input Entropy	Output Entropy	UIQ	IF	NAE
1-bit									
0.2454	0.4954	54.2324	0.9944	0.9998	5.7393	5.7572	0.9980	0.9986	0.0014
0.2466	0.4966	54.2109	0.9944	0.9998	5.7393	5.7573	0.9980	1.0000	0.0014
0.2449	0.4948	54.2418	0.9944	0.9998	5.7393	5.7572	0.9980	1.0000	0.0014
0.2463	0.4963	54.2167	0.9944	0.9998	5.7393	5.7572	0.9980	1.0000	0.0014
0.2463	0.4963	54.2167	0.9944	0.9998	5.7393	5.7573	0.9980	1.0000	0.0014
2-bit									
1.2102	1.1001	47.3024	0.9741	0.9988	6.4593	6.4932	0.9993	0.9994	0.0184
1.2079	1.0991	47.3103	0.9740	0.9988	6.4593	6.4932	0.9993	0.9994	0.0184
1.2138	1.1017	47.2893	0.9739	0.9988	6.4593	6.4932	0.9993	0.9994	0.0184
1.2118	1.1008	47.2965	0.9740	0.9988	6.4593	6.4931	0.9993	0.9994	0.0184
1.2131	1.1014	47.2920	0.9740	0.9988	6.4593	6.4932	0.9993	0.9994	0.0184
3-bit									
4.9203	2.2182	41.2109	0.8959	0.9948	6.4593	6.4988	0.9967	0.9977	0.0373
4.9267	2.2196	41.2053	0.8957	0.9948	6.4593	6.4988	0.9967	0.9977	0.0374
4.9125	2.2164	41.2178	0.8960	0.9948	6.4593	6.4989	0.9967	0.9977	0.0373
4.9332	2.2211	41.1995	0.8959	0.9948	6.4593	6.4988	0.9967	0.9977	0.0374
4.9277	2.2198	41.2043	0.8959	0.9948	6.4593	6.4989	0.9967	0.9977	0.0374

Table 3.4 (b): Objective Analysis of the GHO Algorithm (for Grey-Scale Images)

MSE	RMSE	PSNR	SSIM	CC	Input Entropy	Output Entropy	UIQ	IF	NAE
1-bit									
0.2463	0.4962	54.2168	0.9943	0.9998	5.7406	5.7588	0.997972	0.999992	0.001400
0.2436	0.4935	54.2647	0.9943	0.9998	5.7406	5.7592	0.997972	0.999992	0.001385
0.2449	0.4949	54.2406	0.9943	0.9998	5.7406	5.7589	0.997972	0.999992	0.001393
0.2449	0.4949	54.2409	0.9943	0.9998	5.7406	5.7593	0.997972	0.999992	0.001393
0.2442	0.4941	54.2541	0.9943	0.9998	5.7406	5.7592	0.997972	0.999992	0.001388
2-bit									
1.2083	1.0992	47.3092	0.9805	0.9988	6.4573	6.4910	0.999302	0.999429	0.018376
1.2117	1.1008	47.2967	0.9808	0.9988	6.4573	6.4912	0.999302	0.999427	0.018413
1.2073	1.0988	47.3127	0.9808	0.9988	6.4573	6.4909	0.999302	0.999429	0.018368
1.2120	1.1009	47.2958	0.9806	0.9988	6.4573	6.4911	0.999302	0.999427	0.018405
1.2141	1.1018	47.2884	0.9808	0.9988	6.4573	6.4909	0.999302	0.999426	0.018463
3-bit									
4.8699	2.2068	41.2556	0.9195	0.9949	6.4573	6.4971	0.996723	0.997697	0.037024
4.9147	2.2169	41.2158	0.9194	0.9948	6.4573	6.4978	0.996723	0.997676	0.037223
4.9080	2.2154	41.2217	0.9193	0.9948	6.4573	6.4974	0.996723	0.997679	0.037235
4.9407	2.2228	41.1929	0.9188	0.9948	6.4573	6.4975	0.996013	0.997664	0.037456
4.8713	2.2071	41.2544	0.9197	0.9949	6.4573	6.4973	0.996723	0.997697	0.037041

Table 3.5 (a): Objective Analysis of the EVO Algorithm (For Color Images)

Planes	MSE	RMSE	PSNR	SSIM	CC	Input Entropy	Output Entropy	UIQ	IF	NAE
	1-bit									
R	0.2532	0.5032	54.0956	0.9992	0.9999	7.2596	7.2543	1.000000	0.999980	0.002480
G	0.2500	0.5000	54.1517	0.9990	0.9996	6.6598	6.6593	1.000000	0.999985	0.001768
B	0.2513	0.5013	54.1289	0.9987	0.9990	6.0460	6.0453	1.000000	0.999985	0.001427
Avg.	**0.2515**	**0.5015**	**54.1254**	**0.9989**	**0.9995**	**6.6551**	**6.6529**	**1.000000**	**0.999983**	**0.001892**
R	0.2384	0.4883	54.3579	0.9961	1.0000	7.5235	7.51	1.000000	0.999985	0.001480
G	0.2504	0.5004	54.1451	0.9961	0.9999	7.7137	7.7117	0.999725	0.999985	0.001748
B	0.2744	0.5239	53.7466	0.9925	1.0000	4.6229	4.5464	0.999938	0.999982	0.004049
Avg.	**0.2544**	**0.5042**	**54.0832**	**0.9949**	**0.9999**	**6.6200**	**6.5894**	**0.999888**	**0.999984**	**0.002426**
R	0.2595	0.5094	53.9898	0.9939	0.9999	7.0218	7.0193	1.000000	0.999968	0.004484
G	0.2504	0.5004	54.1439	0.9950	0.9999	7.6111	7.6079	0.999779	0.999975	0.003089
B	0.2678	0.5175	53.8533	0.9932	0.9999	6.5157	6.5069	1.000000	0.999954	0.005922
Avg.	**0.259233**	**0.5091**	**53.9957**	**0.9940**	**0.9999**	**7.0495**	**7.0447**	**0.999926**	**0.999965**	**0.004498**
R	0.2497	0.4997	54.1570	0.9949	0.9999	7.0841	7.0807	0.999548	0.999985	0.001416
G	0.2609	0.5108	53.9664	0.9944	0.9999	6.9935	6.9771	1.000000	0.999970	0.003698
B	0.2504	0.5004	54.1446	0.9949	0.9999	6.2161	7.3826	1.000000	0.999971	0.003130
Avg.	**0.253667**	**0.503633**	**54.0893**	**0.9947**	**0.9999**	**6.7646**	**7.1468**	**0.999849**	**0.999975**	**0.002748**
R	0.2494	0.4994	54.1618	0.9956	0.9999	7.3826	7.3817	0.999416	0.999985	0.001726
G	0.2553	0.5053	54.0606	0.9954	1.0000	7.6544	7.6493	1.000000	0.999984	0.002254
B	0.2581	0.508	54.0135	0.9951	0.9999	7.1774	7.1613	1.000000	0.999958	0.003966
Avg.	**0.254267**	**0.504233**	**54.0786**	**0.9954**	**0.9999**	**7.4048**	**7.3974**	**0.999805**	**0.999976**	**0.002649**
	2-bit									
R	1.2461	1.1163	47.1752	0.9799	0.9995	7.2679	7.2633	0.998890	0.999924	0.003458
G	1.2508	1.1184	47.1590	0.9811	0.9995	7.5935	7.5909	0.999660	0.999901	0.006308
B	1.2454	1.1160	47.1777	0.9794	0.9989	6.9833	6.9798	0.999288	0.999899	0.005913
Avg.	**1.2474**	**1.1169**	**47.1706**	**0.9801**	**0.9993**	**7.2816**	**7.2780**	**0.999280**	**0.999908**	**0.005226**

R	1.2464	1.1164	47.1741	0.9853	0.9995	7.5791	7.5771	0.999587	0.999924	0.004636
G	1.2511	1.1185	47.158	0.9844	0.9994	7.4247	7.419	0.999562	0.9999	0.00613
B	1.2419	1.1144	47.1901	0.9848	0.9995	7.5188	7.515	0.999297	0.99989	0.006664
Avg.	**1.246467**	**1.116433**	**47.17407**	**0.984833**	**0.999467**	**7.507533333**	**7.5037**	**0.999482**	**0.999905**	**0.00581**
R	1.2823	1.1324	47.0509	0.9957	0.9994	7.2638	7.2543	0.998663	0.999897	0.006255
G	1.2552	1.1204	47.1437	0.9949	0.9982	6.6618	6.6593	0.998255	0.999923	0.004441
B	1.2537	1.1197	47.1488	0.9934	0.9952	6.0491	6.0453	0.995885	0.999923	0.003562
Avg.	**1.263733**	**1.124167**	**47.11447**	**0.994667**	**0.9976**	**6.658233333**	**6.652967**	**0.997601**	**0.999914**	**0.004752**
R	1.2580	1.1216	47.134	0.9736	0.9990	6.7861	6.7692	0.999386	0.999587	0.014981
G	1.3001	1.1402	46.991	0.9705	0.9987	6.3500	6.3389	1.000000	0.999309	0.021590
B	1.2672	1.1257	47.1023	0.9716	0.9985	6.2150	6.2105	0.998392	0.999203	0.022861
Avg.	**1.2751**	**1.129167**	**47.07577**	**0.9719**	**0.998733**	**6.450366667**	**6.439533**	**0.999259**	**0.999366**	**0.019811**
R	1.2528	1.1193	47.152	0.9751	0.9997	7.0943	7.0807	0.999096	0.999924	0.003548
G	1.3645	1.1681	46.7811	0.9688	0.9996	7.0323	6.9771	0.999811	0.999841	0.009528
B	1.2516	1.1187	47.1562	0.9754	0.9994	6.2278	6.2126	1.000000	0.999854	0.007822
Avg.	**1.289633**	**1.135367**	**47.02977**	**0.9731**	**0.999567**	**6.7848**	**6.7568**	**0.999636**	**0.999873**	**0.006966**
	3-bit									
R	5.5282	2.3512	40.705	0.8988	0.9964	6.8987	6.8834	0.997705	0.998475	0.029444
G	5.2500	2.2913	40.9292	0.9059	0.9985	7.1216	7.0807	0.996393	0.99968	0.007449
B	5.9645	2.4422	40.3751	0.8864	0.9985	7.0957	6.9771	0.999433	0.999304	0.020443
Avg.	**5.5809**	**2.361567**	**40.66977**	**0.897033**	**0.9978**	**7.038666667**	**6.9804**	**0.997844**	**0.999153**	**0.019112**
R	5.3233	2.3072	40.8690	0.9061	0.9976	6.2722	6.2126	0.999157	0.999379	0.01658
G	5.2246	2.2857	40.9503	0.9217	0.9974	7.3898	7.3817	0.997088	0.999681	0.009046
B	5.4677	2.3383	40.7528	0.9159	0.999	7.6721	7.6493	0.998979	0.999666	0.01195
Avg.	**5.338533**	**2.3104**	**40.85737**	**0.914567**	**0.998**	**7.111366667**	**7.0812**	**0.998408**	**0.999575**	**0.012525**
R	5.6533	2.3777	40.6078	0.91	0.9971	7.2128	7.1613	0.997307	0.999074	0.021252
G	5.2803	2.2979	40.9042	0.902	0.996	6.7884	6.7692	0.997549	0.998269	0.03153
B	5.702	2.3879	40.5705	0.8854	0.9947	6.3592	6.3389	0.997909	0.996983	0.04664
Avg.	**5.5452**	**2.3545**	**40.69417**	**0.899133**	**0.995933**	**6.7868**	**6.756467**	**0.997588**	**0.998109**	**0.033141**
R	5.6149	2.3696	40.6374	0.8927	0.9936	6.2302	6.2105	0.997594	0.996486	0.049885
G	5.4442	2.3333	40.7715	0.9232	0.9973	6.8025	6.7489	0.993314	0.999668	0.007585

B	5.1801	2.276	40.9875	0.9255	0.998	6.8519	6.8106	0.993309	0.999684	0.007304
Avg.	**5.413067**	**2.3263**	**40.7988**	**0.9138**	**0.9963**	**6.6282**	**6.59**	**0.994739**	**0.998613**	**0.021591**
R	5.2884	2.2997	40.8976	0.9196	0.9953	6.3176	6.2682	0.98324	0.999677	0.006967
G	5.4381	2.332	40.7763	0.9822	0.9973	7.2688	7.2543	0.995336	0.999562	0.013199
B	5.4381	2.332	40.7763	0.9822	0.9973	7.2688	7.2543	0.995336	0.999562	0.013199
Avg.	**5.3882**	**2.321233**	**40.81673**	**0.961333**	**0.996633**	**6.951733333**	**6.9256**	**0.991304**	**0.9996**	**0.011122**

Table 3.5 (b): Objective Analysis of the GHO Algorithm (For Color Images)

Planes	MSE	RMSE	PSNR	SSIM	CC	Input Entropy	Output Entropy	UIQ	IF	NAE
	1-bit									
R	0.2378	0.4876	54.3692	0.9961	1	7.5234	7.51	1	0.999985	0.001476
G	0.249	0.499	54.1693	0.9961	0.9999	7.7136	7.7117	1	0.999985	0.001738
B	0.2735	0.523	53.7614	0.9925	1	4.6229	4.5464	0.999938	0.999982	0.004036
Avg.	**0.253433**	**0.5032**	**54.09997**	**0.9949**	**0.999967**	**6.619967**	**6.589367**	**0.999979**	**0.999984**	**0.002417**
R	0.2486	0.4986	54.1766	0.9951	0.9999	7.2751	7.274	1	0.999967	0.003276
G	0.252	0.502	54.116	0.9944	0.9999	7.0415	7.0404	1	0.999944	0.00479
B	0.2527	0.5027	54.1053	0.9945	0.9998	6.8845	6.8834	1	0.99993	0.005444
Avg.	**0.2511**	**0.5011**	**54.13263**	**0.994667**	**0.999867**	**7.067033**	**7.065933**	**1**	**0.999947**	**0.004503**
R	0.2579	0.5079	54.0158	0.9944	0.9998	5.3323	5.3119	1	0.999984	0.001439
G	0.2479	0.4979	54.1879	0.9943	0.9999	5.7505	5.7424	1	0.999985	0.001372
B	0.2484	0.4984	54.1787	0.9942	0.9999	6.6128	6.5953	1	0.999985	0.001743
Avg.	**0.2514**	**0.5014**	**54.12747**	**0.9943**	**0.999867**	**5.898533**	**5.8832**	**1**	**0.999985**	**0.001518**
R	0.2536	0.5036	54.089	0.9992	0.9999	7.2597	7.2543	0.999331	0.99998	0.002484
G	0.251	0.501	54.1344	0.999	0.9996	6.6599	6.6593	1	0.999985	0.001775
B	0.2507	0.5007	54.1386	0.9987	0.999	6.0461	6.0453	1	0.999985	0.001424
Avg.	**0.251767**	**0.501767**	**54.12067**	**0.998967**	**0.9995**	**6.655233**	**6.652967**	**0.999777**	**0.999983**	**0.001895**
R	0.2382	0.488	54.3619	0.9961	1	7.5234	7.51	1	0.999985	0.001479
G	0.2495	0.4995	54.1594	0.9961	0.9999	7.7137	7.7117	0.999725	0.999985	0.001742
B	0.2747	0.5241	53.7419	0.9925	1	4.6228	4.5464	0.999938	0.999982	0.004054
Avg.	**0.254133**	**0.503867**	**54.08773**	**0.9949**	**0.999967**	**6.619967**	**6.589367**	**0.999888**	**0.999984**	**0.002425**
	2-bit									
R	1.239	1.1131	47.2	0.9752	0.9997	7.0943	7.0807	0.999096	0.999924	0.003517
G	1.3538	1.1635	46.8154	0.9687	0.9996	7.0322	6.9771	0.999811	0.999842	0.009457
B	1.2442	1.1154	47.1819	0.9754	0.9994	6.2278	6.2126	1	0.999855	0.007777
Avg.	**1.279**	**1.130667**	**47.06577**	**0.9731**	**0.999567**	**6.784767**	**6.7568**	**0.999636**	**0.999874**	**0.006917**

R	1.2431	1.1149	47.1858	0.9788	0.9994	7.3849	7.3817	0.998833	0.999924	0.004308
G	1.2951	1.138	47.0077	0.9769	0.9998	7.6611	7.6493	0.999796	0.999921	0.005668
B	1.317	1.1476	46.9351	0.9752	0.9993	7.1938	7.1613	0.999551	0.999784	0.010016
Avg.	**1.285067**	**1.1335**	**47.04287**	**0.976967**	**0.9995**	**7.413267**	**7.397433**	**0.999393**	**0.999876**	**0.006664**
R	1.2449	1.1158	47.1793	0.9751	0.9997	7.0941	7.0807	0.999096	0.999924	0.00353
G	1.3599	1.1662	46.7956	0.9687	0.9996	7.0323	6.9771	0.999811	0.999841	0.009496
B	1.2481	1.1172	47.1685	0.9754	0.9994	6.2278	6.2126	1	0.999854	0.007809
Avg.	**1.2843**	**1.133067**	**47.0478**	**0.973067**	**0.999567**	**6.784733**	**6.7568**	**0.999636**	**0.999873**	**0.006945**
R	1.2531	1.1194	47.1509	0.9751	0.9997	7.0942	7.0807	0.999096	0.999924	0.003542
G	1.3634	1.1676	46.7846	0.9688	0.9996	7.0322	6.9771	0.999811	0.999841	0.009504
B	1.2523	1.1191	47.1537	0.9754	0.9994	6.2278	6.2126	1	0.999854	0.007829
Avg.	**1.2896**	**1.135367**	**47.02973**	**0.9731**	**0.999567**	**6.784733**	**6.7568**	**0.999636**	**0.999873**	**0.006959**
R	1.2763	1.1298	47.0711	0.9957	0.9994	7.2638	7.2543	0.998663	0.999897	0.006228
G	1.2495	1.1178	47.1635	0.995	0.9982	6.6616	6.6593	0.996516	0.999924	0.004426
B	1.2476	1.117	47.1699	0.9934	0.9952	6.0492	6.0453	0.995885	0.999924	0.003547
Avg.	**1.2578**	**1.121533**	**47.13483**	**0.9947**	**0.9976**	**6.6582**	**6.652967**	**0.997021**	**0.999915**	**0.004734**
	3-bit									
R	5.5602	2.358	40.6799	0.8933	0.9936	6.2302	6.2105	0.99599	0.99652	0.049553
G	5.2954	2.3012	40.8918	0.9126	0.9972	7.2867	7.274	0.998277	0.999305	0.017474
B	5.5229	2.3501	40.7092	0.8966	0.997	7.0537	7.0404	0.998255	0.998785	0.026007
Avg.	**5.4595**	**2.336433**	**40.7603**	**0.900833**	**0.995933**	**6.856867**	**6.841633**	**0.997508**	**0.998203**	**0.031011**
R	5.5127	2.3479	40.7171	0.8986	0.9964	6.8988	6.8834	0.997705	0.998479	0.029366
G	5.2269	2.2862	40.9484	0.9723	0.9983	7.7395	7.7356	0.998792	0.999681	0.00948
B	5.2551	2.2924	40.925	0.9721	0.9975	7.4538	7.4485	0.99756	0.999679	0.01021
Avg.	**5.331567**	**2.308833**	**40.8635**	**0.947667**	**0.9974**	**7.364033**	**7.355833**	**0.998019**	**0.99928**	**0.016352**
R	5.2748	2.2967	40.9087	0.975	0.9985	7.769	7.7614	0.998595	0.999678	0.011605
G	5.2327	2.2875	40.9436	0.9481	0.9972	7.3268	7.3166	0.99756	0.999681	0.009988
B	5.2855	2.299	40.8999	0.9503	0.9991	7.6677	7.6443	0.999149	0.999677	0.010567
Avg.	**5.264333**	**2.2944**	**40.9174**	**0.9578**	**0.998267**	**7.587833**	**7.5741**	**0.998435**	**0.999679**	**0.01072**
R	5.1507	2.2695	41.0122	0.9484	0.9991	7.3255	7.303	0.999191	0.999686	0.011275
G	5.3062	2.3035	40.8829	0.9018	0.996	6.7885	6.7692	0.997549	0.998261	0.031616

B	5.7354	2.3949	40.5451	0.8848	0.9946	6.3592	6.3389	0.997909	0.996965	0.046711
Avg.	**5.397433**	**2.322633**	**40.8134**	**0.911667**	**0.996567**	**6.8244**	**6.8037**	**0.998216**	**0.998304**	**0.029867**
R	5.5993	2.3663	40.6494	0.8928	0.9936	6.2303	6.2105	0.997594	0.996496	0.049814
G	5.3019	2.3026	40.8865	0.9124	0.9972	7.2864	7.274	0.998277	0.999304	0.01749
B	5.5535	2.3566	40.6851	0.8962	0.997	7.0536	7.0404	0.998255	0.998778	0.026104
Avg.	**5.4849**	**2.341833**	**40.74033**	**0.900467**	**0.995933**	**6.856767**	**6.841633**	**0.998042**	**0.998193**	**0.031136**

Table 3.6 shows the selected cover image (CI), block index (BI), and secret data index (SDI) for grey-scale and color images. The result shows that the index values are not fixed for different secret data. Thus, it is not easy to recover secret data without this index information.

Table 3.6 (a): Cover Index, Block Index, and Secret Data Index for EVO/GHO Algorithms (for Grey Scale Images)

	EVO			**GHO**		
Secret Data	**Cover Image Index**	**Block Index**	**Secret Data Index**	**Cover Image Index**	**Block Index**	**Secret Data Index**
1-bit				**1-bit**		
1	15	3	2	15	4	0
2	13	1	2	13	4	0
3	5	4	1	5	1	2
4	11	3	1	11	1	1
5	14	2	0	14	3	2
2-bit				**2-bit**		
1	11	3	3	11	2	2
2	12	2	3	12	3	1
3	15	4	1	15	4	2
4	11	1	3	11	1	1
5	8	2	0	8	2	1
3-bit				**3-bit**		
1	12	2	1	12	1	1
2	13	1	3	13	2	1
3	7	1	0	7	4	1
4	11	3	3	11	4	1
5	6	1	3	6	2	1

Table 3.6 (b): Cover Index, Block Index, and Secret Data Index for EVO/GHO Algorithms (for Color Images)

	EVO									**GHO**								
Secret Data	**Cover Image Index**			**Block Index**			**Secret Data Index**			**Cover Image Index**			**Block Index**			**Secret Data Index**		
	R	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**
1-bit										**1-bit**								
1	15	15	15	3	4	3	2	0	0	15	15	15	3	4	3	2	0	0
2	13	13	13	1	4	2	2	0	3	13	13	13	1	4	2	2	0	3
3	5	5	5	4	1	2	1	2	3	5	5	5	4	1	2	1	2	3
4	11	11	11	3	1	2	1	1	2	11	11	11	3	1	2	1	1	2
5	14	14	14	2	3	4	0	2	0	14	14	14	2	3	4	0	2	0
2-bit										**2-bit**								
1	11	11	11	3	2	1	3	2	2	11	11	11	3	2	1	3	2	2
2	12	12	12	2	3	4	3	1	2	12	12	12	2	3	4	3	1	2
3	15	15	15	4	4	4	1	2	0	15	15	15	4	4	4	1	2	0
4	11	11	11	1	1	3	3	1	2	11	11	11	1	1	3	3	1	2
5	8	8	8	2	2	3	0	1	0	8	8	8	2	2	3	0	1	0
3-bit										**3-bit**								
1	12	12	12	2	1	4	1	1	1	12	12	12	2	1	4	1	1	1
2	13	13	13	1	2	1	3	1	3	13	13	13	1	2	1	3	1	3
3	7	7	7	1	4	2	0	1	0	7	7	7	1	4	2	0	1	0
4	11	11	11	3	4	2	3	1	2	11	11	11	3	4	2	3	1	2
5	6	6	6	1	2	2	3	1	0	6	6	6	1	2	2	3	1	0

- **Embedding Capacity Vs. PSNR**

In image steganography, the MSE and PSNR parameters depend on how much data is embedded in the cover image. In the proposed model, we have shown the simulation results for the maximum embedding possible for the cover image. For example, we have taken an image of resolution 256×256. Therefore, maximum 65536 bits embedding is possible in the cover image using the single-bit LSB method. In the literature, the researchers have achieved a better PSNR for these types of images when embedding capacity is less than the cover image. Further, to show how MSE and PSNR depend on embedding capacity, we have shown results

for different data embeddings in the cover image. Table 3.7 shows the MSE and PSNR for single and multi-bit methods for different data embeddings (1000 bits to 262144 bits). The result shows that in the single-bit method, the PSNR varies from 78.9516 to 54.2324 dB, whereas for the multi-bit method, it is 71.7662-47.3024 dB and 66.1368-41.2109 dB, respectively. This reflects that less data embedding in the cover image generates less distortion and a high PSNR value.

Table 3.7: MSE and PSNR for Different Data Embedding

Embedding Capacity (in bits)	1000	10000	50000	100000	200000	262144
1bit						
MSE	0.00082779	0.0089	0.0466	0.0930	0.1873	0.2454
PSNR (in dB)	78.9516	68.6278	61.4437	58.4437	55.4044	54.2324
2-bit						
MSE	0.0043	0.0442	0.2206	0.4575	0.9128	1.2102
PSNR (in dB)	71.7662	61.6746	54.6938	51.5267	48.5269	47.3024
3-bit						
MSE	0.0158	0.1878	0.8977	1.7077	3.5882	4.9203
PSNR (in dB)	66.1368	55.3936	48.5993	45.8066	42.5821	41.2109

- **Comparative Analysis**

Table 3.8 (a-c) shows the comparative analysis of the proposed method with the existing and recent bio-inspired optimized data hiding method proposed by researchers for same cover and secret data size. The result shows that the proposed method achiever better PSNR over the existing recent methods proposed by [56, 59-60] for *k*-bit LSB method.

Table 3.8 (a): Comparison of Proposed and Existing Algorithms [56] in terms of PSNR (in dB)

Images	**Simple LSB**	**PSO**	**ABC**	**Proposed Method**
Lena	44.4300	45.1900	56.40	57.22
Jet	44.2700	45.3800	56.39	57.24
Lake	44.1700	45.6700	56.40	57.21
Elaine	44.2400	45.9300	56.36	57.20
Baboon	44.3100	44.3100	56.39	57.21
Average	**44.284**	**45.296**	**56.39**	**57.22**

Table 3.8 (b): Comparison of Proposed and Existing Algorithms [59] in terms of PSNR (in dB)

Images	P. D. Shah and R. S. Bichkar [59]			Proposed Method		
	1-bit	2-bit	3-bit	1-bit	2-bit	3-bit
Living Room	52.17	-	-	54.23	47.30	41.21
Pirates	52.41	-	40.82	54.21	47.31	41.21
Airplane	52.21	46.37	-	54.24	47.29	41.22
Boat	52.35	-	-	54.22	47.30	41.20
Mandrill	52.13	46.42	-	54.22	47.29	41.20
Lake	-	46.42	-	54.23	47.30	41.21
Pepper	-	46.39	-	54.21	47.31	41.21
Lena		46.43	40.75	54.24	47.29	41.22
Blonde	-	-	40.91	54.22	47.30	41.20
Cameraman	-	-	40.82	54.22	47.29	41.20

Table 3.8 (c): Comparison of Proposed and Existing Algorithms [60] in terms of PSNR (in dB)

Images	Hameed et al. [60]		Proposed Method	
	2-bit	3-bit	2-bit	3-bit
Image1	44.3589	39.8798	47.3024	41.2109
Image2	44.3083	39.8404	47.3103	41.2053
Image3	44.5281	39.9505	47.2893	41.2178
Image4	44.4704	39.9159	47.2965	41.1995
Image5	45.3950	41.1958	47.2920	41.2043
Image6	44.6054	39.9975	47.3024	41.2109

- **Intentional/Non-Intentional Attacks**

In this section, we have applied the international/non-intentional attacks on the proposed method and evaluate its performance using two performance metrics, such as SF and BER. The result shows tha the proposed method achieves the high value of SF and BER because a small change in the pixel values of the stego image is difficult to recover the original secret data.

Table 3.9: Performance Metrics for different Intentional/Non-Intentional Attacks on the Proposed Method

Attacks		Salt and Pepper (D=0.001)	Gaussian Attack (V=0.001)	Rotate	Low Pass Filtering
		1-bit			
Image1	SF	184	184	177	183
	BER	13.3270	5.9585e+03	7.5324e+03	2.2487e+03
Image2	SF	184	184	177	183
	BER	13.9221	5.9995e+03	7.5324e+03	2.2487e+03
Image3	SF	184	184	177	183
	BER	11.6669	5.9678e+03	7.5324e+03	2.2487e+03
		2-bit			
Image1	SF	63	61	31	58
	BER	16.4917	3.4014e+03	4.6982e+03	2.2884e+03
Image2	SF	63	61	31	58
	BER	10.5286	3.4156e+03	4.6982e+03	2.2884e+03
Image3	SF	63	61	31	58
	BER	9.5337	3.4259e+03	4.6982e+03	2.2884e+03
		3-bit			
Image1	SSIM	63	60	29	57
	BER	11.0718	3.2220e+03	4.4995e+03	2.0993e+03
Image2	SSIM	63	60	29	57
	BER	7.1533	3.2426e+03	4.4995e+03	2.0993e+03
Image3	SSIM	63	60	29	57
	BER	15.0879	3.2388e+03	4.4995e+03	2.0993e+03

3.4 Data Matching Method & Hiding the Matched Index in an Optimal Way

The main motive of the matching method is to match the secret data bits with the cover image LSB bits and determine the matched index. After that, the hiding of the matched index is performed in the same cover image. In the literature, in [58], the authors split the secret data bits into 2-bit chunks, and each chunk is matched with a cover image pixel. They have worked on grayscale images. Therefore, the image pixel is 8 bits long; thus, the optimally matched index value varies from 0-7. Besides that, if the matching is not found with the cover image pixels, then data hiding is performed in the LSB of the cover image pixel, and the '0' index is defined. After that, the matched index is hidden in the cover image using the genetic algorithm. The advantage of their method is that the secret data extraction is not possible until a matching index is known. On the other hand, the disadvantage of their method is the reduced embedding capacity because the matched index varies from 0-7. Thus, one quarter of the cover image is used for matching purposes, whereas the remaining part of the cover image is used for hiding the matched index. Further, in [61], the authors have matched the complemented or non-complemented form of the secret data with the LSB 2-bits of the cover image pixels and determined the matched index. After that, they have hidden the matched index in the same cover image using the 2-bit LSB algorithm. The advantage of their method is that the complemented or non-complemented form of the secret data always matches with the LSB bits of the cover image pixel. Thus, half of the cover image has zero variability. Further, the embedding capacity of their method is superior to Shah et al. [58] because the matched index value varies from 0 to 3. On the other hand, the disadvantage of their method is that the matched index is hidden in the cover image using the conventional LSB algorithm, which generates variability. Next, in [62], we designed a matching method in which the cover image is split into two parts based on the edges and named the smooth region and the edge region. The smooth region pixels of the cover image are matched with secret data bits, and matched indexes are determined. The matched index was then hidden in the edge region using the LSB algorithm. The limitation of their method is that the reference cover image needs to communicate with the receiver, and embedding capacity is dependent on how many edges are available in the cover image for hiding matched indexes. These challenges are taken into consideration in the proposed method.

In the proposed method, the secret data bits are matched with cover image pixel LSB bits, and a matched index is determined. Further, if the bits are not matched, they are hidden in the LSB

of the cover image pixel, and the matched index is set to 0. After that, the matched index is hidden in the same cover image in the optimal way using the 2-bit LSB method by determining the optimal starting pixel index in the cover image. The secret data bits are split into 2-bit chunks, and matching is performed in the LSB 4-bits of the cover image pixel. As a result, the matched index ranges from 0 to 3. Next, how the optimal starting pixel index is determined in the cover image is explained below.

Cover images are available in matrix format, which scans the entire image from first to last pixel to hide data. However, if the scanning process is started from any other pixel in place of the first pixel, then it gives a different stego image in the output. Thus, in this approach, the main motive is to scan the optimal starting pixel index in the cover image to hide the secret data in order to enhance the imperceptibility of the stego image. The data embedding and data extraction process for this approach is given below.

3.4.1 Data Embedding and Extraction for the Data Matching Method

The flowchart of the data embedding process of the proposed matching method is shown in Figure 3.6.

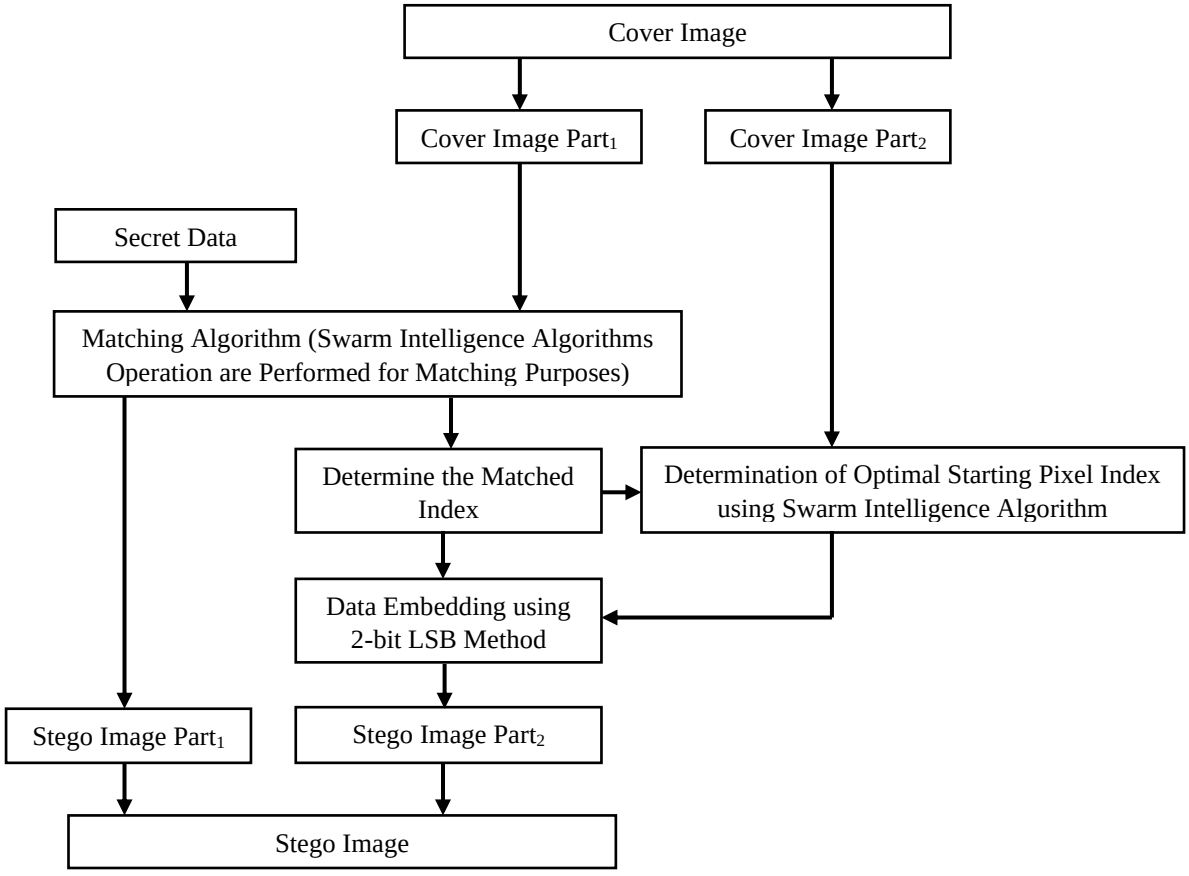


Figure 3.6: Flowchart of Data Embedding in Matching Method

Initially, the cover image is read and split into two parts (cover image $Part_1$ and cover image $Part_2$). The secret data, along with cover image $Part_1$ is given to the matching algorithm. The matching algorithm performs swarm intelligence algorithm operations (such as hitting with a pebble, rolling with twigs, and changing angles in the EVO algorithm, whereas steps such as baiting, changing angles, and attracting a prey swarm in the Green Heron optimization algorithm) and returns the stego image Part1 and matched index in the output.

The swarm intelligence algorithm operations give an LSB index value. Based on this index value, the secret data bits are matched with the LSB bits of the cover image. For example, in the EVO algorithm, the hit with pebble operation index is randomly generated in the LSB 4-bit range. After that, according to the index value, those LSB bits are matched with secret data bits. If the matching is successful, the matched index is determined; otherwise, the remaining operations (rolling with twigs and changing the angle) are performed to generate other index values for matching purposes. This same operation is performed for the GHO algorithm.

Before the matched index is hidden in the cover image $Part_2$, the matched index along with cover image $Part_2$ is given to the swarm intelligence algorithm. In Part 2, the swarm intelligence algorithm determines the best starting pixel index. After determining the optimal starting pixel index in the cover image, the matched index is hidden in the cover image $Part_2$ using a 2-bit LSB algorithm that gives the stego image $Part_2$ in the output. Further, stego image parts ($Part_1$ and $Part_2$) are concatenated to get the stego image in the output. The stego image and optimal starting pixel index are communicated to the receiver for data extraction. The mathematical model for data embedding for the data matching method is given below.

- **For determine the Matched Index**

$$M_i = Cmod2^n \ll i \qquad i = 0-3, n = 2-5 \tag{3.5}$$

$$OP = \begin{cases} i & If\ M_i == D \\ 0 & If\ M_i \approx D \end{cases} \tag{3.6}$$

- **Data Embedding**

$If\ OP == 0$

$$S = C - Cmod2^n + d \qquad \text{n=2} \tag{3.7}$$

$If\ OP == \{1-3\}$

$$T_i = Cmod2^n \ll i \qquad \text{n=3-5 i=1-3} \tag{3.8}$$

$$T1_i = T_i + d \gg i \tag{3.9}$$

$$S = T1_i + Cmod2^n \qquad \text{n=1-3} \tag{3.10}$$

Further, the steps taken to determine the optimal starting pixel index using the swarm intelligence algorithm are given below.

- In step 1, The population, iterations, the objective function, the lower and upper limits of the starting pixel index, and the objective function's operations (hitting with a pebble, rolling with twigs, and changing angles in EVO; baiting, changing positions, and attracting a prey swarm in GHO) are all initialized. MSE is used as an objective function in this work.
- In step 2, the initial population array is randomly initialized at the lower and upper limits of the starting pixel index.
- In step 3, the fitness evaluation of each population is accomplished using an objective function to determine the population that gives the minimum MSE.
- In step 4, next, random population is chosen from the population array, and the first operation of the EVO/GHO algorithm is performed on it to generate a new population, which gives another starting pixel index. In the EVO, the first operation is a pebble hit, whereas in the GHO, the first operation is baiting in the random position. The fitness evaluation of the generated population is accomplished using an objective function. Further, it is compared with the finest population, which was determined in the previous step. If the generated population is better, then the finest population is updated; otherwise, remaining operations are performed one after another only when the previous operation's generated population is not giving superior results over the finest population. In EVO algorithms, the remaining operations are rolling with twigs and changing angles, whereas in GHO algorithms, it is changing position and attracting a prey swarm.
- Step 4 is iterated for a fixed number of iterations, and the optimal starting pixel index is determined.

The flowchart of the data extraction for the matching method is shown in Figure 3.7. Initially, the stego image is read and split into two parts (stego image $Part_1$ and stego image $Part_2$). The stego image $Part_2$ is given to the 2-bit LSB data extraction algorithm along with information about the starting pixel index. The extraction algorithm extracts the LSB 2-bits from the

optimal starting pixel index and returns the matched index. Based on this information, the secret data bits are extracted from the stego image $Part_1$ using the data extraction method.

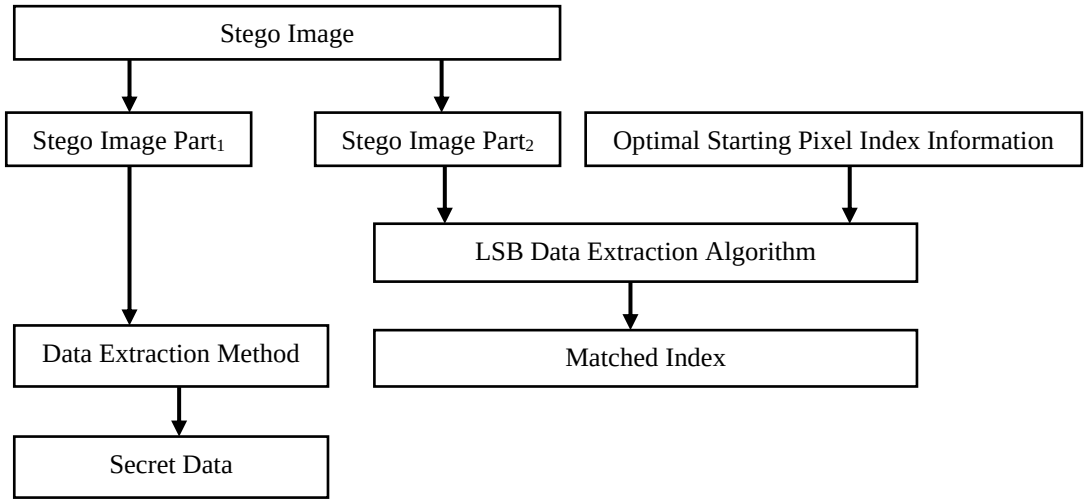


Figure 3.7: Block Diagram of Data Extraction for Matching Method

3.4.2 Results and Analysis for the Data Matching Method

The simulation evaluation of the EVO/GHO algorithm is shown for the matching method and compared with the existing methods in this section. The images are taken under consideration are Lena, Baboon, Barbara, Pepper, Boat, Cameraman, Airplane, Female, couple, house. The initial parameter value of the EVO/GHO algorithm for match the secret data bits and to determine the optimal starting pixel index is given in Table 3.10.

Table 3.10: Initial Parameter Values of the EVO/GHO Algorithm for Matching Method

Parameter	Values	Parameter	Value
Population	50	Starting Pixel Index Range	[1-N]
Iterations	30	Matching Positions in the Cover Image	LSB 4-bit
Objective Function	MSE	Data Hiding Method	2-bit LSB

Note: N denotes the total row and columns in Cover Image $Part_2$

- **Subjective Analysis**

Table 3.11 (a-b)-3.12 (a-b) shows the subjective analysis of the matching method for the grey-scale and color images. In this analysis, original cover image and stego image are compared. The result shows that the images look indistinguishable for EVO/GHO algorithm.

Table 3.11 (a): Subjective Analysis of the Matching Method for EVO/GHO Algorithm (for Grey-Scale Image)

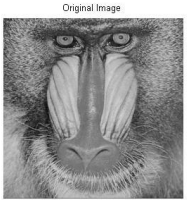
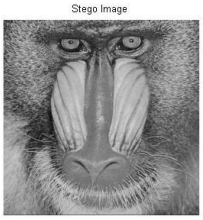
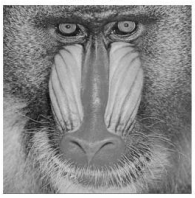
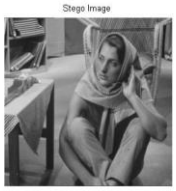
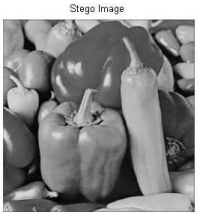
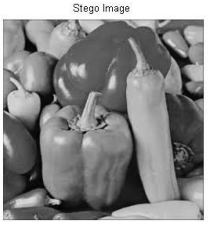
Images	**Cover Image**	**EVO Algorithm**	**GHO Algorithm**
		Stego Image	**Stego Image**
Lena			
Baboon			
Barbara			
Pepper			
Boat			

Table 3.11 (b): Subjective Analysis of the Matching Method for EVO/GHO Algorithm (for Grey-Scale Image)

Images	**Cover Image**	**EVO Algorithm**	**GHO Algorithm**
		Stego Image	**Stego Image**
Camera man			
Airplane			
Female			
Couple			
House			

Table 3.12 (a): Subjective Analysis of the Matching Method for EVO/GHO Algorithm (for Color Images)

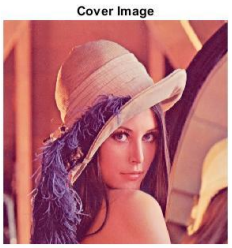
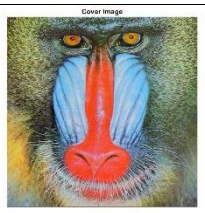
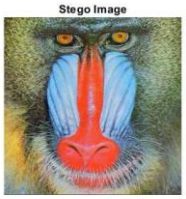
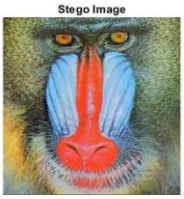
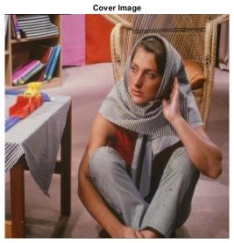
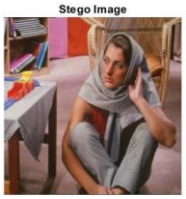
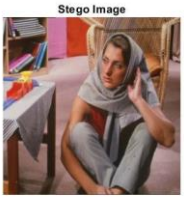
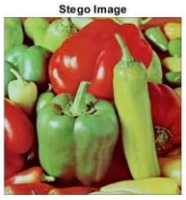
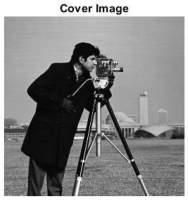
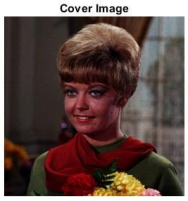
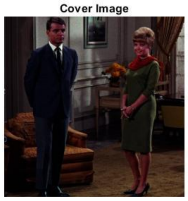
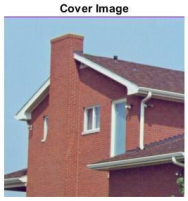
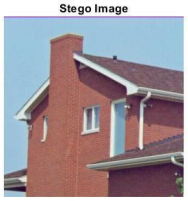
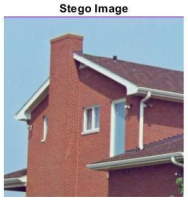
Images	Cover Image	EVO Algorithm	GHO Algorithm
		Stego Image	Stego Image
Lena			
Baboon			
Barbara			
Pepper			
Boat			

Table 3.12 (b): Subjective Analysis of the Matching Method for EVO/GHO Algorithm (for Color Images Image)

Images	**Cover Image**	**EVO Algorithm**	**GHO Algorithm**
		Stego Image	**Stego Image**
Camera man			
Airplane			
Female			
Couple			
House			

- **Objective Analysis**

Table 3.13-3.14 shows the objective analysis of the matching method based on the various parameter for grey-scale and color images. The parameters are taken under consideration are MSE, RMSE, PSNR, SSIM, CC, entropy, UIQ, IF, and NAE. The result shows that the correlation coefficient, SSIM, IF, and UIQI values are near 1. Further, PSNR of the proposed method is achieved near 50 dB. Finally, the entropy value of the output stego image is a little bit varied over the input cover image due to data hiding in the same cover image using the 2-bit LSB method.

Table 3.13(a): Objective Analysis of the Matching Method for EVO Algorithm (for Grey-Scale Images)

Image	CC	SSIM	Input Entropy	Output Entropy	MSE	RMSE	PSNR	IF	NAE	UIQI
Lena	0.9998	0.9923	7.2469	7.2292	0.5918	0.7693	50.4087	0.999983	0.001509	0.999437
Baboon	0.9998	0.9978	7.6439	7.6261	0.5681	0.7537	50.5869	0.999974	0.001901	0.999679
Barbara	0.9998	0.9957	7.5518	7.5313	0.5629	0.7502	50.6269	0.999973	0.001937	1.000000
Pepper	0.9997	0.9947	7.3789	7.3606	0.5754	0.7586	50.5309	0.999975	0.001834	0.999379
Boat	0.9998	0.9948	7.1766	7.1570	0.5465	0.7393	50.7546	0.999971	0.001952	0.999276
Cameraman	0.9999	0.9895	7.0911	7.0729	0.5509	0.7423	50.7197	0.999969	0.002146	1.000000
Airplane	0.9997	0.992	6.7421	6.7232	0.5581	0.7471	50.6636	0.999983	0.001459	0.999005
Female	0.9997	0.9927	7.2761	7.2607	0.5551	0.7451	50.6869	0.999927	0.003366	1.000429
Couple	0.9996	0.9934	6.7693	6.7583	0.5412	0.7356	50.7975	0.999823	0.005984	0.999391
House	0.9995	0.9917	6.4005	6.3835	0.7125	0.8441	49.6029	0.999968	0.002201	0.998693

Table 3.13(b): Objective Analysis of the Matching Method for EVO Algorithm (for Color Images)

Image	Plane	CC	SSIM	Input Entropy	Output Entropy	MSE	RMSE	PSNR	IF	NAE	UIQI
Lena	R	0.9998	0.9923	7.2469	7.2292	0.5918	0.7693	50.4087	0.99998	0.001509	0.99943
	G	0.9998	0.9932	7.5733	7.5514	0.5911	0.7688	50.4143	0.99995	0.002739	0.99966
	B	0.9995	0.9919	6.9403	6.9181	0.6016	0.7756	50.3380	0.99995	0.002616	0.99853
	Avg.	**0.9997**	**0.9925**	**7.2535**	**7.2329**	**0.5948**	**0.7712**	**50.3870**	**0.99996**	**0.002288**	**0.99921**
Baboon	R	0.9998	0.9978	7.6439	7.6261	0.5681	0.7537	50.5869	0.99997	0.001901	0.99968
	G	0.9997	0.9976	7.3529	7.3363	0.5655	0.752	50.6063	0.99997	0.002031	1
	B	0.9999	0.9979	7.6786	7.66	0.5543	0.7445	50.6934	0.99997	0.002257	0.99975
	Avg.	**0.9998**	**0.997767**	**7.558467**	**7.5408**	**0.562633**	**0.750067**	**50.62887**	**0.99997**	**0.002063**	**0.99981**
Barbara	R	0.9998	0.9957	7.5518	7.5313	0.5629	0.7502	50.6269	0.99997	0.001937	1
	G	0.9997	0.9958	7.3756	7.3548	0.5923	0.7696	50.4053	0.99995	0.002671	1
	B	0.9998	0.9957	7.4773	7.4535	0.6012	0.7754	50.3403	0.99995	0.002953	1
	Avg.	**0.999767**	**0.995733**	**7.468233**	**7.446533**	**0.585467**	**0.765067**	**50.4575**	**0.99996**	**0.00252**	**1**
Pepper	R	0.9997	0.9947	7.3789	7.3606	0.5754	0.7586	50.5309	0.99998	0.001834	0.99938
	G	0.9999	0.9949	7.6462	7.6293	0.5578	0.7468	50.6663	0.99997	0.002268	1
	B	0.9997	0.9951	7.162	7.1613	0.5335	0.7304	50.8595	0.99991	0.003819	1
	Avg.	**0.999767**	**0.9949**	**7.3957**	**7.383733**	**0.555567**	**0.745267**	**50.68557**	**0.99995**	**0.00264**	**0.99979**
Boat	R	0.9998	0.9948	7.1766	7.157	0.5465	0.7393	50.7546	0.99997	0.001952	0.99928

	G	0.9998	0.9947	7.1766	7.1571	0.5523	0.7432	50.709	0.999971	0.001975	0.99928
	B	0.9998	0.9948	7.1766	7.1569	0.5399	0.7347	50.808	0.999971	0.001923	0.99928
	Avg.	**0.9998**	**0.994767**	**7.1766**	**7.157**	**0.546233**	**0.739067**	**50.7572**	**0.999971**	**0.00195**	**0.99928**
Cameraman	R	0.9999	0.9895	7.0911	7.0729	0.5509	0.7423	50.7197	0.999969	0.002146	1
	G	0.9999	0.9896	7.0911	7.0734	0.5442	0.7377	50.7735	0.99997	0.002121	1
	B	0.9999	0.9894	7.0911	7.0741	0.5529	0.7436	50.704	0.999969	0.002149	1
	Avg.	**0.9999**	**0.9895**	**7.0911**	**7.073467**	**0.549333**	**0.7412**	**50.7324**	**0.999969**	**0.002139**	**1**
Airplane	R	0.9997	0.992	6.7421	6.7232	0.5581	0.7471	50.6636	0.999983	0.001459	0.99900
	G	0.9998	0.9921	6.8249	6.8054	0.552	0.743	50.7115	0.999984	0.00143	0.99924
	B	0.9995	0.9909	6.2475	6.2262	0.5372	0.7329	50.8297	0.999986	0.001305	0.99801
	Avg.	**0.999667**	**0.991667**	**6.604833**	**6.584933**	**0.5491**	**0.741**	**50.73493**	**0.999984**	**0.001398**	**0.99875**
Female	R	0.9997	0.9927	7.2761	7.2607	0.5551	0.7451	50.6869	0.999927	0.003366	1.00043
	G	0.9997	0.9922	7.0377	7.015	0.5546	0.7447	50.6913	0.999878	0.004855	0.99957
	B	0.9997	0.9924	6.8786	6.8604	0.552	0.743	50.711	0.999847	0.005507	0.99949
	Avg.	**0.9997**	**0.992433**	**7.064133**	**7.045367**	**0.5539**	**0.744267**	**50.6964**	**0.999884**	**0.004576**	**0.99983**
Couple	R	0.9996	0.9934	6.7693	6.7583	0.5412	0.7356	50.7975	0.999823	0.005984	0.99939
	G	0.9995	0.993	6.3381	6.3192	0.5367	0.7326	50.8338	0.999716	0.008327	1
	B	0.9994	0.9931	6.2083	6.1905	0.5675	0.7533	50.5912	0.999645	0.009415	1
	Avg.	**0.9995**	**0.993167**	**6.438567**	**6.422667**	**0.548467**	**0.7405**	**50.74083**	**0.999728**	**0.007908**	**0.99980**
House	R	0.9995	0.9917	6.4005	6.3835	0.7125	0.8441	49.6029	0.999968	0.002201	0.99869

	G	0.9999	0.9929	6.5603	6.5853	0.3876	0.6226	52.2471	0.999981	0.001445	1
	B	0.9999	0.9906	6.4042	6.3971	0.868	0.9316	48.7459	0.999964	0.002818	0.99956
	Avg.	**0.999767**	**0.991733**	**6.455**	**6.4553**	**0.656033**	**0.799433**	**50.19863**	**0.999971**	**0.002155**	**0.99942**

Table 3.14 (a): Objective Analysis of the Matching Method for GHO Algorithm (for Grey-Scale Images)

Image	CC	SSIM	Input Entropy	Output Entropy	MSE	RMSE	PSNR	IF	NAE	UIQI
Lena	0.9998	0.9932	7.5733	7.5514	0.5911	0.7688	50.4143	0.999953	0.002739	0.999656
Baboon	0.9997	0.9976	7.3529	7.3363	0.5655	0.752	50.6063	0.999969	0.002031	1
Barbara	0.9997	0.9958	7.3756	7.3548	0.5923	0.7696	50.4053	0.999952	0.002671	1
Pepper	0.9999	0.9949	7.6462	7.6293	0.5578	0.7468	50.6663	0.999969	0.002268	1
Boat	0.9998	0.9947	7.1766	7.1571	0.5523	0.7432	50.709	0.999971	0.001975	0.999276
Cameraman	0.9999	0.9896	7.0911	7.0734	0.5442	0.7377	50.7735	0.99997	0.002121	1
Airplane	0.9998	0.9921	6.8249	6.8054	0.552	0.743	50.7115	0.999984	0.00143	0.999242
Female	0.9997	0.9922	7.0377	7.015	0.5546	0.7447	50.6913	0.999878	0.004855	0.999565
Couple	0.9995	0.993	6.3381	6.3192	0.5367	0.7326	50.8338	0.999716	0.008327	1
House	0.9999	0.9929	6.5603	6.5853	0.3876	0.6226	52.2471	0.999981	0.001445	1

Table 3.14 (b): Objective Analysis of the Matching Method for GHO Algorithm (for Color Images)

Image	Planes	CC	SSIM	Input Entropy	Output Entropy	MSE	RMSE	PSNR	IF	NAE	UIQI
Lena	R	0.9998	0.9923	7.2469	7.2292	0.5918	0.7693	50.4087	0.999983	0.001509	0.999437
	G	0.9998	0.9932	7.5733	7.5514	0.5911	0.7688	50.4143	0.999953	0.002739	0.999656
	B	0.9995	0.9919	6.9403	6.9181	0.6016	0.7756	50.338	0.999951	0.002616	0.998529
	Avg.	**0.9997**	**0.992467**	**7.2535**	**7.2329**	**0.594833**	**0.771233**	**50.387**	**0.999962**	**0.002288**	**0.999208**
Baboon	R	0.9998	0.9978	7.6439	7.6261	0.5681	0.7537	50.5869	0.999974	0.001901	0.999679
	G	0.9997	0.9976	7.3529	7.3363	0.5655	0.752	50.6063	0.999969	0.002031	1
	B	0.9999	0.9979	7.6786	7.66	0.5543	0.7445	50.6934	0.999966	0.002257	0.999752
	Avg.	**0.9998**	**0.997767**	**7.558467**	**7.5408**	**0.562633**	**0.750067**	**50.62887**	**0.99997**	**0.002063**	**0.99981**
Barbara	R	0.9998	0.9957	7.5518	7.5313	0.5629	0.7502	50.6269	0.999973	0.001937	1
	G	0.9997	0.9958	7.3756	7.3548	0.5923	0.7696	50.4053	0.999952	0.002671	1
	B	0.9998	0.9957	7.4773	7.4535	0.6012	0.7754	50.3403	0.999946	0.002953	1
	Avg.	**0.999767**	**0.995733**	**7.468233**	**7.446533**	**0.585467**	**0.765067**	**50.4575**	**0.999957**	**0.00252**	**1**
Pepper	R	0.9997	0.9947	7.3789	7.3606	0.5754	0.7586	50.5309	0.999975	0.001834	0.999379
	G	0.9999	0.9949	7.6462	7.6293	0.5578	0.7468	50.6663	0.999969	0.002268	1
	B	0.9997	0.9951	7.162	7.1613	0.5335	0.7304	50.8595	0.999913	0.003819	1
	Avg.	**0.999767**	**0.9949**	**7.3957**	**7.383733**	**0.555567**	**0.745267**	**50.68557**	**0.999952**	**0.00264**	**0.999793**
Boat	R	0.9998	0.9948	7.1766	7.157	0.5465	0.7393	50.7546	0.999971	0.001952	0.999276

	G	0.9998	0.9947	7.1766	7.1571	0.5523	0.7432	50.709	0.999971	0.001975	0.999276
	B	0.9998	0.9948	7.1766	7.1569	0.5399	0.7347	50.808	0.999971	0.001923	0.999276
	Avg.	**0.9998**	**0.994767**	**7.1766**	**7.157**	**0.546233**	**0.739067**	**50.7572**	**0.999971**	**0.00195**	**0.999276**
Cameraman	R	0.9999	0.9895	7.0911	7.0729	0.5509	0.7423	50.7197	0.999969	0.002146	1
	G	0.9999	0.9896	7.0911	7.0734	0.5442	0.7377	50.7735	0.99997	0.002121	1
	B	0.9999	0.9894	7.0911	7.0741	0.5529	0.7436	50.704	0.999969	0.002149	1
	Avg.	**0.9999**	**0.9895**	**7.0911**	**7.073467**	**0.549333**	**0.7412**	**50.7324**	**0.999969**	**0.002139**	**1**
Airplane	R	0.9997	0.992	6.7421	6.7232	0.5581	0.7471	50.6636	0.999983	0.001459	0.999005
	G	0.9998	0.9921	6.8249	6.8054	0.552	0.743	50.7115	0.999984	0.00143	0.999242
	B	0.9995	0.9909	6.2475	6.2262	0.5372	0.7329	50.8297	0.999986	0.001305	0.998012
	Avg.	**0.999667**	**0.991667**	**6.604833**	**6.584933**	**0.5491**	**0.741**	**50.73493**	**0.999984**	**0.001398**	**0.998753**
Female	R	0.9997	0.9927	7.2761	7.2607	0.5551	0.7451	50.6869	0.999927	0.003366	1.000429
	G	0.9997	0.9922	7.0377	7.015	0.5546	0.7447	50.6913	0.999878	0.004855	0.999565
	B	0.9997	0.9924	6.8786	6.8604	0.552	0.743	50.711	0.999847	0.005507	0.999493
	Avg.	**0.9997**	**0.992433**	**7.064133**	**7.045367**	**0.5539**	**0.744267**	**50.6964**	**0.999884**	**0.004576**	**0.999829**
Couple	R	0.9996	0.9934	6.7693	6.7583	0.5412	0.7356	50.7975	0.999823	0.005984	0.999391
	G	0.9995	0.993	6.3381	6.3192	0.5367	0.7326	50.8338	0.999716	0.008327	1
	B	0.9994	0.9931	6.2083	6.1905	0.5675	0.7533	50.5912	0.999645	0.009415	1
	Avg.	**0.9995**	**0.993167**	**6.438567**	**6.422667**	**0.548467**	**0.7405**	**50.74083**	**0.999728**	**0.007908**	**0.999797**
House	R	0.9995	0.9917	6.4005	6.3835	0.7125	0.8441	49.6029	0.999968	0.002201	0.998693
	G	0.9999	0.9929	6.5603	6.5853	0.3876	0.6226	52.2471	0.999981	0.001445	1

	B	0.9999	0.9906	6.4042	6.3971	0.868	0.9316	48.7459	0.999964	0.002818	0.999562
	Avg.	**0.999767**	**0.991733**	**6.455**	**6.4553**	**0.656033**	**0.799433**	**50.19863**	**0.999971**	**0.002155**	**0.999418**

- **Comparative Analysis**

Table 3.15 shows the comparative analysis of the proposed method with the existing matching method proposed by researchers. The result shows that the proposed method achiever approximate similar PSNR as compared to Kamil et al. [61] with same embedding capacity. On the other hand, low PSNR with double embedding capacity as compared to Shah et al. [58].

Table 3.15: Comparison of Proposed and Existing Algorithms in terms of PSNR (in dB)

		Images					
Methods		**Lena**	**Baboon**	**Barbara**	**House**	**Cameraman**	**Average**
LSB [58]		52.20	52.18	52.17	52.27	52.23	52.21
Shah et al. [58]		52.33	54.43	53.80	52.64	52.36	53.11
Kamil et al. [61]		50.1590	50.2133	50.1801	50.1701	50.180	50.1805
Proposed Method	**EVO**	50.1692	50.2241	50.1879	50.1806	50.1969	50.191
	GHO	50.1826	50.2455	50.1861	50.1506	50.1720	50.187

3.5 Conclusion

In this chapter, Egyptian Vulture optimization and Green Heron optimization algorithms are used to achieve optimized data hiding for image steganography. These optimization algorithms are used to design two approaches. In the first approach, these algorithms determine the optimal cover image index, block index, and secret data index whereas in the second approach, these algorithms determine the scanning order in the cover image for matching method. Further, the subjective and objective analysis are performed on the standard dataset images for evaluation purposes. From the result analysis, we found that the proposed method enhances the imperceptibility parameter without affecting the embedding capacity parameter.

Chapter 4

Image Steganography Method based on Evolutionary Algorithm

4.1 Introduction

Image steganography hides the secret data in the cover image using a data hiding algorithm such as the least significant bit (LSB) [2]. The data hiding process generates distortion in the output image, which negatively impacts the security parameter of steganography known as imperceptibility [2]. Thus, the central idea of the imperceptibility parameter of image steganography is that the output image that is obtained after hiding the data in the cover image should contain the least amount of distortion [80]. In order to reduce distortions, either the secret data bits are rearranged or the optimal scanning order in the cover image is determined before data hiding [51-58]. In the literature, the rearrangement of the secret data bits/cover image is done using the evolutionary algorithm because a huge number of rearrangement combinations of the secret data bits/cover image are possible and finding the optimal form is a difficult task. Evolutionary algorithms hide the secret data in the cover image by using the objective function to find the best way to organize the secret data and scan it in order.

Evolutionary algorithms, a class of the bio-inspired optimization algorithm, are based on the biological evolution process of living organisms [81-82]**.** It is a subfield of the bio-inspired algorithm. In the literature, genetic algorithms [83] and differential evolution [84] are the two most common evolutionary algorithms. Out of these, the genetic algorithm is the most preferred in image steganography to enhance the imperceptibility parameter [51-52,55,57-58]. The genetic algorithm performs initialization, selection, reproduction, and termination steps to find the optimal solution in the solution space [55]. The population is randomly initialized in the initialization step. Further, in the selection step, some of the population is chosen as a breed to generate population. In the reproduction step, crossover and mutation steps are performed on the selected population to generate new population. Based on the fitness of the population, new population is replaced with the initial population. In the termination step, the selection and reproduction steps are repeated until desired solution is found. Genetic algorithms, on the other

hand, have numerous limitations, such as the fact that the initial population is selected at random to generate new offspring in the reproduction step using crossover and mutation [85]. Thus, if the randomly selected population is not of good quality, superior offspring generation is not possible. Aside from that, each iteration only allows for a limited number of offspring generations. Thus, the exploration rate to find the optimal solution in the solution space is low. These challenges are taken into consideration when studying the other evolutionary algorithms.

In the recent year, a new evolutionary algorithm, named the "black widow optimization algorithm (BWO)," has gained popularity over the genetic algorithm due to a better exploration rate [79]. Therefore, it quickly searches for solutions. The BWO algorithm is based on the mating process of black widow spiders. The spiders can mate in parallel. Thus, it can generate a number of eggs known as "offspring." Further, it contains one cannibalism stage, in which inappropriate solutions are eliminated while exploring the solution space. Due to these two features of the BWO algorithm, this algorithm is chosen for the proposed image steganography method. In the literature, the BWO algorithm is successfully applied to 100 benchmark algorithms, and it provides superior results over the existing algorithms [79]. Further, the novelty of the proposed method is that, instead of searching the optimal secret data index, it searches the optimal secret data and cover image indexes. The cover image indexes define the chosen cover image as well as the best block order for it. On the other hand, the secret data index defines what operation was performed on the secret data, which gives the minimum variability. The rest of the chapter is organized in four sections. Section 4.2 explains the proposed image steganography method based on the BWO algorithm. Sections 4.3-4.4 shows the results, their analysis, and the conclusion.

4.2 Proposed Image Steganography Method based on Evolutionary Algorithm

The main motive of the proposed image steganography method is to employ the evolutionary BWO algorithm for finding the optimal index of secret data and a cover image before data embedding. The procreate step of the BWO algorithm generates a number of offspring, whereas the cannibalism step removes the inadequate solutions while exploring the solution space based on the objective function. These two features of the black widow optimization algorithm allow it to generate a number of combinations of optimal solutions and remove the inadequate combinations while exploring the solution space. Next, a detailed description of how the optimal secret data index and cover image index are determined is explained.

4.2.1 Secret Data Index

Secret data index is defined what operations are performed on the secret data to determine its optimal form. These operations are explained below.

- Flipping: In this operation, the secret data bits are flipped from 0's to 1's and vice versa.
- Swapping: In this operation, the secret data bit positions are swapped.
- Shifting: In this operation, the secret data bits are randomly circular shifted in order to match the secret data bits with cover image pixels.

4.2.2 Cover Image Index

Initially, the optimal cover image is selected from *n* number of images. Further, optimal block order index is determined for the optimal cover image. The detailed description of the cover image determination is given below.

- **Optimal Cover Image:** The optimal cover image selection from *n* number of images gives more chances to enhance the imperceptibility parameter. To achieve this goal, initially, *n* number of images are read, as shown in Figure 4.1. After that, based on the objective function, the optimal cover image is chosen that gives the minimum variability over other cover images. In the proposed method, mean square error (MSE) is used the objective function.

C_1	C_2	C_3	.....	C_n

Figure 4.1: *n* Number of Cover Images

- **Determination of Optimal Block Order for Selected Cover Image:** In this operation, the selected cover image is split into blocks, as shown in Figure 4.2 (a). After that, rearrangement of the block is done (as shown in Figure 4.2 (b)) to determine the optimal block order index that gives the minimum variability after data hiding. The determination of optimal block order index is done based on the objective function.

B_1	B_2	B_3
B_4	B_5	B_6
B_7	B_8	B_9

(a) Cover Image Blocks

B_1	B_2	B_8
B_3	B_4	B_6
B_5	B_7	B_9

B_1	B_2	B_4
B_8	B_7	B_5
B_9	B_3	B_6

B_1	B_9	B_2
B_6	B_5	B_7
B_4	B_3	B_8

(b) Rearrangement of the Cover Image Blocks

Figure 4.2: (a) Cover Image Blocks (b) Rearrangement of the Cover Image Blocks

4.2.3 Data Embedding and Extraction Method

The flowchart of the proposed data embedding method based on BWO algorithm is shown in Figure 4.3.

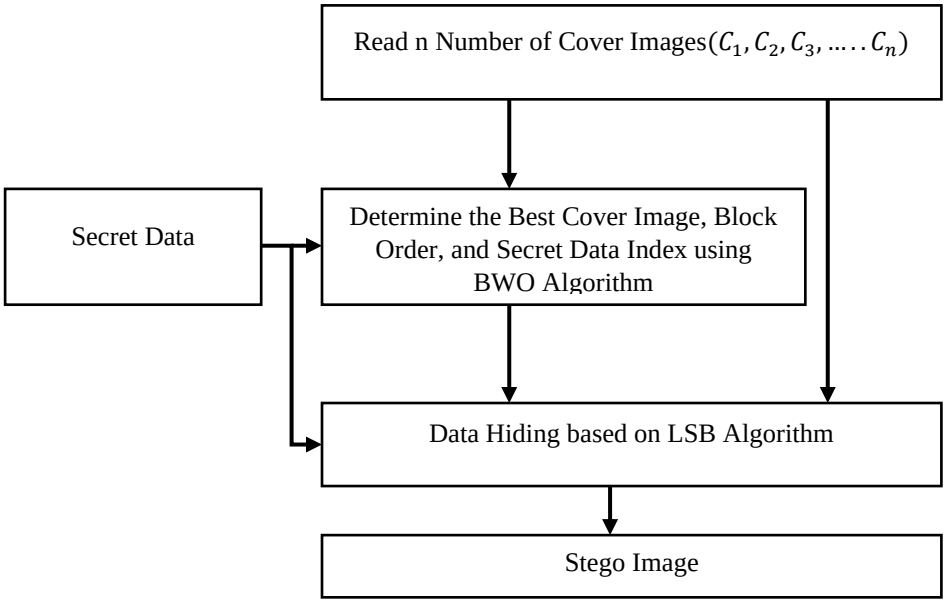


Figure 4.3: Flowchart of the Proposed Data Embedding Method using BWO Algorithm

Initially, a number of cover images and secret data are read. After that, it is given to the BWO algorithm and that performs procreation, cannibalism, and mutation steps to determine the best

cover image, optimal blocks in it, and secret data index based on the objective function. After that, the best cover image, optimal block order, and secret data index are given to the data embedding algorithm. Based on this information, the data embedding algorithm reads the best cover image, performs the operation on the secret data based on the optimal secret data index, and hides it in the optimal blocks based on the optimal block order information. In the last, the stego image, along with optimal block and secret data index information, is communicated from the transmitter to the receiver for data extraction purposes.

Figure 4.4 shows the flowchart of the data extraction method. On the receiver side, the optimal block order information, secret data index and stego image are read and given to the data extraction unit. The data extraction method extracts the secret data from the blocks. In the last, based on the secret data index, the operation is performed on the secret data to get the original secret data in the output.

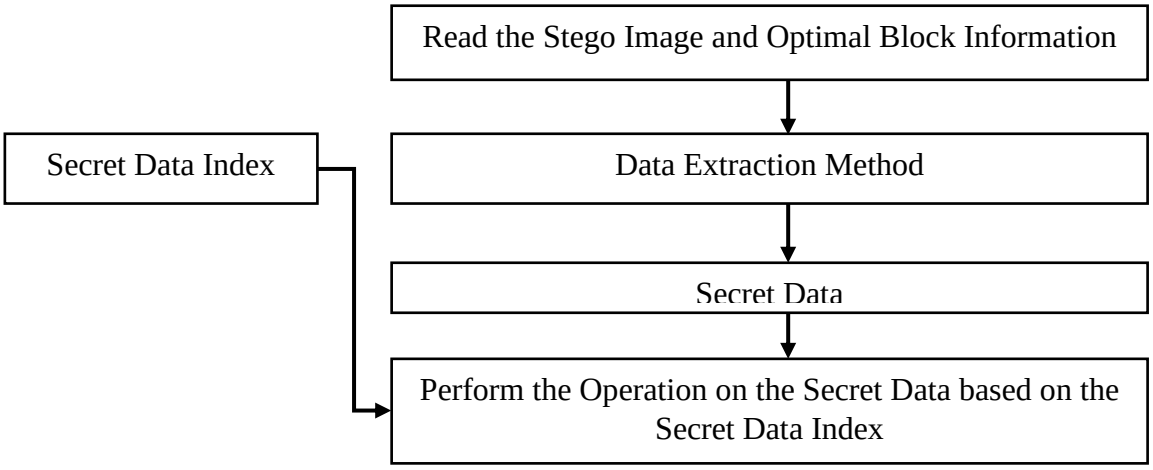


Figure 4.4: Flowchart of the Data Extraction Method using BWO Algorithm

Next, the detailed explanation is given on how black widow optimization algorithm searches the optimal cover image, block order and secret data index.

- In the first step, the parameter values for the black widow optimization algorithm are defined (procreate rate, cannibalism rate, mutation rate, objective function, total population and its dimension, lower and upper limits of cover image, secret data, and block order index).
- In the second step, a random population is generated according to the population size. Each population has a dimension of three. The first element of the population defines the optimal cover image index, second element defines the block order, and the third element defines the secret data index. The cover image index varies from $[1 - n]$, block

order varies from $[1-4]$, and secret data index varies from $[1-4]$. Here, n denotes the total number of cover images.

- In the third step, the fitness evaluation of each population is done based on the objective function. The Mean Square Error (MSE) is taken as an objective function in the proposed method.
- In the fourth step, the best population is determined which gives the minimum MSE over the other population.
- In the fifth step, the procreate step is performed, in which random populations are chosen as parents and offspring are generated from them. The offspring denotes the new cover image, blocks, and secret data index values. After that, fitness evaluation of the offspring is done based on the objective function and added into the original population array. Further, the population is sorted based on the fitness function.
- In the sixth step, the cannibalism step is performed, in which, based on the cannibalism rate, inappropriate solutions are removed from the population array in terms of cover image, block, and secret data index.
- In the seventh step, the mutation step is performed, in which, based on the mutation rate, the population array value is altered to explore new solutions.
- In the eighth step, steps 4-7 are performed for fixed number of iterations and the best index values of cover image, block order and secret data index are determined.

4.3 Results and Analysis

This section presents the simulation evaluation of the proposed method based on the BWO algorithm for image steganography. The USC SIPI image database images [70] are used as cover images in the proposed method. The proposed method is simulated 10 times for different secret data. Table 4.1 shows the parameter values of the BWO algorithm is defined to find the optimal cover image, block, and secret data index for data hiding.

4.3.1 Subjective Analysis

The subjective analysis is done based on visual inspection. In the visual analysis, the selected cover image is compared with the stego image that is generated after data hiding. Tables 4.2-4.3 shows the subjective analysis of the proposed method for grey-scale and color images. The result shows that the images look similar. Thus, it is difficult to the attacker to distinguish secret data in the stego image.

Table 4.1: Parameter Values of BWO Algorithm to Find the Optimal Cover Image, Block, and Secret Data Index

Parameter	Values	Parameter	Values
Total Number of Cover Images	[1-10]	Population Size	50
Resolution of the Cover Image (in	256×256	Iterations	30
Resolution of the Secret Data (in	256×256	Procreate Rate	0.5
Block Index	[1-4]	Cannibalism	0.5
Cover Image Block Index	[1-10]	Mutation Rate	0.1
Secret Data Index	[1-4]	Objective	MSE

Table 4.2 (a): Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Grey-Scale Image)

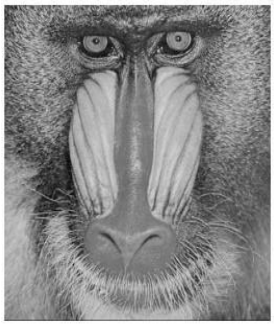
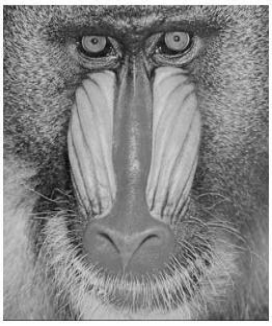
Secret Data	**Cover Image**	**Stego Image**
1		
2		

Table 4.2 (b): Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Grey-Scale Image)

Secret Data	Cover Image	Stego Image
3	Original Image 	Stego Image 
4	Original Image 	Stego Image 
5	Original Image 	Stego Image 
6	Original Image 	Stego Image 

Table 4.3 (a): Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Color Images)

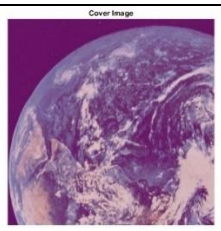
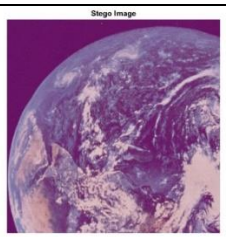
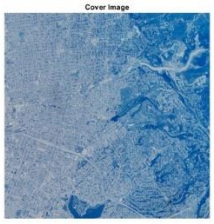
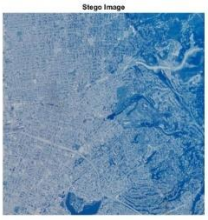
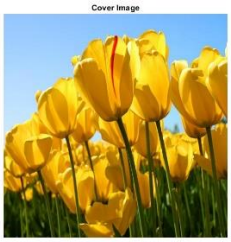
Secret Data	Cover Image	Stego Image
	1-bit	
1		
2		
3		
4		
5		

Table 4.3 (b): Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Color Images)

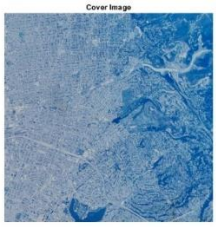
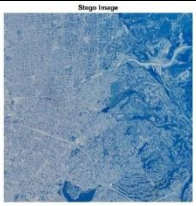
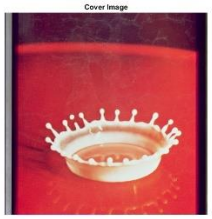
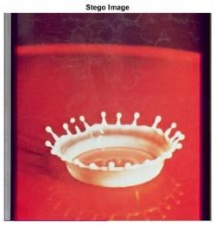
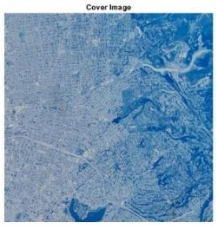
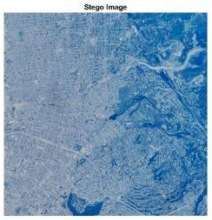
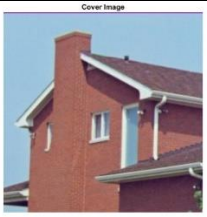
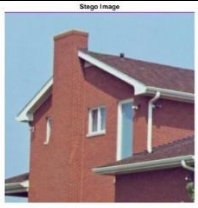
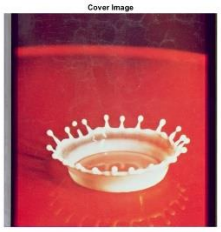
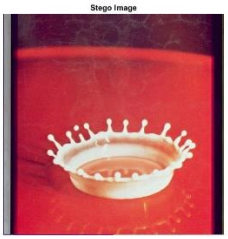
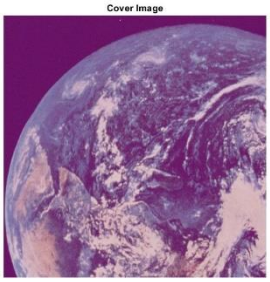
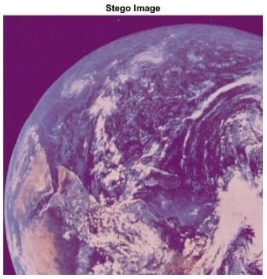
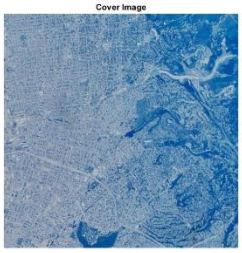
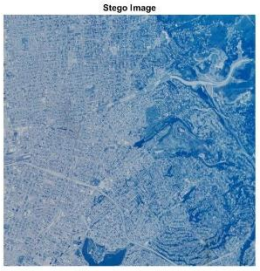
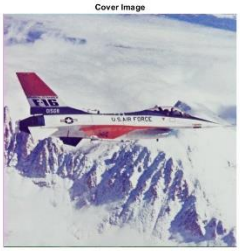
Secret Data	Cover Image	Stego Image
	2-bit	
1		
2		
3		
4		
5		

Table 4.3 (c): Subjective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Color Images)

Secret Data	Cover Image	Stego Image
	3-bit	
1		
2		
3		
4		
5		

4.3.2 Objective Analysis

Table 4.4 shows the selected cover image, optimal block order, and secret data index generated with inherent variability for grey-scale and color images. The result shows that selected cover image, optimal block order, and secret data index is not static. Further, from the analysis, we found that the cover image index for 1-bit is 9^{th} image and for 2-bit and 3-bit is 7^{th} image whereas, the block index and secret data index is changeable. Thus, it is difficult for the attacker to retrieve the secret data from the cover image due to flexible block order and secret data index. Thus, the proposed method enhances the security.

Table 4.4 (a): Optimal Selected Cover Image, Block Order, and Secret Data Index based on BWO Algorithm (for Grey-Scale Image)

Secret Data	Cover Image Index	Block Index	Secret Data Index
1-bit			
1	9	3	2
2	9	3	1
3	9	1	1
4	9	1	0
5	9	1	1
2-bit			
1	7	2	1
2	7	1	2
3	7	2	2
4	7	3	1
5	7	3	3
3-bit			
1	7	3	2
2	7	1	1
3	7	2	2
4	7	4	3
5	7	1	3

Table 4.4 (b): Optimal Selected Cover Image, Block Order, and Secret Data Index based on BWO Algorithm (for Color Image)

Secret Data	**Cover Image Index**	**Block Index**			**Secret Data Index**		
		R	**G**	**B**	**R**	**G**	**B**
	1-bit						
1	9	3	1	3	2	2	1
2	9	1	3	3	1	1	1
3	9	1	2	1	1	1	2
4	9	3	2	1	1	3	2
5	9	1	1	1	0	0	1
	2-bit						
1	7	2	1	1	1	1	1
2	7	1	1	1	2	1	1
3	7	2	2	1	2	2	1
4	7	3	2	2	1	2	1
5	7	3	3	2	3	2	2
	3-bit						
1	7	3	1	1	2	1	3
2	7	1	1	2	1	1	3
3	7	2	2	1	2	1	2
4	7	4	2	3	3	2	1
5	7	1	1	4	3	2	1

Further, Table 4.5 (a, b) shows the objective analysis of the proposed method based on the BWO algorithm for grey-scale and color images for single and multi-bit data embedding. In the objective analysis, various performance metrics, namely, MSE, RMSE, PSNR, SSIM, CC, Entropy, UIQ, IF, NAE are determined for the proposed method. The result shows that the proposed method achieves on average low MSE, RMSE, and NAE and high PSNR, CC, SSIM, UIQ, IF. Further, the proposed model achieves similar entropy between cover and stego image.

Table 4.5 (a): Objective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Grey-Scale Image)

MSE	RMSE	PSNR	SSIM	CC	Input Entropy	Output Entropy	UIQ	IF	NAE
1-bit									
0.2432	0.4932	54.2707	0.9943	0.9998	5.7406	5.7589	0.997972	0.999992	0.001383
0.2454	0.4953	54.2327	0.9942	0.9998	5.7406	5.7592	0.997972	0.999992	0.001395
0.2455	0.4955	54.2306	0.9943	0.9998	5.7406	5.7591	0.997972	0.999992	0.001396
0.2445	0.4945	54.2479	0.9943	0.9998	5.7406	5.7589	0.997972	0.999992	0.001390
0.2434	0.4934	54.2672	0.9943	0.9998	5.7406	5.7591	0.997972	0.999992	0.001384
2-bit									
1.2043	1.0974	47.3234	0.9807	0.9988	6.4573	6.4909	0.999302	0.999431	0.018314
1.2153	1.1024	47.2841	0.9807	0.9988	6.4573	6.4908	0.999302	0.999425	0.018486
1.2050	1.0977	47.3208	0.9807	0.9988	6.4573	6.4912	0.999302	0.999430	0.018325
1.2038	1.0972	47.3252	0.9808	0.9988	6.4573	6.4910	0.999302	0.999431	0.018330
1.2108	1.1004	47.3001	0.9806	0.9988	6.4573	6.4912	0.999302	0.999428	0.018404
3-bit									
4.9320	2.2208	41.2006	0.9190	0.9948	6.4573	6.4973	0.996018	0.997668	0.037363
4.9007	2.2137	41.2283	0.9193	0.9949	6.4573	6.4971	0.996018	0.997683	0.037093
4.9131	2.2165	41.2173	0.9188	0.9948	6.4573	6.4970	0.996723	0.997677	0.037116
4.8882	2.2109	41.2393	0.9188	0.9948	6.4573	6.4970	0.996723	0.997689	0.037187
4.9320	2.2208	41.2006	0.9188	0.9948	6.4573	6.4975	0.997429	0.997668	0.037428

Table 4.5 (b): Objective Analysis of the Proposed Image Steganography Method based on BWO Algorithm (for Color Image)

Plane	MSE	RMSE	PSNR	SSIM	CC	Input Entropy	Output Entropy	UIQ	IF	NAE
	1-bit									
R	0.2523	0.5023	54.1122	0.9992	0.9999	7.2596	7.2543	1.000000	0.999980	0.002471
G	0.2501	0.5001	54.15	0.999	0.9996	6.6599	6.6593	1.000000	0.999985	0.001769
B	0.251	0.501	54.1335	0.9987	0.999	6.046	6.0453	1.000000	0.999985	0.001426
Avg.	**0.251133**	**0.501133**	**54.1319**	**0.998967**	**0.9995**	**6.655167**	**6.652967**	**1**	**0.999983**	**0.001889**
R	0.2497	0.4997	54.157	0.9973	0.9999	7.3172	7.3166	0.999511	0.999985	0.001905
G	0.249	0.499	54.1686	0.9974	1.0000	7.6458	7.6443	1.000000	0.999985	0.002004
B	0.2504	0.5004	54.1446	0.9972	1.0000	7.3053	7.303	1.000000	0.999985	0.002178
Avg.	**0.2497**	**0.4997**	**54.15673**	**0.9973**	**0.999967**	**7.422767**	**7.4213**	**0.999837**	**0.999985**	**0.002029**
R	0.2538	0.5038	54.0853	0.9992	0.9999	7.2597	7.2543	1.000000	0.999980	0.002486
G	0.2504	0.5004	54.1445	0.999	0.9996	6.6598	6.6593	1.000000	0.999985	0.001771
B	0.2503	0.5003	54.1458	0.9987	0.999	6.046	6.0453	1.000000	0.999985	0.001422
Avg.	**0.2515**	**0.5015**	**54.1252**	**0.998967**	**0.9995**	**6.655167**	**6.652967**	**1**	**0.999983**	**0.001893**
R	0.2585	0.5085	54.0057	0.9939	0.9999	7.0217	7.0193	1.000000	0.999968	0.004467
G	0.2498	0.4998	54.1545	0.995	0.9999	7.6111	7.6079	0.999779	0.999975	0.003082
B	0.2666	0.5163	53.8722	0.9932	0.9999	6.5156	6.5069	1.000000	0.999954	0.005897
Avg.	**0.2583**	**0.5082**	**54.0108**	**0.994033**	**0.9999**	**7.049467**	**7.0447**	**0.999926**	**0.999966**	**0.004482**
R	0.2518	0.5018	54.1204	0.9992	0.9999	7.2596	7.2543	1.000000	0.999980	0.002466
G	0.2499	0.4999	54.1526	0.999	0.9996	6.6599	6.6593	1.000000	0.999985	0.001768
B	0.2495	0.4995	54.1592	0.9987	0.999	6.0461	6.0453	1.000000	0.999985	0.001418
Avg.	**0.2504**	**0.5004**	**54.14407**	**0.998967**	**0.9995**	**6.6552**	**6.652967**	**1**	**0.999983**	**0.001884**
	2-bit									
R	1.2474	1.1169	47.1706	0.9751	0.9997	7.0942	7.0807	0.999096	0.999924	0.003535
G	1.366	1.1688	46.7762	0.9686	0.9996	7.0323	6.9771	0.999811	0.999841	0.009512
B	1.2484	1.1173	47.1674	0.9754	0.9994	6.2278	6.2126	1.000000	0.999854	0.007821
Avg.	**1.287267**	**1.134333**	**47.03807**	**0.973033**	**0.999567**	**6.784767**	**6.7568**	**0.999636**	**0.999873**	**0.006956**

R	1.2447	1.1157	47.1801	0.9788	0.9994	7.3848	7.3817	0.998833	0.999924	0.004309
G	1.3003	1.1403	46.9903	0.9769	0.9998	7.6612	7.6493	0.999796	0.999921	0.005695
B	1.325	1.1511	46.9087	0.975	0.9993	7.1939	7.1613	0.999551	0.999783	0.01005
Avg.	**1.29**	**1.1357**	**47.02637**	**0.9769**	**0.9995**	**7.4133**	**7.397433**	**0.999393**	**0.999876**	**0.006685**
R	1.3473	1.1607	46.8362	0.968	0.9997	7.0269	7.0193	0.999849	0.999831	0.011496
G	1.2496	1.1178	47.1631	0.9766	0.9996	7.6147	7.6079	0.999779	0.999876	0.007708
B	1.4266	1.1944	46.5877	0.9629	0.9997	6.5299	6.5069	1.000000	0.999754	0.015417
Avg.	**1.341167**	**1.157633**	**46.86233**	**0.969167**	**0.999667**	**7.057167**	**7.0447**	**0.999876**	**0.99982**	**0.01154**
R	1.3406	1.1578	46.8578	0.9683	0.9997	7.0269	7.0193	0.999849	0.999832	0.011461
G	1.254	1.1198	47.1478	0.9766	0.9996	7.6147	7.6079	0.999779	0.999876	0.007719
B	1.4246	1.1936	46.5939	0.9628	0.9997	6.53	6.5069	0.999823	0.999754	0.015414
Avg.	**1.339733**	**1.157067**	**46.8665**	**0.969233**	**0.999667**	**7.0572**	**7.0447**	**0.999817**	**0.999821**	**0.011531**
R	1.2751	1.1292	47.0753	0.9755	0.9988	6.4338	6.3868	0.997305	0.999922	0.004339
G	1.2524	1.1191	47.1533	0.976	0.9996	6.5831	6.5354	0.999696	0.999924	0.004732
B	1.1939	1.0927	47.3611	0.9758	0.9997	6.4468	6.3887	0.999781	0.999927	0.004244
Avg.	**1.240467**	**1.113667**	**47.19657**	**0.975767**	**0.999367**	**6.4879**	**6.436967**	**0.998927**	**0.999924**	**0.004438**
	3-bit									
R	5.2493	2.2911	40.9298	0.973	0.9804	6.0614	6.0453	0.97166	0.99968	0.007455
G	5.9421	2.4376	40.3914	0.8849	0.9989	7.0416	7.0193	0.999396	0.999257	0.025014
B	5.2623	2.294	40.919	0.9127	0.9985	7.6161	7.6079	0.999115	0.999479	0.016241
Avg.	**5.484567**	**2.3409**	**40.74673**	**0.923533**	**0.9926**	**6.906367**	**6.890833**	**0.990057**	**0.999472**	**0.016237**
R	6.5879	2.5667	39.9433	0.8654	0.9986	6.5613	6.5069	0.999044	0.998865	0.034447
G	5.2791	2.2976	40.9052	0.902	0.996	6.7885	6.7692	0.997549	0.99827	0.031519
B	5.7288	2.3935	40.5502	0.8849	0.9946	6.3591	6.3389	0.997909	0.996968	0.046604
Avg.	**5.865267**	**2.419267**	**40.46623**	**0.8841**	**0.9964**	**6.569633**	**6.538333**	**0.998167**	**0.998034**	**0.037523**
R	5.5993	2.3663	40.6494	0.8928	0.9936	6.2303	6.2105	0.997594	0.996496	0.049814
G	5.3019	2.3026	40.8865	0.9124	0.9972	7.2864	7.274	0.998277	0.999304	0.01749
B	5.5535	2.3566	40.6851	0.8962	0.997	7.0536	7.0404	0.998255	0.998778	0.026104
Avg.	**5.4849**	**2.341833**	**40.74033**	**0.900467**	**0.995933**	**6.856767**	**6.841633**	**0.998042**	**0.998193**	**0.031136**
R	5.5602	2.358	40.6799	0.8933	0.9936	6.2302	6.2105	0.99599	0.99652	0.049553
G	5.2954	2.3012	40.8918	0.9126	0.9972	7.2867	7.274	0.998277	0.999305	0.017474

B	5.5229	2.3501	40.7092	0.8966	0.997	7.0537	7.0404	0.998255	0.998785	0.026007
Avg.	**5.4595**	**2.336433**	**40.7603**	**0.900833**	**0.995933**	**6.856867**	**6.841633**	**0.997507**	**0.998203**	**0.031011**
R	5.5127	2.3479	40.7171	0.8986	0.9964	6.8988	6.8834	0.997705	0.998479	0.029366
G	5.2269	2.2862	40.9484	0.9723	0.9983	7.7395	7.7356	0.998792	0.999681	0.009480
B	5.2551	2.2924	40.925	0.9721	0.9975	7.4538	7.4485	0.99756	0.999679	0.010210
Avg.	**5.331567**	**2.308833**	**40.8635**	**0.947667**	**0.9974**	**7.364033**	**7.355833**	**0.998019**	**0.99928**	**0.016352**

4.3.3 Embedding Capacity Vs. PSNR

Table 4.6 shows the embedding capacity vs. PSNR for the proposed method. The result shows that the PSNR varies from 72.6595 dB to 54.2228 dB for 1-bit data hiding for embedding capacity 1000 bits to 65536 bits for the cover image resolution of 256x256. In the similar way, the PSNR for 2-bit and 3-bit varies from 65.9815 dB to 47.3067 dB and 59.4552 dB to 41.1910 dB, respectively. This shows that the embedding capacity has large impact on the PSNR factor.

Table 4.6: EC vs. PSNR for the Proposed Method

Embedding Capacity (in bits)	**1000**	**10000**	**20000**	**25000**	**50000**	**65536**
1bit						
MSE	0.0035	0.0372	0.0736	0.0929	0.1852	0.2459
PSNR (in dB)	72.6595	62.4288	59.4615	58.4509	55.4534	54.2228
2-bit						
MSE	0.0164	0.1723	0.3587	0.4525	0.9150	1.2090
PSNR (in dB)	65.9815	55.7675	52.5833	51.5748	48.5166	47.3067
3-bit						
MSE	0.0737	0.7179	1.3623	1.7027	3.5516	4.9429
PSNR (in dB)	59.4552	49.5702	46.7882	45.8193	42.6266	41.1910

4.3.4 Comparative Analysis

Finally, based on the PSNR value, the proposed method is compared with the existing image steganography methods based on bio-inspired algorithms [56, 59-60]. In Table 4.7 (a), the comparative analysis is performed for same cover images (512×512) and secret data size (128×128). The result shows that the proposed method achieves the average PSNR of 57.21dB, whereas the existing methods based on PSO and ABC achieve the average PSNR of 45.296dB and 56.39dB, respectively. This indicates that the proposed method achieves superior performance over the PSO and ABC algorithm, respectively.

Table 4.7 (a): Comparative Analysis of the Proposed Image Steganography Method based on BWO Algorithm with the Existing Steganography Methods [56] based on PSNR Value

Images	**PSO**	**ABC**	**Proposed Method**
Lena	45.1900	56.40	57.19
Jet	45.3800	56.39	57.25
Lake	45.6700	56.40	57.20
Elaine	45.9300	56.36	57.19
Baboon	44.3100	56.39	57.24
Average	**45.296**	**56.39**	**57.21**

Further, Table 4.7 (b) shows the comparative analysis with the recent existing method [59] which used the GA algorithm for optimized data hiding using the single and multi-bit data embedding. The result shows that the proposed model achieves the better PSNR in the single and multi-bit data embedding method for different cover images.

Table 4.7 (b): Comparison of Proposed and Existing Algorithms [59] in terms of PSNR (in dB)

	P. D. Shah and R. S. Bichkar [59]			**Proposed Method**		
	1-bit	**2-bit**	**3-bit**	**1-bit**	**2-bit**	**3-bit**
Living Room	52.17	-		54.2324	47.3024	41.2109
Pirates	52.41	-	40.82	54.2109	47.3103	41.2053
Airplane	52.21	46.37		54.2418	47.2893	41.2178
Boat	52.35	-		54.2167	47.2965	41.1995
Mandrill	52.13	46.42		54.2167	47.2920	41.2043
Lake		46.42		54.2324	47.3024	41.2109
Pepper		46.39		54.2109	47.3103	41.2053
Lena		46.43	40.75	54.2418	47.2893	41.2178
Blonde			40.91	54.2167	47.2965	41.1995
Cameraman			40.82	54.2167	47.2920	41.2043

Finally, Table 4.7(c) shows the comparative analysis of the proposed method with the existing method which used the HHO algorithm for hide the multi-bit data in the cover image. The result shows that the proposed method achieves the better PSNR in the range of 47.2893-47.3103dB for 2-bit and 41.1995-41.2178dB for the 3-bit LSB method, respectively.

Table 4.7 (c): Comparison of Proposed and Existing Algorithms [60] in terms of PSNR (in dB)

Images	**Hameed et al. [60]**		**Proposed Method**	
	2-bit	**3-bit**	**2-bit**	**3-bit**
Image1	44.3589	39.8798	47.3024	41.2109
Image2	44.3083	39.8404	47.3103	41.2053
Image3	44.5281	39.9505	47.2893	41.2178
Image4	44.4704	39.9159	47.2965	41.1995
Image5	45.3950	41.1958	47.2920	41.2043
Image6	44.6054	39.9975	47.3024	41.2109

4.3.5 Intentional/Non-Intentional Attacks

In this section, we have applied the international/non-intentional attacks on the proposed method. The attacks are considered for evaluate the proposed method is salt & pepper, gaussian, rotate, and low-pass filtering attack. These attacks are evaluated using the two-performance metrics, such as SF and BER. The result shows that the rotate and low-pass filtering attacks more impact the stego image than the salt and pepper attack for recovering the secret data. However, the impact can be reduced by adding an error correction code while embedding the secret data in the cover image.

Table 4.8: Performance Metrics for different Intentional/Non-Intentional Attacks

Attacks		Salt and Pepper (D=0.001)	Gaussian Attack (V=0.001)	Rotate	Low Pass Filtering
		1-bit			
Image1	SF	184	177	184	183
	BER	10.7239	7.5324e+03	5.9936e+03	2.2487e+03
Image2	SF	85	56	85	83
	BER	14.3555	7.9129e+03	4.9918e+03	2.7339e+03
Image3	SF	184	177	184	183
	BER	13.8947	7.5324e+03	5.9679e+03	2.2487e+03
		2-bit			
Image1	SF	63	31	61	58
	BER	12.7258	4.6982e+03	3.4043e+03	2.2884e+03
Image2	SF	63	31	61	58
	BER	9.9365	4.6982e+03	3.4171e+03	2.2884e+03
Image3	SF	63	31	61	58
	BER	17.3035	4.6982e+03	3.4002e+03	2.2884e+03
		3-bit			
Image1	SF	63	29	60	57
	BER	15.2710	4.4995e+03	3.2248e+03	2.0993e+03
Image2	SF	63	29	60	57
	BER	10.3882	4.4995e+03	3.2272e+03	2.0993e+03
Image3	SF	63	29	60	57
	BER	12.1460	4.4995e+03	3.2208e+03	2.0993e+03

4.4 Conclusion

In this chapter, we have proposed an optimized image steganography method based on the BWO algorithm. In the proposed method, the BWO algorithm searches the optimal cover image, block order, and secret data index to enhance the imperceptibility parameter by minimizing the objective function. The simulation results show that the optimal cover image, block order, and secret data index has sufficient variability for different secret data. Further,

the objective analysis shows that the proposed method achieves low values of MSE, RMSE, NAE; high values of PSNR, correlation coefficient, SSIM, UIQ, IF; and comparable entropy between cover and stego image. In the last, comparative analysis is done based on the PSNR parameter with some of the existing implementation from literature. When compared to existing techniques, the proposed method yields superior PSNR results.

Chapter 5

Evolutionary Algorithm based Key Generation for Image Encryption

5.1 Introduction

Digital images are now-a-days utilized to communicate sensitive information for a number of applications, such as for military, medical, and private conferencing [86]. Quite often, it is prone to numerous attacks, namely, unauthorized access and modification, when communicating on the internet [87]. As a result, before being transmitted over the internet, digital images are encrypted using encryption methods. The secret image is transformed into an encrypted image using a random key in the encryption method. In this chapter, the bio-inspired evolutionary algorithms have been employed for key generation in an optimal sense for image encryption applications.

In the literature, image encryption is performed either in the "spatial domain" or in the "transform domain" [18]. In the spatial domain, the image pixels are directly manipulated using the encryption method. On the other hand, in the transform domain, the images are encrypted in the frequency domain, and an inversed transform is performed before communicating the encrypted image. We concentrated on the spatial domain in our work due to its lower complexity. Further, in the literature, chaotic function, DNA, elliptic curve, and bio-inspired-based image encryption methods are proposed [38, 69, 88-89, 18]. Out of these methods, chaotic function and bio-inspired-based image encryption methods are more preferred. Therefore, in our research, these encryption methods are taken into consideration. The chaotic functions are used in the image encryption method for key generation because these functions are extremely sensitive to initial state of the parameter values. On the other hand, bio-inspired-based encryption methods are used to optimize the image encryption parameters based on the objective function. In the literature, bio-inspired algorithms are employed for key generation and to choose the most optimal encrypted image.

Bio-inspired algorithms are broadly categorized into two types, such as swarm intelligence and evolutionary algorithms [82]. Evolutionary algorithms are more commonly used in the

literature for image encryption methods [5, 86, 43-45]. These algorithms search for the best random key from a set of *n* keys and give the optimal key as the output. To accomplish this, a few populations of the evolutionary algorithm are initially defined in the key's lower and upper bound ranges. The fitness evaluation of each population is done based on the objective function, which determines the best key. Next, new populations are generated from the initial populations based on the operations of evolutionary algorithms. The fitness evaluation of the new population is done in a similar way it was done for the initial population. If the new population fitness evaluation is superior to the best key, then the best key will be updated. The whole operation is iterated for a predetermined number of iterations.

The evolutionary algorithms use a predetermined number of iterations to explore all possible solutions to give the best key in the output. The advantage of evolutionary algorithm-based key generation methods is that they generate completely random keys. In the literature, the genetic algorithm is the most preferred evolutionary algorithm for image encryption. The exploration rate of the GA algorithm is low due to the limited number of offspring generated using crossover and mutation operations [85]. Besides that, inappropriate solutions are not removed while searching for optimal solutions. These challenges are taken into consideration, and other evolutionary algorithms have also been explored.

Recently, a new evolutionary optimization algorithm was proposed by “V Hayyolalam and Ali A Kazem” [79], which is based on the mating process of the black widow spider. Black widow spiders can mate in pairs. Thus, it generates a number of offspring. Further, strong spiders eat the weak spiders as their food for survival purposes. This process is known as cannibalism. These properties were taken into consideration by the authors, and they proposed the “black widow optimization” (BWO) algorithm. In the BWO algorithm, the offspring generation process is known as the "procreate step," whereas the consuming weak spider process is known as the "cannibalism step." Due to these steps, the BWO algorithm has a better exploration rate to find the optimal solution than the genetic algorithm. Thus, the proposed image encryption method takes into consideration the BWO algorithm for encrypting the secret images. We have proposed two image encryption methods. The novelty of the first image encryption method, the BWO algorithm, and its operation is utilized for key generation and encryption purposes, whereas in the second method, a completely random key for image encryption is generated by determining the initial parameter values of the chaotic map using the BWO algorithm. The rest of the chapter is organized into four sections. Section 5.2 explains the detailed description of

the proposed methods based on the evolutionary algorithm. Section 5.3 explains the image encryption method, which is based on the black widow optimization algorithm, and its operation. Further the results of subjective and objective analysis are provided in this section that evaluate the effectiveness of the presented method. Next, in Section 5.4 the image encryption method is explained that is based on the chaotic function. In this method, BWO algorithm is used to compute the parameter values of the chaotic function. Further, the proposed method is evaluated using subjective and objective analysis. Section 5.5 provides the conclusion.

5.2 Proposed Methods based on BWO Algorithm

The basic principle of the BWO algorithm is based on the mating process of black widow spiders. These spiders can mate in parallel and their cannibalism nature makes it unique optimization over others. The mating process generates a number of offspring. Thus, numerous solutions are explored while searching the solution space. Cannibalistic nature, on the other hand, eliminates inappropriate solutions while searching the search space. As we know, the optimization algorithms are iterative methods. Thus, due to cannibalism, the mating process in the next iteration is performed by superior-quality spiders. The steps of the BWO algorithm are classified into three stages. In the first stage, the procreate step is performed, in which offspring are generated by selecting random spiders as parents. In the second stage, the cannibalism step is performed, in which parent and offspring solutions are sorted based on the objective function and those that are inappropriate are removed. To explore new solutions, the third step involves performing mutation on the solutions left over from the cannibalism step. These steps are iterated for a fixed number of iterations, and the best solutions are updated in this process. In the end, the best solution is determined.

We have proposed two image encryption methods based on the BWO algorithm. In the first method, the BWO algorithm is used for key generation based on the objective function. Further, its operation known as "mutation" is used in the encryption process. On the other hand, the second method is based on the chaotic function. The chaotic function's output is highly sensitive to the input parameter values. Therefore, the optimal selection of parameter values enhances the security of the image encryption method. Therefore, the BWO algorithm is used to determine the best values for the parameter based on the objective function. Entropy is taken as an objective function in both methods. In the first method, the best random key is chosen

from *n* keys that give the best entropy. On the other hand, in the second method, the best parameter values are chosen, which give the entropy value close to the ideal value required in the image encryption. Thus, in both methods, the objective function value is maximized. A in-depth explanation of these methods is provided in the following two sections.

5.3 Image Encryption Method based on BWO Algorithm and its Operation

In the majority of the image encryption methods, the exclusive-OR procedure is used to encrypt images with the secret data and private key. The private key generation is accomplished using various bio-inspired algorithms, chaotic map, linear and non-linear feedback shift register [7-10]. The proposed method is based on the classical substitution-permutation network. In the proposed method, an optimal random key is generated using the BWO algorithm. The secret image is processed in the form of blocks. After that, in the substitution step, exclusive-OR operation is executed among image block data and random key. Next, in the permutation step, the block data is circular rotated based on the mutation step of black widow optimization algorithm. Besides that, key scheduling is performed for subsequent blocks. The detailed description of the proposed image encryption method is given below.

The flowchart of the proposed image encryption method is shown in Figure 5.1. Initially, the secret image is read and split into 256-bit blocks. Afterwards, a 512-bit key is generated using a black widow optimization algorithm and it is grouped into two parts, namely, left key (L) and right key (R). The 256-bit length is selected for both the keys. Next, the exclusive-OR operation is carried out between the 256-bit block and the left key. Further, the black widow operation, also called as mutation, is performed on the Exclusive-OR output to get the final encryption. The black widow operations provide confusion and diffusion in the encryption process. Further, the keys of the subsequent blocks are determined from the previous blocks. As shown in Figure 5.1, the left key (L) is replaced with the right key (R); and the right key (R) is replaced with the XOR output of the previous block. This whole process is repeated for the next blocks. The mathematical model for one round for encryption is given below.

$$P = \{P_{127,}P_{126,}\ldots\ldots\ldots\ldots\ldots\ldots P_{2,}P_1P_0\} \tag{5.1}$$

$$K = \{K_{255,}K_{254,}\ldots\ldots\ldots\ldots\ldots\ldots K_{2,}K_1K_0\} \tag{5.2}$$

$$K_L = \{K_{127,}K_{126,}\ldots\ldots\ldots\ldots\ldots\ldots K_{2,}K_1K_0\} \tag{5.3}$$

$$K_R = \{K_{255,}K_{254,}\ldots\ldots\ldots\ldots\ldots\ldots K_{130,}K_{129}K_{128}\} \tag{5.4}$$

For Encryption

$$C' = P \oplus K_L \tag{5.6}$$

$$R = \sum_{i=0}^{127} D_i \qquad D_i\text{==1 if } K_{R(i)} == 1,\ D_i\text{==0 if } K_{R(i)} == 0 \tag{5.7}$$

$$C = ror(C', R) \tag{5.8}$$

Key Updation for the Next Round

$$K_L = C' \tag{5.9}$$

$$K_R = \{K_{127,}K_{126,\ldots\ldots\ldots\ldots\ldots\ldots}K_{2,}K_1K_0\} \tag{5.10}$$

Next, the comprehensive explanation of the 512-bit key generation using BWO algorithm is given below.

1. In the first step, BWO algorithm parameters, namely, total population, dimension of the population, procreate rate, cannibalism rate, mutation rate, iterations, objective function [entropy], lower and upper limit of the key [0-255] is defined. In the secret images, the pixel value varies in between 0-255. Therefore, lower, and upper limit is defined in the range because during encryption, exclusive-OR operation needs to perform between secret image pixel and random key.
2. In the second step, the population array is needed to initialize. The dimension of each population is 64 and each dimension value represents the 8-bit of the key. Therefore, 64-dimension population gives the 512-bit in the output. The initialized is performed randomly in the lower and upper limit of the key.
3. In the third step, fitness evaluation of each population is performed based on objective function. After that, the fitness evaluation of population array is compared and determined the best population which gives the maximum entropy.
4. In the fourth step, random populations are chosen from the population array. Further, based on the procreate rate, new populations are generated using Eq. (2.15). The generated new population is added in the initial population array and sorted according to the objective function.
5. In the fifth step, based on the cannibalism rate, inappropriate populations are removed from the population array.
6. In the sixth step, population array is updated according to the mutation rate.
7. Steps 3-6 is performed until desired objective is not meet or total iterations are not finished.

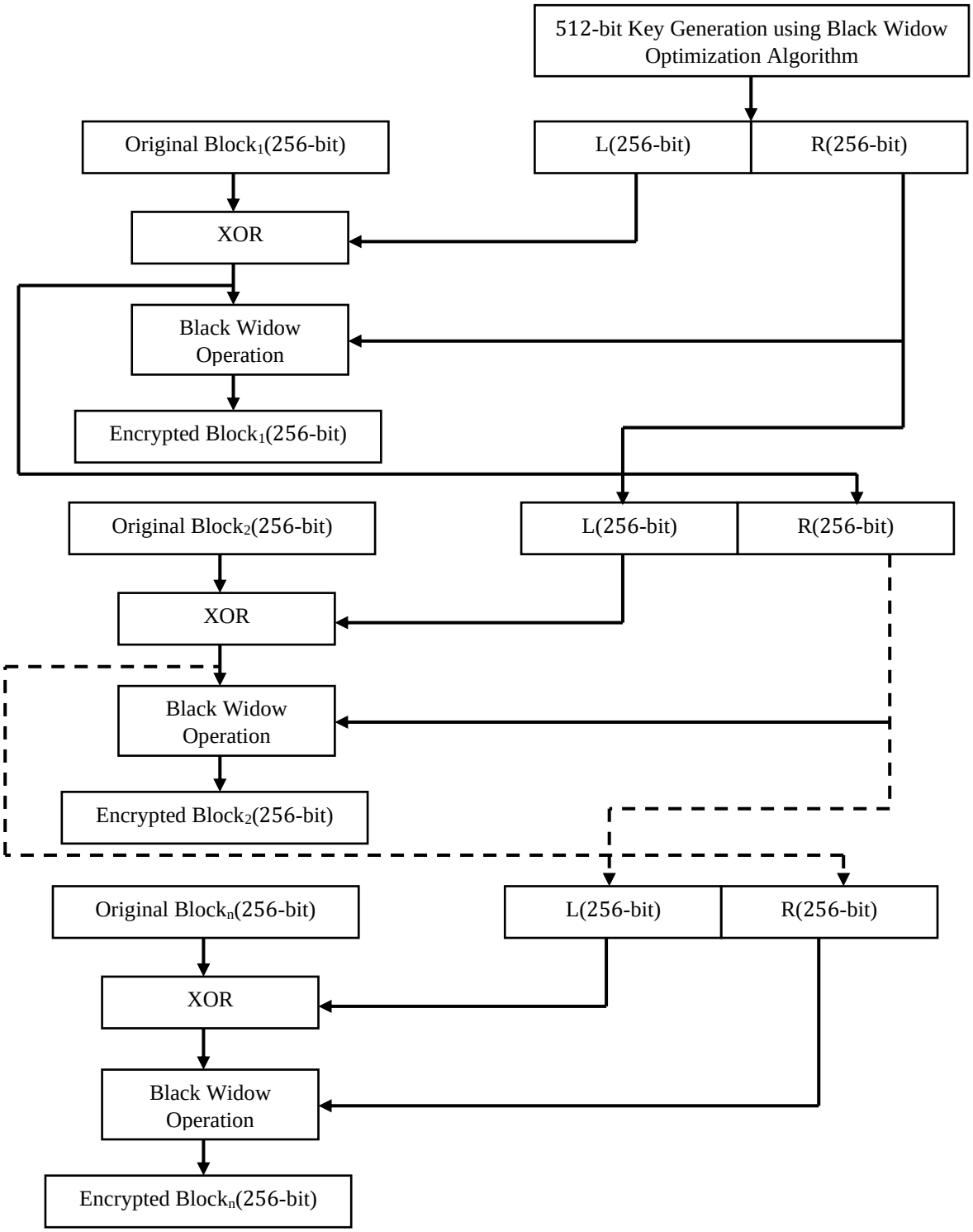


Figure 5.1: Flowchart of the Image Encryption using BWO Algorithm and its Operation

5.3.1 Results and Analysis

Here, we have presented the subjective and objective analysis of the proposed method based on the BWO algorithm. Further, it is compared with the existing image encryption method based on various parameters. Table 5.1 shows the parameter values are taken under consideration for key generation and to perform encryption.

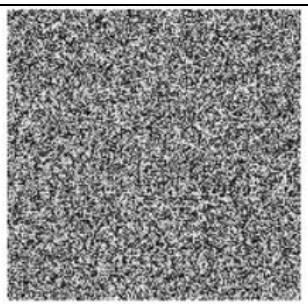
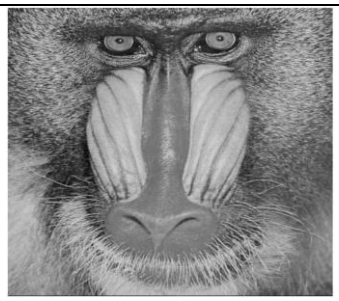
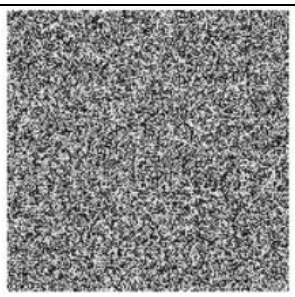
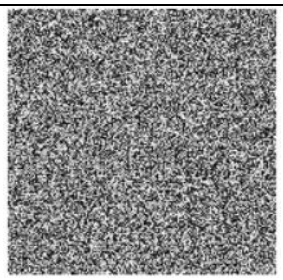
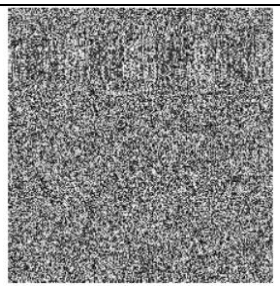
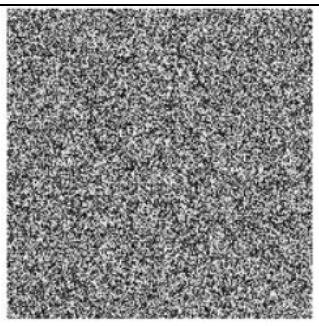
The standard images database is taken as secret image in the proposed method. Further, population and iterations lower value chosen because choosing the higher value increases the computation time to achieve the image encryption. Next, objective function, entropy is chosen because it checks the 0's and 1's probability in the random key. In the ideal case, a key contains equal probability of 0's and 1's. The procreate and cannibalism rate has equal values because these operations are performed in the BWO algorithm to generate new population and removing the inappropriate population from the population array.

Table 5.1: Parameter Values of BWO Algorithm for Key Generation and Encryption

Parameter	Values
Standard Images Database	USC-SIPI image database [70]
Image Resolution	512×512
Total Population (n)	50
Total Number of Iterations	20
Procreate Rate	$n/2$
Cannibalism Rate	$n/2$
Mutation Rate	0.0098
Key Size (in Bytes)	64
Lower Bound of the Key	0
Upper Bound of the Key	255
Objective Function for Key Generation	Entropy

Table 5.2 shows the subjective analysis of the image encryption method based on the BWO algorithm for different images. The standard dataset images, namely, *Lena, Baboon, Pepper, Airplane, and Barbara* are taken under consideration. In the analysis, the original image is compared with the encrypted image based on the visual appearance [44, 72]. The results indicate that encrypted images look completely noisy. Thus, this makes it extremely difficult for the attacker to recover the original image.

Table 5.2: Subjective Analysis of the Proposed Image Encryption Method based on BWO Algorithm

Images	Original Image	Encrypted Image
Lena		
Baboon		
Pepper		
Airplane		
Barbara		

Further, to determine the distribution of grayscale pixels in an image, histogram analysis is a common statistical metric. A uniform histogram is one sign that an image is more resistant to statistical attacks. An image's histogram can reveal information about its source if it isn't uniform [44]. Table 5.3 (a-b) shows the histogram analysis for different original images for the proposed method. The results clearly indicate that the histogram of images which are encrypted is more uniform. Thus, the proposed method is capable of concealing more information and hence provides more shielding against the statistical attacks.

Table 5.3 (a): Histogram Analysis of the Proposed Image Encryption Method based on BWO Algorithm

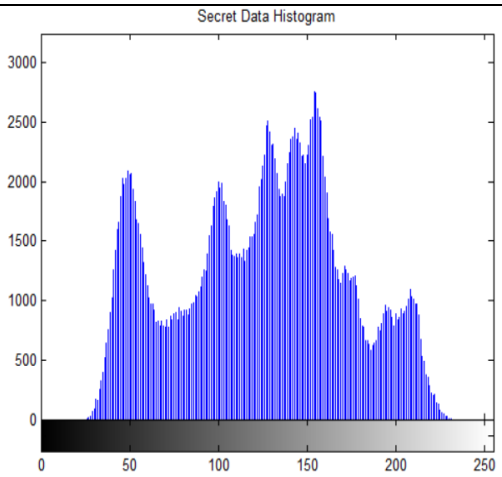
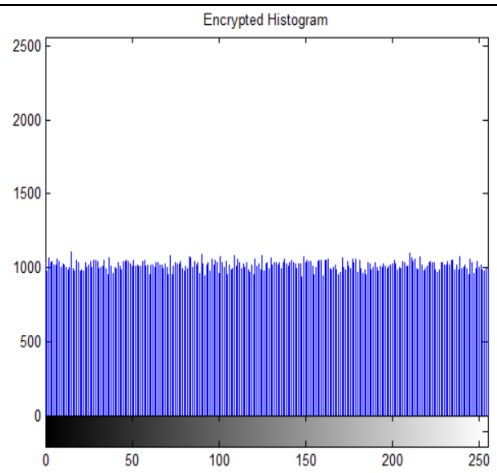
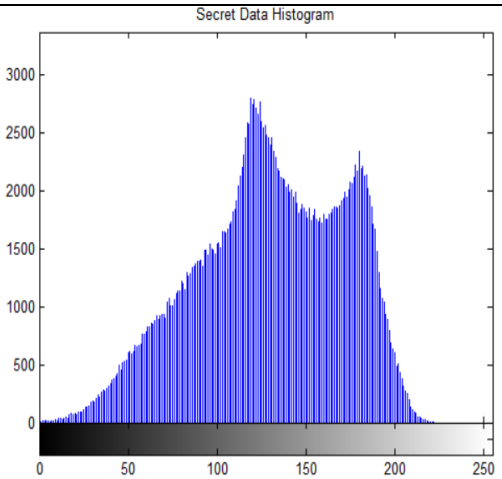
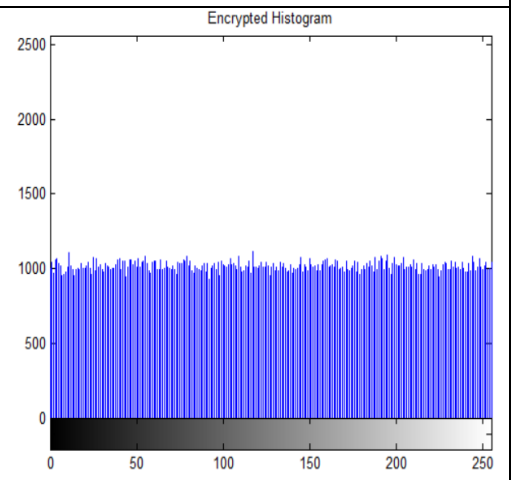
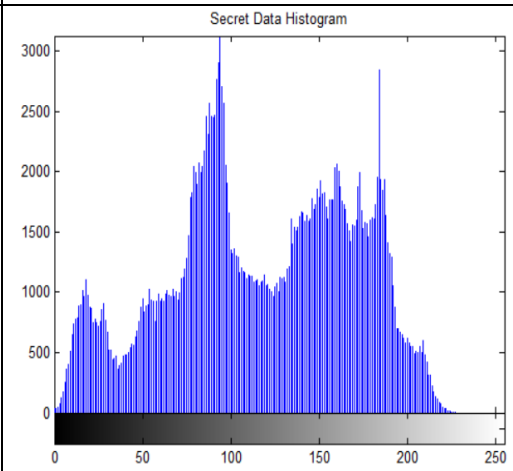
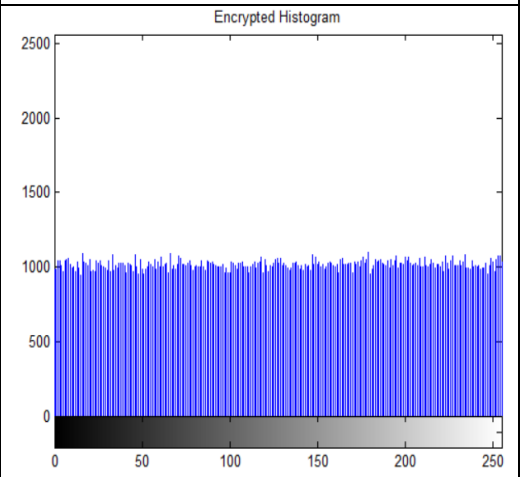
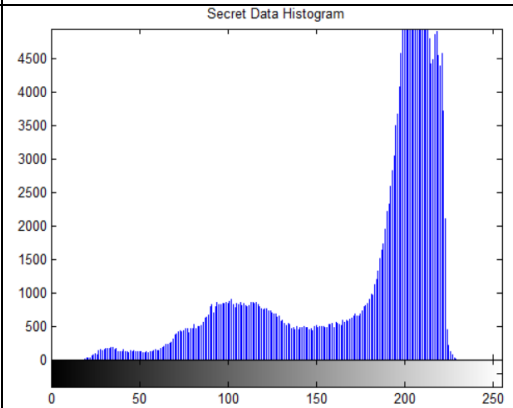
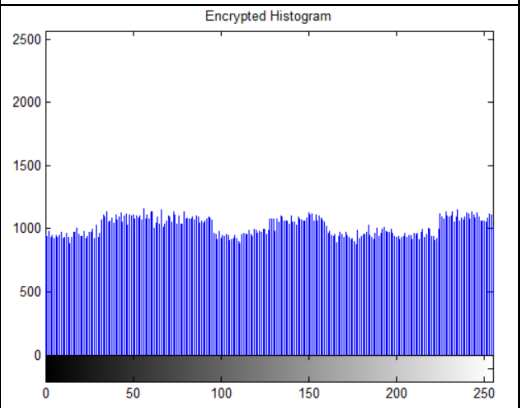
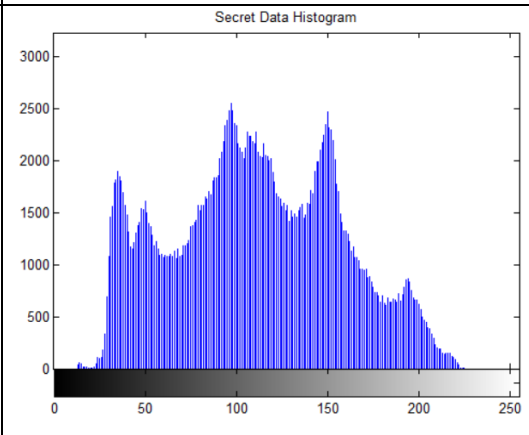
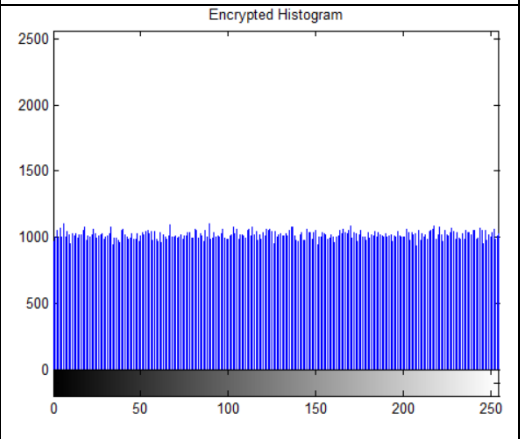
Images	**Original Image Histogram**	**Encrypted Image Histogram**
Lena		
Baboon		

Table 5.3 (b): Histogram Analysis of the Proposed Image Encryption Method based on BWO Algorithm

Images	Original Image Histogram	Encrypted Image Histogram
Pepper		
Airplane		
Barbara		

Next, the histogram uniformity is verified using Chi-square test (χ^2). Table 5.4 shows the Chi-square test for the different images that are taken under consideration. The results show that the computed values of Chi-square are less than 293.2478 and it passes the histogram uniformity test.

Table 5.4: Chi-Square Test for the Proposed Image Encryption Method based on BWO Algorithm

Images	χ^2 **Test**	**Remarks**
Lena	209.30	Pass
Baboon	217.97	Pass
Pepper	247.70	Pass
Airplane	275.22	Pass
Barbara	292.39	Pass

Table 5.5 shows the objective analysis of the proposed image encryption method based on the various parameters such as PSNR, NPCR, entropy, correlation coefficient, maximum deviation, and execution time.

In the PSNR analysis, PSNR between original and encrypted image is estimated for the proposed method. The results demonstrate that the proposed method is able to provide low values of PSNR for a variety of image types. Out of different images, Airplane achieves the lowest PSNR. Further, in the NPCR analysis, original image and key sensitivity analysis is done by altering the original secret image/original key. Table 5.5 shows the NPCR analysis for different images. In both instances, the proposed method accomplishes high NPCR near to ideal value is required in the image encryption method. This reflects that mere a slight variation in original image/original key changes a large number of pixels of encrypted image. Further, Table 5.5 indicates the entropy analysis. The results indicate that the proposed method achieves an entropy value near to 8 for the encrypted images. Thus, the proposed method provides enough randomness in the encrypted image that makes it robust against statistical attacks. Next, the proposed method is evaluated using the correlation coefficient parameter. In the cryptography, ideal value of 0 is required which represents the low correlation between original and encrypted image. Table 5.5 shows that the proposed method provides a lower correlation coefficient between images. Next, in the table, maximum deviation parameter value shows that maximum deviation achieved by proposed image encryption method between original and encrypted image. In the last, in the table, the execution time for different encrypted images is shown. The results indicate that the proposed method takes much lesser time due to fast key generation and simple operations for image encryption.

Table 5.5: Objective Analysis for the Proposed Image Encryption Method based on BWO Algorithm

Images	***PSNR*** **(in dB)**	**NPCR**		**Entropy**		**CC**	**Maximum Deviation**	**Execution Time (in Seconds)**
		Original Image Sensitivity Analysis	**Key Sensitivity Analysis**	**Original Image Entropy**	**Encrypted Image Entropy**			
Lena	12.54	99.554	99.58	7.4471	7.9993	0.0013	168480	3.51
Baboon	12.42	99.540	99.57	7.3519	7.9993	0.0018	201520	3.01
Pepper	12.90	99.572	99.63	7.5733	7.9993	0.0020	147609	3.06
Airplane	8.64	99.603	99.60	6.7056	7.9992	0.0019	276186	3.05
Barbara	13.78	99.540	99.57	7.4439	7.9993	0.0023	175760	3.16

5.3.2 Comparative Analysis with the Existing Image Encryption Methods

In this section, the proposed method is compared with the known existing methods like AES [90], Li et al. [91], and Mondal et al. [44] based on NPCR, entropy, correlation coefficient, and execution time parameter. Table 5.6 provides a NPCR parameter based comparative analysis with the other existing techniques. The results indicate that the proposed method provides high NPCR as compared to AES [90] and Li et al. [91] and a little lesser to Mondal et al. [44].

Table 5.6: Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on NPCR Value

Image	**AES [90]**	**Li et al. [91]**	**Mondal et al. [44]**	**Proposed Method**
Lena	0.0061	97.7646	99.6342	99.554
Baboon	0.0061	96.9589	99.6361	99.540
Pepper	0.0061	97.5632	99.6391	99.572
Airplane	0.0061	95.9206	99.6655	99.603
Barbara	0.0061	97.3125	99.6227	99.540

Table 5.7 provides the entropy parameter based on comparative analysis with the other existing techniques. The results indicate that the proposed method achieves higher entropy as compared to Li et al. [91] and approximately same entropy as compared to AES [90] and Mondal et al. [44].

Table 5.7: Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on Entropy Value

Image	**AES [90]**	**Li et al. [91]**	**Mondal et al. [44]**	**Proposed Method**
Lena	7.9994	7.3866	7.9994	7.9993
Baboon	7.9993	7.2101	7.9992	7.9993
Pepper	7.9994	7.3597	7.9993	7.9993
Airplane	7.9981	7.2991	7.9991	7.9992
Barbara	7.9992	7.2990	7.9993	7.9993

Table 5.8 provides the correlation coefficient parameter based comparative analysis with the other existing techniques. The results indicated that the proposed method achieves lower correlation coefficient as compared to Mondal et al. [44] and approximate same correlation coefficient as compared to AES [90] and Li et al. [91].

Table 5.8: Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on Correlation Coefficient Value

Image	**AES [90]**	**Li et al. [91]**	**Mondal et al. [44]**	**Proposed Method**
Lena	0.0015	1.2899e-05	0.1114	0.0013
Baboon	-0.0013	-4.1219e-04	0.0141	0.0018
Pepper	0.0021	-6.0429e-04	0.0353	0.0020
Airplane	2.4233e-04	-0.0060	0.0250	0.0019
Barbara	0.0020	-2.7831e-4	0.1398	0.0023

Table 5.9 provides the execution time parameter based comparative analysis with the other existing techniques. The results indicate that the suggested method achieves lowest execution time over other techniques such as Li et al. [91] and Mondal et al. [44].

Table 5.9: Comparative Analysis of Proposed Image Encryption Method and Existing Methods based on Execution Time (in Seconds)

Image	**Li et al. [91]**	**Mondal et al. [44]**	**Proposed Method**
Lena	34.855	35.810	3.51
Baboon	32.376	29.659	3.01
Pepper	33.672	29.756	3.06
Airplane	30.925	28.850	3.05
Barbara	32.349	28.965	3.16

5.4 Image Encryption using Chaotic Map Algorithm

The working of the proposed image encryption method is elaborated in Figure 5.2. The proposed method employs traditional confusion and diffusion architecture which is achieved using substitution and permutation stages.

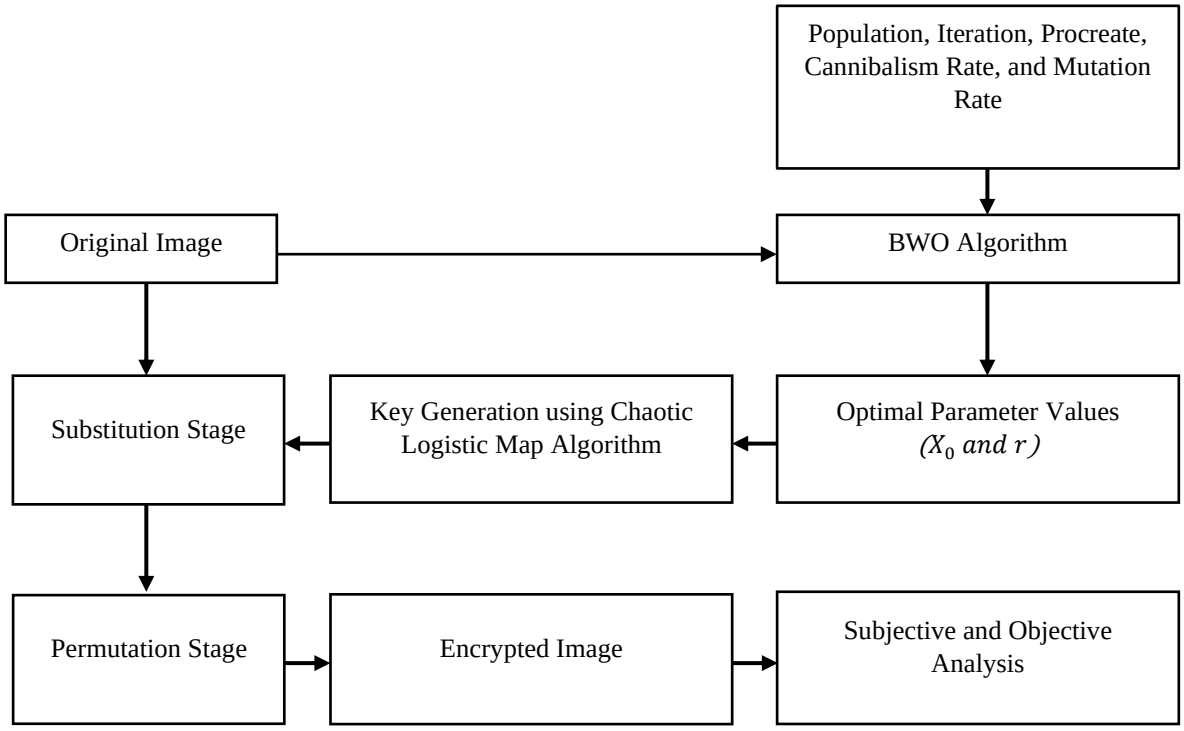


Figure 5.2: Block Diagram of Proposed Image Encryption Method based CLM Algorithm

In substitution stage, exclusive-OR operation is performed between original image pixel and random key. The random key is generated using the chaotic logistic map (CLM) algorithm. The BWO algorithm is used to find the best values for the parameters of a CLM algorithm. The BWO algorithm gives the optimal parameter values based on the objective function. We have designed an objective function based on the entropy parameter. Further, in the permutation stage, circular shifting is performed horizontally and vertically based on two random numbers, K_1, K_2 to get encrypted image. K_1 performs the circular shift row-wise to achieve horizontal permutation, whereas K_2 performs the circular shift column-wise to achieve vertical permutation. The values of K_1, K_2 are determined by how many odd pixels are available in the row and column-wise. Next, subjective and objective analysis of encrypted image is performed to validate its performance over the existing method. In the last, encrypted image along with optimal parameter values of rx_n is communicated to the receiver to decrypt the image.

5.4.1 Determination of Optimal Parameter Values using BWO Algorithm

Here, we have detailed how the BWO algorithm finds the optimal parameter values of the CLM function.

Step 1. In the first step, total number of populations, objective function, iterations, procreate rate, cannibalism rate, and mutation rate are defined.

Step 2. In the second step, initial population of r and x_n is generated in the range of $[3.57 - 4]$ and [0-1]. Therefore, the dimension of each population is 2. The first value represents r and second value x_n.

Step 3. In the third step, fitness evaluation of each population is done based on the objective function and best population is determined as best solution value of r and x_n.

Step 4. In the fourth step, randomly populations are selected to generate new offspring's using procreate step.

Step 5. In the fifth step, generated offspring are added in the initial population. Next, initial population is sorted based on the objective function.

Step 6. In the sixth step, inappropriate population which provides inferior solutions are removed from the population using the cannibalism step.

Step 7. In the seventh step, mutation step is performed randomly to update the population.

Step 8. The whole process of generation is performed until optimal parameter values are found.

5.4.2 Results and Analysis for the Chaotic Logistic Map Algorithm

Table 5.10 shows the input parameter values of BWO algorithm is setup for find the optimal parameters of the chaotic map for random key generation. In the chaotic logistic map, the x_0 value is varied in between 0-1 whereas r parameter value is varied in between 3.57-4. Therefore, the BWO population is initialized in this range. The proposed method is then analyzed on both subjective and objective levels and compared to the current methods in use. The images are taken under consideration for simulation purposes are "*Lena", "Baboon", "Barbara", "Pepper", "Boat", "Airplane", "Cameraman", and "House".*

Table 5.10: Parameter Values of BWO Algorithm for Determine Optimal Parameter Values of CLM Algorithm

Parameter	Values
Population	50
Dimension	2
Iterations	100
Procreate Rate	0.50
Cannibalism Rate	0.50
Mutation Rate	0.1
Lower and Upper Bound Values of x_n and r	(0,1) and (3.57,4)
Objective Function	Entropy

Table 5.11 (a-d) shows the subjective analysis of the image encryption method based on the CLM algorithm. In this analysis, based on the visual quality, original image and its histogram are compared with encrypted image and its histogram. The result shows that encrypted image is completely noisy and histograms are approximate equally distributed.

Table 5.11(a): Subjective Analysis of the Image Encryption Method based CLM Algorithm

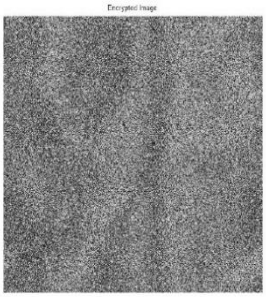
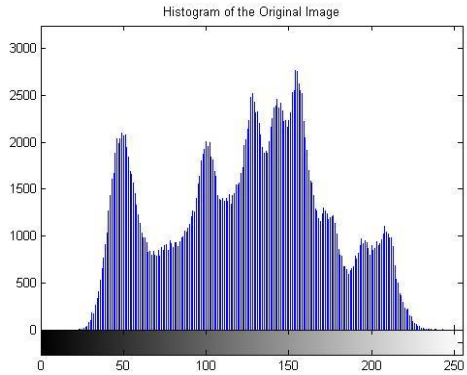
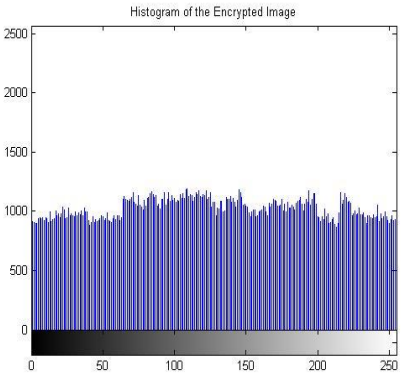
Images	**Original Image**	**Encrypted Image**
Lena		
		

Table 5.11(b): Subjective Analysis of the Image Encryption Method based CLM Algorithm

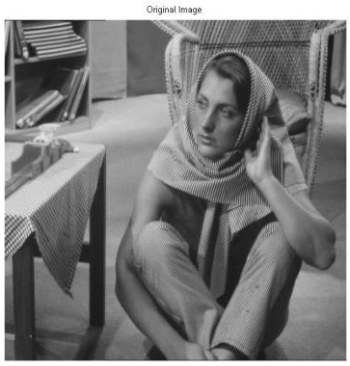
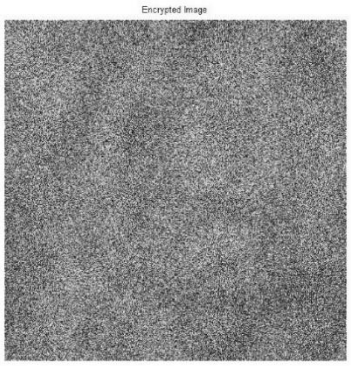
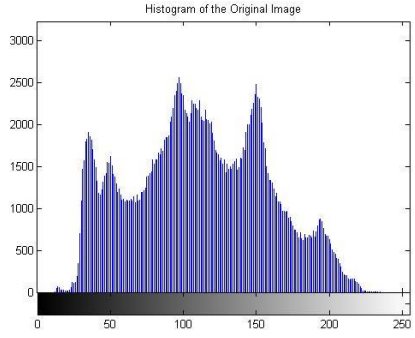
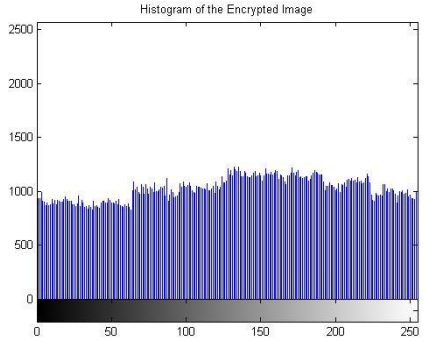
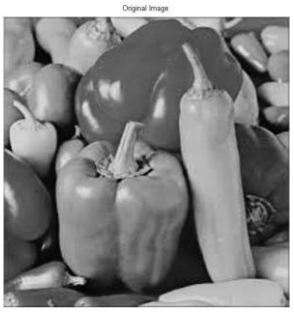
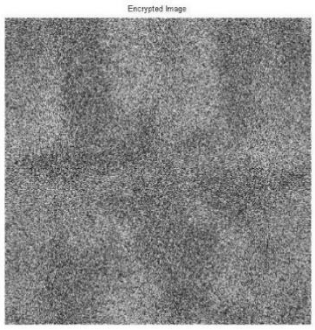
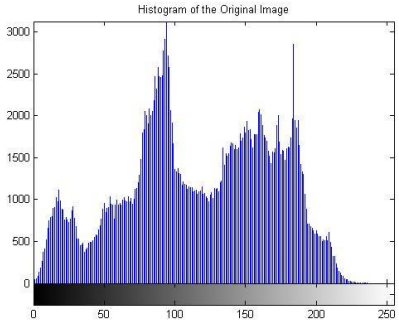
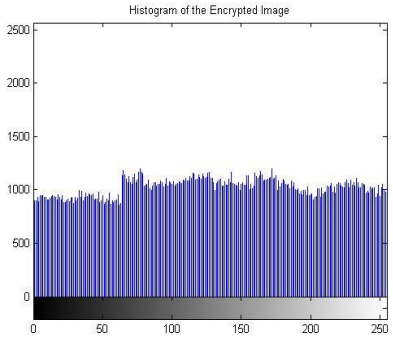
Images	Original Image	Encrypted Image
Barbara		
		
Pepper		
		

Table 5.12(c): Subjective Analysis of the Image Encryption Method based CLM Algorithm

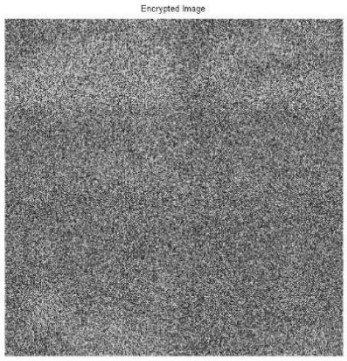
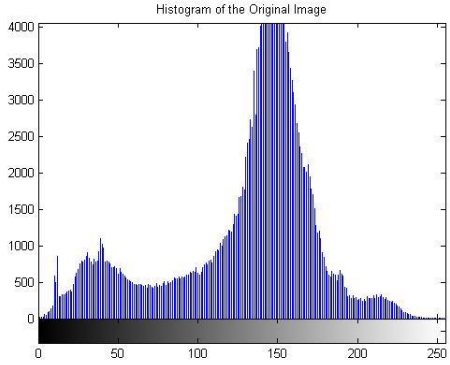
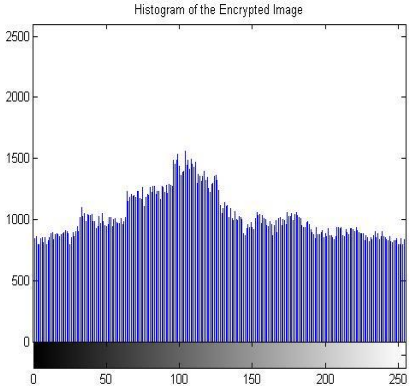
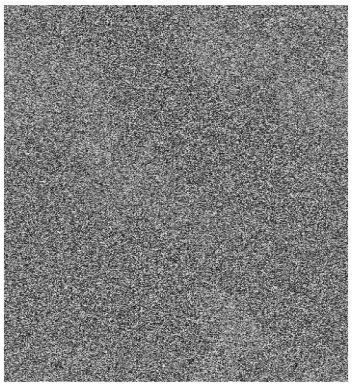
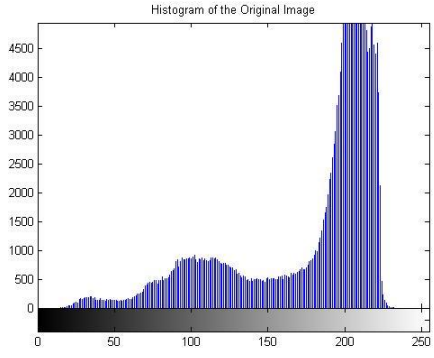
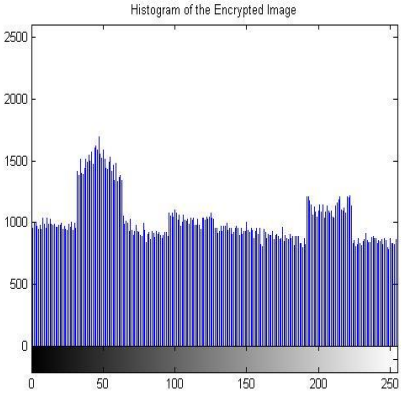
Images	Original Image	Encrypted Image
Boat		
		
Airplane		
		

Table 5.12(d): Subjective Analysis of the Image Encryption Method based CLM Algorithm

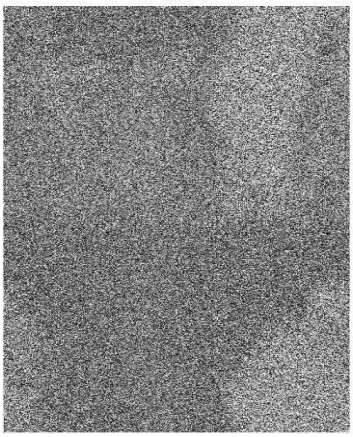
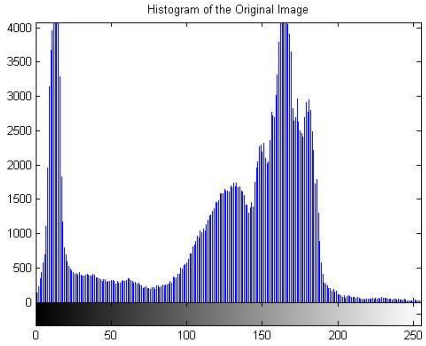
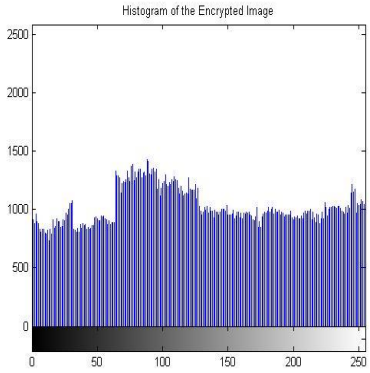
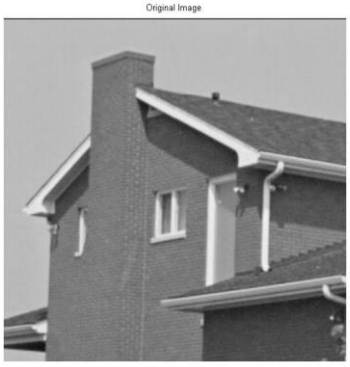
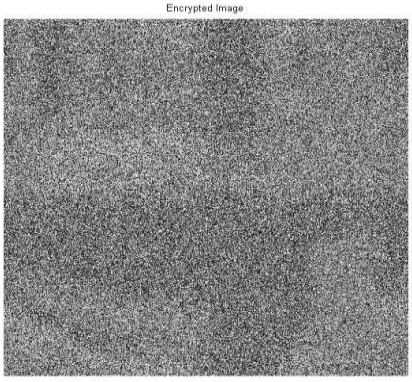
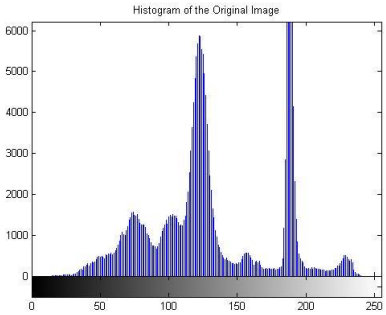
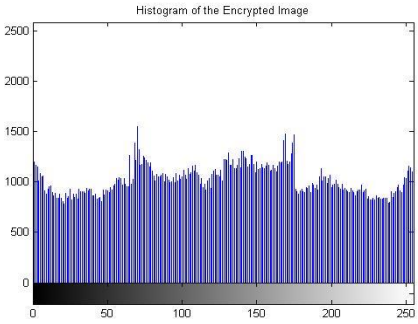
Images	Original Image	Encrypted Image
Cameraman		
		
House		
		

Table 5.12 shows the objective analysis of the proposed method based on the CLM algorithm using various parameters. The parameters are considered for evaluation purposes are entropy, correlation coefficient, MSE, PSNR, maximum deviation, NPCR, execution time, and optimal value of X_0 and r. The result shows that the proposed method achieves high entropy near to ideal value (8) in the grey scale images, low correlation coefficient value near to zero value. Further, low value of PSNR and high value of MSE between original and encrypted image is observed. Next, the result shows that the proposed method achieves maximum deviation and high value of NPCR near to ideal value (100). Further, execution time parameter shows the proposed method takes on average 99.69 seconds for image encryption because in the BWO algorithm, Exclusive-OR operation is needed to perform for complete secret image to determine the objective function. In the last, X_0 and r parameter value shows that it is different for different images. Thus, the generated key is different. Thus, it is difficult for the attacker to retrieve the secret image without knowing the optimal parameter value of X_0 and r.

Table 5.12: Objective Analysis for the Image Encryption Method based CLM Algorithm

Images	**Original Entropy**	**Encrypted Entropy**	**Correlation Coefficient**	**MSE**	**PSNR (in dB)**	**Maximum Deviation**	**NPCR**	**Execution Time (in Seconds)**	X_0	r
Lena	7.4471	7.9955	-0.0067	3.4690e+03	12.7288	1.6418e+05	99.55	98.964900	0.5860	3.8770
Baboon	7.3519	7.9935	-0.0194	3.5503e+03	12.6281	184110	99.62	94.051544	0.6301	3.9281
Barbara	7.4439	7.9925	-0.0123	2.4786e+03	14.1888	174915	99.56	96.423779	0.6623	3.8823
Pepper	7.5733	7.9956	-0.0049	3.1440e+03	13.1560	1.3753e+05	99.58	102.456793	0.1595	3.9281
Boat	7.1763	7.9783	0.0468	3.5926e+03	12.5768	221554	99.58	103.681815	0.6865	3.9378
Airplane	6.7056	7.9754	0.0052	9.6152e+03	8.3012	272608	99.54	104.369682	0.3648	3.9848
Cameraman	7.0853	7.9853	0.0402	3.5343e+03	12.6477	255793	99.55	103.933243	0.5599	3.9385
House	6.4764	7.9860	0.0010	4.4086e+03	11.6878	271515	99.55	93.659861	0.3890	3.9293

5.4.3 Comparative Analysis of the Proposed Image Encryption Method based on Chaotic Logistic Map Algorithm with the Existing Encryption Methods

Table 5.13-5.14 show the comparative analysis between the proposed method and the existing methods based on entropy and number of pixel change rate. The results reveal that the proposed method achieves superior results over Shelza Suri and Ritu Vijay [43] and achieves approximately closer values to Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [41].

Table 5.13: Comparative Analysis of Proposed Image Encryption Method based on CLM Algorithm and Existing Methods based on based on Entropy Parameter

Images	**Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [41]**	**Shelza Suri and Ritu Vijay [43]**	**Proposed Method**
Lena	7.9815	7.82200	7.9869
Baboon	7.9839	-	7.9816
Pepper	7.9857	-	7.9873
Boat	7.9784	-	7.9698
Cameraman	7.9893	7.79944	7.9779
Coin	-	7.80898	7.9765
Rice	-	7.82904	7.9461

Table 5.14: Comparative Analysis of Proposed Image Encryption Method based on CLM Algorithm and Existing Methods based on based on NPCR Parameter

Images	**Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [41]**	**Shelza Suri and Ritu Vijay [43]**	**Proposed Method**
Lena	99.5918	99.2188	99.4751
Baboon	99.6027	-	99.5361
Pepper	99.6409	-	99.9920
Boat	99.6265	-	99.5300
Cameraman	99.6171	99.5117	99.9920
Coin	-	99.5117	99.4202
Rice	-	99.5117	99.3041

5.5 Conclusion

In this chapter, two image encryption methods are proposed based on the BWO algorithm. In the first method, the BWO algorithm and its mutation operation are used for image encryption, whereas in the second method, the BWO algorithm determines the optimal parameter values of the CLM algorithm. The simulation evaluation of both methods is done using subjective and objective analysis. The subjective analysis shows that the encrypted image is completely noisy and the histograms are equally distributed. On the objective analysis, various performance metrics are measured that make it robust against various attacks such as statistical and differential attacks. Finally, the comparative analysis shows that the proposed encryption method provides superior results.

Chapter 6

Privacy-Preserving Method based on Hybridization of Cryptography and Steganography Algorithms

6.1 Introduction

In this chapter, an optimal privacy-preserving method is designed to secure the people's information using bio-inspired black widow optimization (BWO) algorithm. The attractiveness of the presented method is that it uses the BWO algorithm for encryption as well as hiding the data in the steganography in the optimal way. Three processes—procreation, cannibalism, and mutation [79]—are used by the BWO algorithm to arrive at the best possible outcomes for key generation, secret data index, and cover image starting pixel. For the encryption purposes, key generation is done using BWO algorithm then performed the exclusive-OR operation with sensitive data. After that, used the BWO algorithm to determine the optimal secret data index and starting pixel in the cover image then hiding in the cover image using the LSB algorithm. Besides that, pre-processing of the cover image is done to choose the most optimal plane for hiding the information.

The rest of the chapter is organised into five sections. Section 2 gives the detailed description of how cover image plane is selected for data hiding purposes. Section 3 explains the proposed privacy-preserving method is designed by hybrid the cryptography and steganography method. Further, in this section, the comprehensive explanation of key generation and how optimal secret data index and starting pixel is determined in the cover image using BWO algorithm is given. Finally, the results are given along with their analysis and subsequently the conclusions are drawn in Section 4-5.

6.2 Cover Image Plane Selection

In the proposed privacy-preserving method, optimal cover image selection is done before hiding the secret data in it. In the literature, cover image plane selection is done based on the human visual system (HVS) characteristics [2, 62, 92]. According to the HVS characteristics,

human eyes are more sensitive to green color over the blue color. Thus, blue plane is chosen for data hiding purposes. The limitation of selecting cover image plane based on HVS characteristics is that the selected plane is fixed for data hiding. Further, if the blue plane is the most dominant color over other planes, then data hiding in it generates distortions which negatively impact the imperceptibility parameter. These challenges are taken under consideration while choosing the optimal cover image plane selection.

In the proposed method, the pre-processing on the cover image planes is done to determine which plane plays minimum or maximum role in it. To achieve this goal, the cover image plane is categorized into three classes, namely, superior, intermediate, and inferior based on their pixel intensity value. The categorization of planes based on the pixel intensity value is successfully done in the enhancement methods [93]. The plane which plays minimum role in the cover image is chosen for data hiding purposes. Therefore, the pixel intensity of the RGB plane of the cover image is determined using Eq. (6.1-6.3) [93].

$$Sum(P_{red}) = \sum_{m=1}^{A} \sum_{n=1}^{B} P_{red}(m,n) \tag{6.1}$$

$$Sum\left(P_{green}\right) = \sum_{m=1}^{A} \sum_{n=1}^{B} P_{green}(m,n) \tag{6.2}$$

$$Sum(P_{Blue}) = \sum_{m=1}^{A} \sum_{n=1}^{B} P_{Blue}(m,n) \tag{6.3}$$

Here, $P_{red}, P_{green}, and\ P_{blue}$ denotes the pixel values of the RGB plane, and A, B denote the size of the images.

6.3 Proposed Privacy-Preserving Method

The main motive of the proposed privacy-preserving method is to use the bio-inspired black widow optimization (BWO) algorithm for data encryption as well as optimized data hiding in the cover image. The BWO algorithm generates the optimal random key, secret data index, and starting pixel in the cover image based on the objective function. The block diagram of the proposed privacy-preserving method is shown in Figure 6.1. Initially, secret data is read. In the proposed method, DICOM images are taken as secret data which contains patient's personal information along with medical images generated due to medical scan, namely, MRI, ultrasound [94]. After that, secret data is split into sensitive and non-sensitive data. The sensitive data contains the information of the patient's personal information whereas non-sensitive data contains medical image information. The sensitive data is encrypted by performing the exclusive-OR operation with random key. The random key is generated using

the BWO algorithm based on the objective function. In our work, entropy is taken as the objective function. It is calculated using Eq. (6.4). Next, encrypted sensitive data and non-sensitive data is concatenated and given as secret data to the steganography method.

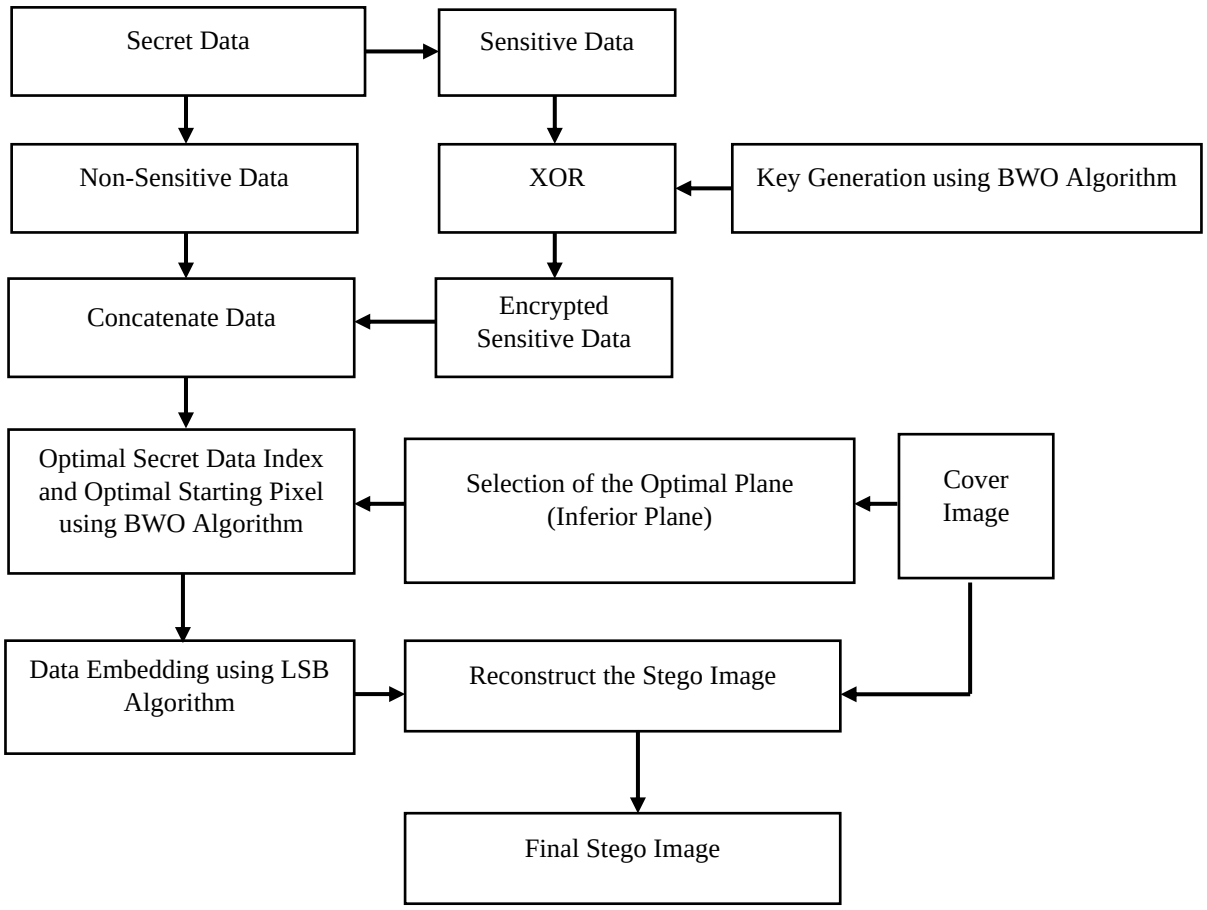


Figure 6.1: Block Diagram of the Proposed Privacy-Preserving Method

$$E = \sum_{i=1}^{n} -p_i \log p_i \tag{6.4}$$

In the steganography method, the secret data along with optimal cover plane that is chosen based on the pixel intensity value is given to the BWO algorithm. The BWO algorithm determines the optimal secret data index and starting pixel in the cover image plane for hide the secret data in optimal way. After determining the optimal index information, it is given to the data embedding algorithm. The data embedding based on the index information, hides the secret data in the cover image plane in the optimal way and gives the stego image. The final stego plane is reconstructed by concatenating the stego image generated after data hiding and other planes (intermediate and superior plane) of the cover image. Finally, the stego image along with secret data index, starting pixel in the cover image, optimal cover image plane index, random key are communicated to the receiver to retrieve the encrypted data from the cover image and decrypt it by performing the exclusive-OR operation with random key.

6.3.1 Key Generation using BWO Algorithm

The following steps are taken for key generation using the BWO algorithm.

1. Initially, define the size of the key, objective function, number of iterations, number of black widows, procreate, cannibalism, and mutation rate.
2. Next, initialize the black widow population matrix ($B \times D$). B represents the total number of black widows and D represents the dimension of each black widow.
3. After that, the fitness evaluation of each black widow is done based on the objective function to determine the initial best key.
4. Further, randomly $B/2$ black widows are selected as parents to generate offspring using procreate steps. Next, the fitness function is evaluated for generated offspring. Further, according to the fitness function, inadequate optimal solutions are removed using the cannibalism step and the population matrix is updated.
5. The mutation step is applied to the population matrix to generate a new solution after performing the procreate and cannibalism steps.
6. 3-5 steps are repeated until the stopping condition is not met to determine the optimal key.

6.3.2 Optimal Secret Data Index and Starting Pixel in the Cover Image using BWO Algorithm

The following steps are taken for optimal data hiding in the cover image using the BWO algorithm.

- Initially, the cover image and secret data matrix is read ($M \times N$) and transformed into a vector ($1 \times K$). The value of the K equal to $M \times N$.
- Next, the black widow population matrix ($B \times D$) is initialized. B represents the total number of black widows and D represents the dimension of each black widow. In the proposed method, the value of D is 2. The first value represents the optimal starting pixel in the cover image and the second value represents the secret data index. The possible secret data index value and its description are shown in Table 6.1.
- The fitness function is evaluated for each black widow using the MSE parameter and the initial optimal solution is determined.
- After that, randomly $B/2$ black widows are selected as parents to generate offspring using procreate steps. Next, the fitness function is evaluated for generated offspring.

Table 6.1: Secret Data Index Value and its Description

Secret Data Index Value	Description
0	No Operation on the Secret Data
1	Circular Shifting
2	Flipping the Secret Data
3	Reverse the Secret Data

- Further, according to the fitness function, inadequate optimal solutions are removed using the cannibalism step and the population matrix is updated.
- The mutation step is applied to the population matrix to generate a new solution after performing the procreate and cannibalism step.
- 3-5 steps are repeated until the stopping condition is not met to determine the optimal solution.
- In the step, based on the optimal solution, the secret data is embedded in the cover image to generate a stego image.
- In the last, the stego image vector $(1 \times K)$ is transformed into a matrix $(M \times N)$ to generate a stego image matrix. The stego image along with an optimal solution (optimal starting point and secret data index) information is communicated to the receiver.

6.4 Results and Analysis

This section shows the simulation results of the proposed method and comparative analysis with the existing methods. Table 6.2 (a-b) shows the parameter values as taken under consideration for key generation, optimal secret data index, and starting pixel in the cover image using the BWO algorithm. In the parameters, objective function plays an important role. Therefore, objective function is selected carefully for key generation (entropy) and optimized data hiding (mean square error).

Table 6.2 (a): Parameter Values of BWO Algorithm in the Proposed Privacy-Preserving Method for Key Generation

Sr No.	**Parameter**	**Value**
1.	Objective Function for Key	Entropy
2.	Key Size (in Byte)	64
3.	Lower Limit	0
4.	Upper Limit	255
5.	Iterations	50

Table 6.2 (b): Parameter Values of BWO Algorithm in the Proposed Privacy-Preserving Method for Optimal Secret Data Index and Starting Pixel in the Cover Image

Sr No.	**Parameter**	**Value**
1.	Objective Function for Data Hiding	MSE
2.	Iterations	20
3.	Total Population (pop)	50
4.	Procreate Rate	Pop/2
5.	Cannibalism Rate	Pop/2
6.	Mutation Rate	50%
7.	Cover Image	512X512
8.	Secret Data (in bits)	512X512
9.	Data Hiding Method	LSB
10.	Secret Data Index	$[0-3]$
11.	Optimal Starting Pixel	$[1-N]$ $N=(row\times col)$

Table 6.3: Selected Plane, Optimal Starting Pixel, and Secret Data Index for Proposed Privacy-Preserving Method

Images	Selected Plane	Cover Index	Secret Index
Lena	2	45854	0
Barbara	3	212409	0
Baboon	3	136435	0
Pepper	3	189674	2
Female	3	137206	1
Couple	3	238113	1
House	2	89662	3
Aeroplane	1	159071	2
Jellybeans	3	92894	3
Splash	2	66685	3

Next, Table 6.3 shows the selected plane that is determined based on the pixel intensity value. Further, this table shows the optimal starting pixel and secret data index that are determined using the BWO algorithm. In the simulation analysis, 10 cover images are taken under consideration. The result shows that the selected cover image plane, optimal starting pixel, and secret data index is not fixed. Thus, the proposed method enhances security because it is difficult for the attacker to determine which cover image plane contains the secret data. Further, from which pixel starting pixel data hiding is performed and what optimal index of the secret data.

Table 6.4 (a-b) shows the subjective analysis of the proposed privacy-preserving method. The subjective analysis is performed between selected cover image plane and stego image plane is generated after optimized data hiding. The result shows that the images look similar. This reflects that the stego image contains minimum distortion after data hiding and provides better imperceptibility. Thus, the proposed privacy-preserving method gives no indication to the attacker is that some secret information is communicating through stego images

Table 6.4 (a): Subjective Analysis of the Proposed Privacy-Preserving Method

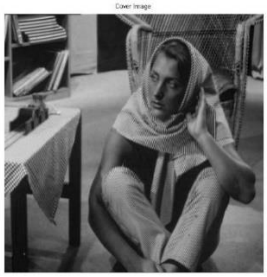
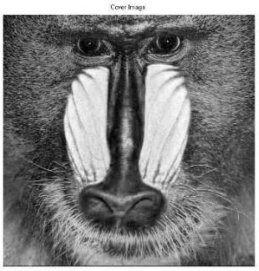
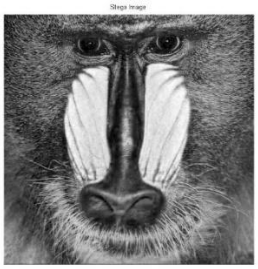
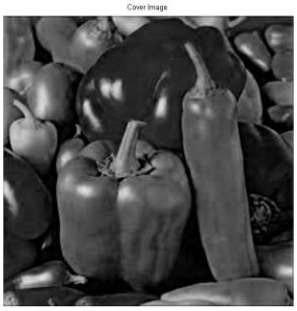
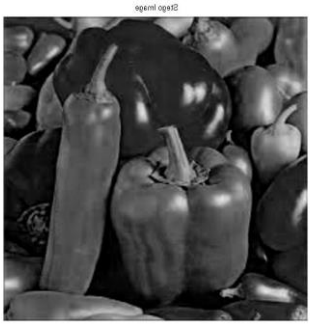
Images	Cover Image	Stego Image
Lena		
Barbara		
Baboon		
Pepper		

Table 6.4 (b): Subjective Analysis of the Proposed Privacy-Preserving Method

Images	Cover Image	Stego Image
Female		
Couple		
Airplane		
Cameraman		
Boat		

Table 6.5 shows the objective analysis of the proposed privacy-preserving method in terms of CC, SSIM, entropy, MSE, RMSE, PSNR, IF, NAE, and UIQI for different cover images are taken under consideration. The result indicates that the proposed privacy-preserving method achieves a high value near to one for CC, SSIM, IF, and UIQI. On the other hand, the proposed method achieves similar entropy between input and output images. Finally, the proposed method achieves the high PSNR due to the lower error between the input and output images. The error matrices are determined using the MSE, RMSE, and NAE.

Table 6.5: Objective Analysis of the Proposed Privacy-Preserving Method

	CC	**SSIM**	**Input Entropy**	**Output Entropy**	**MSE**	**RMSE**	**PSNR**	**IF**	**NAE**	**UIQI**
Lena	0.9999	0.9961	7.5909	7.5914	0.2491	0.4991	54.1675	0.999980	0.002515	1.000000
Barbara	0.9999	0.9969	7.515	7.5158	0.2476	0.4976	54.1939	0.999978	0.002648	0.999649
Baboon	0.9999	0.9987	7.7614	7.7637	0.2483	0.4983	54.1808	0.999985	0.002186	1.000000
Pepper	0.9999	0.9951	7.1613	7.1774	0.2406	0.4905	54.3184	0.999961	0.003698	0.999101
Female	0.9998	0.9945	6.8834	6.8845	0.2459	0.4959	54.2226	0.999932	0.005299	1.000000
Couple	0.9997	0.9941	6.2105	6.2119	0.2486	0.4986	54.1755	0.999844	0.008988	1.000000
House	0.9999	0.9949	6.5354	6.5548	0.2502	0.5002	54.1472	0.999985	0.001882	0.999696
Aeroplane	0.9999	0.9957	6.7489	6.7531	0.2483	0.4983	54.1802	0.999985	0.001398	1.000000
Jellybeans	0.9999	0.9942	6.5953	6.6130	0.2520	0.5020	54.1171	0.999985	0.001768	1.000000
Splash	0.9999	0.9944	6.9771	6.9934	0.2395	0.4894	54.3381	0.999972	0.003396	1.000000

The result reflects that the parameters, namely, CC, SSIM, IF, and UIQI, achieve the value approximate near to 1, which is required in the image steganography, as shown in Figure 6.2.

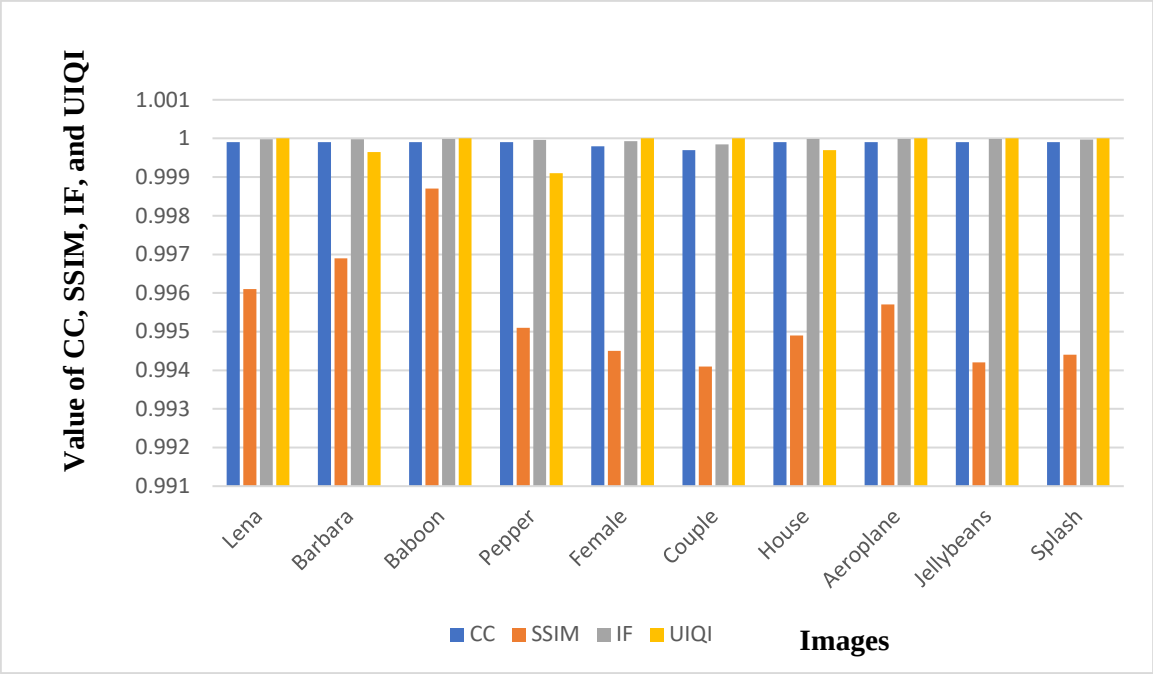


Figure 6.2: Performance Evaluation of the Proposed Method based on CC, SSIM, IF, and UIQI Parameter

Further, input and output entropy is determined for different images is almost similar, which reflects that the pixel distribution remains similar after data hiding, as shown in Figure 6.3.

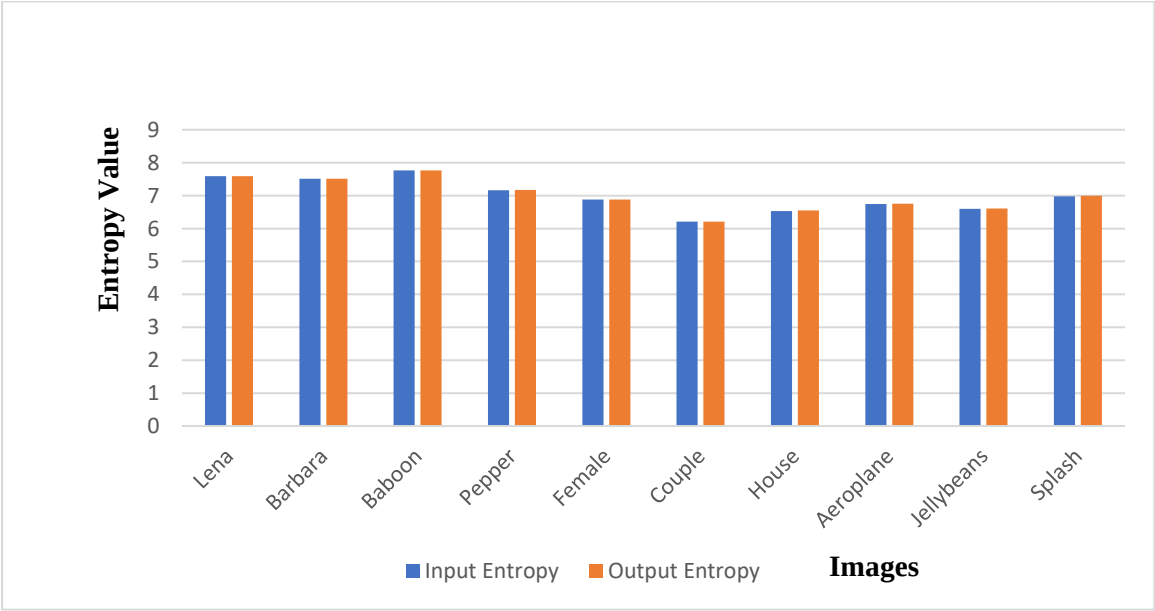


Figure 6.3: Performance Evaluation of the Proposed Method based on Input and Output Entropy

Next, MSE, RMSE, and NAE parameters value near to 0 value, as shown in Figure 6.3. This reflects that the error between cover and stego image is minimum. Thus, the proposed model achieves the desired PSNR value.

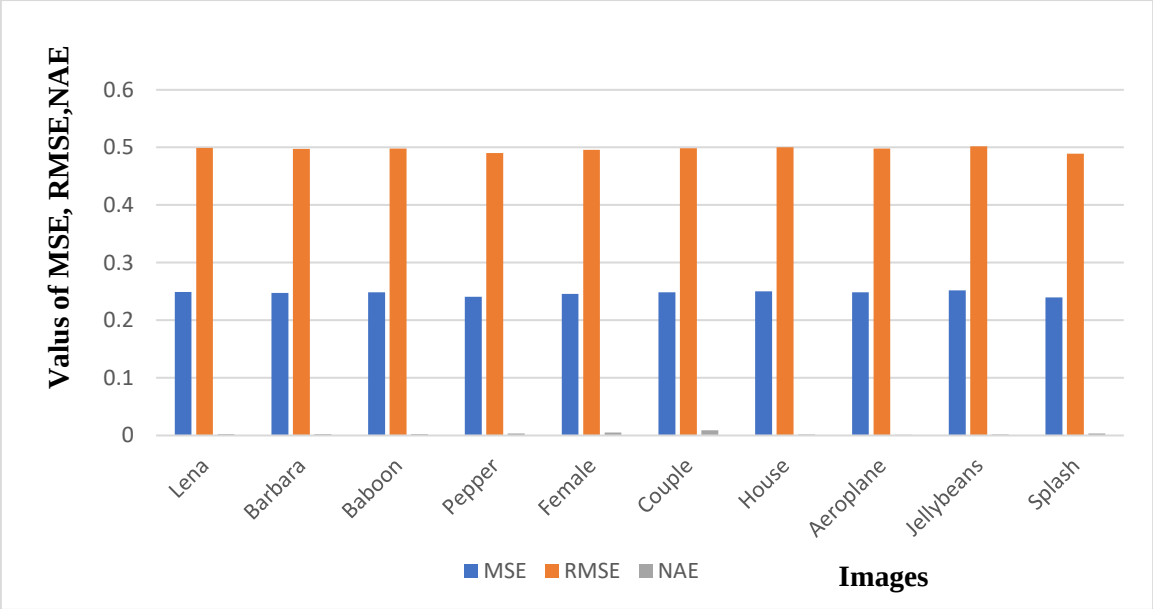


Figure 6.4: Performance Evaluation of the Proposed Method based on MSE, RMSE, NAE

Finally, the presented method is compared with the existing optimized data hiding methods based on the PSNR parameter for the same secret and cover image sizes, in Table 6.6. The results reveal that the presented method is better than existing methods developed by Aman Banharnsakun [56] and Kanan et al. [51] with a PSNR of 57.22 dB compared to 56.39 dB and 47.23 dB, respectively.

Table 6.6: Comparative Analysis with the Proposed Privacy-Preserving Method

		PSNR (in dB)	
Optimization Technique		**ABC**	**BWO**
Secret Image (128 X128)	**Cover Image (512X512)**	**Aman Banharnsakun [56]**	**Proposed Method**
	Lena.jpg	56.40	57.20
	Jet.jpg	56.39	57.24
	Lake.jpg	56.40	57.22
	Elaine.jpg	56.36	57.21
	Baboon.jpg	56.39	57.22
	Average	**56.39**	**57.22**

Optimization Technique		GA	BWO
Secret Image (256X256)	**Cover Image (512X512)**	**Kanan et al. [51]**	**Proposed Method**
	Lena.jpg	45.12	47.19
	Jet.jpg	45.18	47.17
	Pepper.jpg	45.13	47.36
	Sailboat.jpg	45.10	47.20
	Baboon	45.12	47.22
	Average	**45.13**	**47.23**

6.5 Conclusion

In this chapter, a privacy preserving method is designed by hybridizing the cryptography and steganography algorithms. The key benefit of the presented method is that the bio-inspired black widow optimization algorithm is used for encryption and optimized data hiding. The BWO algorithm performs three operations, namely, procreate, cannibalism, and mutation to determine the optimal key generation and to determine the optimal secret data index and starting pixel in the cover image. Besides that, the pre-processing the cover image is done to determine the best plane over other planes for data hiding based on the pixel intensity value of the cover image planes. Out of all planes, the plane that has minimum pixel intensity value is chosen as data hiding plane. Further, the other advantage of the presented method is that in place of encrypting the entire secret information, only sensitive information is encrypted. The result and analysis part shows that the cover image plane, secret data index, and starting pixel in the cover image is not fixed. Thus, it is difficult for the attacker to determine which plane contains the secret information. Further, the subjective analysis and objective analysis show that the cover and stego image are similar in terms of their visual quality; the low value of MSE, RMSE, and NAE is near 0; the input and output entropy of the different images is approximate similar; and a high value of CC, SSIM, UIQI, and IF near 1 is achieved for the proposed method. Finally, the PSNR-based comparison demonstrates that the suggested strategy is superior to the existing optimization techniques.

Chapter 7

Conclusions

7.1 Key Contributions & Findings

The key contributions and the findings of the work in the thesis are given below:

- Image steganography methods are proposed based on two swarm intelligence algorithms, namely, EVO and GHO. In the first method, the swarm intelligence algorithms are used for determining the optimal cover image, block order index, and secret data index before performing the hiding process in the cover image using the "LSB algorithm". In the second method, the secret data bits are matched with the *k*-LSB bits of the cover image pixel, and a matched index is determined. Following this, the matched index is concealed in the cover image using the 2-bit LSB algorithm by determining the optimal starting pixel in the cover image using the EVO and GHO algorithms. The simulation evaluation is performed for grey-scale and color images. Further, single-bit, and multi-bit data embedding is done. The subjective analysis shows that input ("cover") and output ("stego") images are very similar, whereas the objective analysis reveals that the proposed method achieves a better PSNR than the existing methods. Besides that, the cover image, block order index, and secret data index are not fixed, which enhances the security parameter because it is tough for the attacker to extract the secret data. The superior performance of the proposed image steganography methods is due to the fact that EVO and GHO algorithms have better exploration rates enabling it to find the optimal solution better.
- An evolutionary optimization algorithm, namely, "Black Widow Optimization (BWO)" has been employed to propose image steganography method where the inappropriate solutions are hidden and the secret data is concealed in the most optimal way possible. The algorithm searches the optimal cover image, block order, and secret data index by minimizing the objective function to enhance the imperceptibility parameter. The simulation evaluation of the method is presented with the simulation setup configuration followed by subjective and objective analysis, and comparative analysis. Thus, it is observed that BWO algorithm removes the inappropriate solutions while

exploring the solution space, making it reach the optimal solution with a better population.

- In the matching method, the matching is performed between secret data bits and cover image pixels on the LSB side because matching all pixel bits of the cover image with secret data, negatively impacts the payload capacity. Further, the security of the image steganography method is enhanced because optimal starting pixel index knowledge are required on the receiver side to retrieve the original secret data from the stego image.
- Two image encryption methods have been proposed by generating the random keys based on the Black Widow Optimization (BWO) algorithm. In the first method, the BWO algorithm is used for key generation based on the “objective function”, where the "mutation" operation is used in the encryption process. The second method proposed is based on the chaotic function whose output is extremely sensitive to the input parameter values, thus, the optimal selection of parameter values enhances the security of the image encryption method. Entropy is utilized as an objective function in both methods. Performance metrics are measured that make it robust against various attacks.
- The preserving-preserving method, the same bio-inspired BWO algorithm is used for proposition of a hybridized method utilizing both image encryption and optimized data hiding. The privacy-preserving method is intended to secure people's sensitive and non-sensitive information. The sensitive information is encrypted by performing an exclusive-OR operation with a random key. The sensitive and non-sensitive information are concatenated and are embedded in the cover image in an optimal way using LSB algorithm. The advantage of the presented privacy preserving method is that the same bio-inspired BWO algorithm is used for image encryption and optimized data hiding. We have also worked on the color cover images, and selected the most optimal cover plane for the data hiding. The intensity value of each pixel is used to determine which plane contributes the least to the overall cover image, and that plane is the one chosen for the final step of the plane selection process. The subjective analysis has shown that the stego image is indistinguishable from the cover image. The objective analysis shows the cover image plane, secret data index, and optimal starting pixel in the cover image are not static, thus enhancing security.

7.2 Limitations of the Work

A certain number of limitations on the bio-inspired algorithms resulting from their implementations that impact the performance of the proposed image steganography and cryptography algorithms are given below:

- In the EVO and GHO algorithms, a random population is chosen to generate a new population by performing three operations, i.e., hitting with a pebble, rolling with twigs, and changing the angle in the EVO algorithm, whereas baiting, changing position, and attracting a prey swarm in the GHO algorithm. If these operations do not produce a population that is superior to the chosen population, no population is removed from the initial population array. Thus, there are chances that the same population may be chosen in the next iteration while searching the solution space.
- In case of BWO, the procreation, cannibalism, and mutation rates need to be defined carefully because if this rate is increased for searching the solution space, then it increases computation time to search for the optimal solution.
- Initial populations for bio-inspired algorithms are generated arbitrarily using the *rand* function. This function produces populations that have a high degree of unpredictability inside the solution space but are not necessarily distributed equally across the solution space. As a result, the population search occasionally tedious, and the algorithm lacks diversity.
- The secret data index determination using a bio-inspired algorithm makes it applicable to only the 1-bit LSB method.

7.3 Scope for Future Work

Based on the work that has been presented in this thesis, the following pointers of future work could be listed as follows:

- In the presented methods, a single objective function is considered in the image encryption and steganography methods, that improves the single security characteristic. In the future, multi-objective functions will be designed to enhance the multiple characteristics of security.
- In the presented methods of steganography and encryption methods, a few parameters need to communicate from the transmitter side to decrypt on the receiver side. In the

future, a security method can be designed to securely communicate this reference information with the receiver.

- In this thesis, only one imperceptibility parameter of image steganography is enhanced using the bio-inspired optimization algorithm. The other parameters, namely, payload and robustness, could possibly be enhanced by adding the data compression and error correction code to the steganography method.
- In the image encryption method, the optimal parameter values are determined using the BWO algorithm for the chaotic logistic map algorithm. However, in the literature, numerous image encryption methods are available, such as DNA, ECC, and cellular automata. So, the bio-inspired algorithm could be used to find the best parameter values for these encryption methods.

References

[1] Shyam Nandan Kumar, "Review on network security and cryptography," *International Transaction of Electrical and Computer Engineers System,* vol. 3, no. 1, pp. 1-11, 2015.

[2] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[3] Padate, Roshni, and Aamna Patel, "Encryption and decryption of text using AES algorithm," *International Journal of Emerging Technology and Advanced Engineering*, vol. 4, no. 5, pp. 54-9, May 2014.

[4] Rabah, Kefa, "Theory and implementation of data encryption standard: A review," *Information Technology Journal*, vol. 4, no. 4, pp. 307-325, 2005.

[5] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, Oct. 2012, doi: 10.1016/j.aeue.2012.01.015.

[6] Gupta, Aaditya, Richa Thawait, K. Abhimanyu Kumar Patro, and Bibhudendra Acharya, "A novel image encryption based on bit-shuffled improved tent map," *Int J Control Theory Appl* 9, no. 34 (2016): 1-16.

[7] P. P. Deepthi, D. S. John, and P. S. Sathidevi, "Design and analysis of a highly secure stream cipher based on linear feedback shift register," *Computers & Electrical Engineering*, vol. 35, no. 2, pp. 235–243, Mar. 2009, doi: 10.1016/j.compeleceng.2008.06.005.

[8] P.-C. Lin and S. Khatri, "VLSI Implementation of a Non-Linear Feedback Shift Register for High-Speed Cryptography Applications," Accessed: Jan. 11, 2023. [Online]. Available: https://people.engr.tamu.edu/sunilkhatri/projects-web/papers/nlfsr.pdf

[9] L. Dongjiang, W. Yandan, and C. Hong, "The Research on Key Generation in RSA Public-Key Cryptosystem," *2012 Fourth International Conference on Computational and Information Sciences*, Aug. 2012, doi: 10.1109/iccis.2012.348.

[10] M. Vasim Ahamad, M. Urrahman Siddiqui, M. Masroor, and U. Fatima, "An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret

Key," *International Journal of Engineering & Technology*, vol. 7, no. 4.5, p. 347, Sep. 2018, doi: 10.14419/ijet.v7i4.5.20104.

[11] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, Jul. 2018, doi: 10.1016/j.image.2018.03.012.

[12] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008, doi: 10.1109/tifs.2008.926097.

[13] N. Hitaswi and K. Chandrasekaran, "A bio-inspired model to provide data security in cloud storage," *2016 International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds*, Oct. 2016, doi: 10.1109/incite.2016.7857617.

[14] H.-C. Huang, F.-C. Chang, Y.-H. Chen, and S.-C. Chu, "Survey of Bio-inspired Computing for Information Hiding," *Journal of Information Hiding and Multimedia Signal Processing c*, vol. 6, no. 3, 2015, Accessed: Jan. 11, 2023. [Online]. Available: http://bit.kuas.edu.tw/~jihmsp/2015/vol6/JIH-MSP-2015-03-003.pdf

[15] A. Darwish, "Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications," *Future Computing and Informatics Journal*, vol. 3, no. 2, pp. 231–246, Dec. 2018, doi: 10.1016/j.fcij.2018.06.001.

[16] M. Črepinšek, S.-H. Liu, and M. Mernik, "Exploration and exploitation in evolutionary algorithms," *ACM Computing Surveys*, vol. 45, no. 3, pp. 1–33, Jun. 2013, doi: 10.1145/2480741.2480752.

[17] G. Kessler, "An Overview of Cryptography An Overview of Cryptography," 1998. [Online]. Available: https://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pdf

[18] M. Kaur, S. Singh, and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review," *Mathematical Problems in Engineering*, vol. 2021, p. e5012496, Jul. 2021, doi: 10.1155/2021/5012496.

[19] Z. Pourmirza, S. Walker, and J. Brooke, "Data reduction algorithm for correlated data in the smart grid," *IET Smart Grid*, Feb. 2021, doi: 10.1049/stg2.12010.

[20] Raju, K. Upendra, and N. Amutha Prabha, "A review of reversible data hiding technique based on steganography," *ARPN Journal of Engineering and Applied Sciences*, vol. 13, no. 3, pp.1105-1114, Feb. 2018.

[21] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727-752, 2010.

[22] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14867–14893, May 2015, doi: 10.1007/s11042-015-2671-9.

[23] M. N, N. Siddiqa, and T. H. Sardar, "Multi-Layered Security System Using Cryptography and Steganography," *International Journal of Innovative Research in Computer Science & Technology*, vol. 7, no. 2, pp. 8–11, Mar. 2019, doi: 10.21276/ijircst.2019.7.2.1.

[24] H. E. Rostam, H. Motameni, and R. Enayatifar, "Privacy-preserving in the Internet of Things based on steganography and chaotic functions," *Optik*, vol. 258, p. 168864, May 2022, doi: 10.1016/j.ijleo.2022.168864.

[25] T. Jambhale and M. Sudha, "A Privacy Preserving Hybrid Neural-Crypto Computing-Based Image Steganography for Medical Images," *Intelligent Data Communication Technologies and Internet of Things*, pp. 277–290, 2021, doi: 10.1007/978-981-15-9509-7_24.

[26] A. DANLAMI MOHAMMED, O. A. OJERINDE, M. FOLORUNSHO VICTOR, and M. OGBUKA KENNETH, "Privacy Preservation in Big Data Application using Advanced Encryption Standard and Least Significant Bit Steganography," *i-manager's Journal on Information Technology*, vol. 9, no. 2, p. 1, 2020, doi: 10.26634/jit.9.2.17550.

[27] O. Hosam and M. H. Ahmad, "Hybrid design for cloud data security using combination of AES, ECC and LSB steganography," *International Journal of Computational Science and Engineering*, vol. 19, no. 2, p. 153, 2019, doi: 10.1504/ijcse.2019.100236.

[28] Binitha, S., and S. Siva Sathya, "A survey of bio inspired optimization algorithms," *International journal of soft computing and engineering* 2, no. 2 (2012): 137-151.

[29] J. Brownlee, "What Does Stochastic Mean in Machine Learning?," *MachineLearningMastery.com*, Nov. 17, 2019. https://machinelearningmastery.com/stochastic-in-machine-learning/#:~:text=For%20example%2C%20a%20deterministic%20algorithm (accessed Jan. 07, 2023).

[30] M. Kaur, S. Singh, M. Kaur, A. Singh, and D. Singh, "A Systematic Review of Metaheuristic-based Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol.29, pp. 2563-2577, Oct. 2021, doi: 10.1007/s11831-021-09656-w.

[31] P. Game and V. Vaze, "Bio-inspired Optimization: metaheuristic algorithms for optimization," NTCOMIS-2020. Accessed: Jan. 11, 2023. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/2003/2003.11637.pdf

[32] Can, Ümit, and Bilal Alataş, "Physics based metaheuristic algorithms for global optimization," 2015.

[33] "Math 407 Definitions : Sections 1-3." [Online]. Available: https://sites.math.washington.edu/~burke/crs/407/PS/defn1-3.pdf

[34] "Nature-Inspired Optimization Algorithms | ScienceDirect," *www.sciencedirect.com*. https://www.sciencedirect.com/book/9780128219867/nature-inspired-optimization-algorithms (accessed Sep. 27, 2021).

[35] A. D. Bull, "Convergence rates of efficient global optimization algorithms," *arXiv:1101.3501 [math, stat]*, Oct. 2011, Accessed: Jan. 16, 2023. [Online]. Available: https://arxiv.org/abs/1101.3501#:~:text=Efficient%20global%20optimization%20is%20the

[36] Patel, Komal D., and Sonal Belani, "Image encryption using different techniques: A review," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, no. 1, pp. 30-34, 2011.

[37] V. G, D. S, and M. M, "AES Based Algorithm for Image Encryption and Decryption," *Perspectives in Communication, Embedded-systems and Signal-processing - PiCES*, vol. 2, no. 11, pp. 342–345, Mar. 2019, Accessed: Jan. 11, 2023. [Online]. Available: http://pices-journal.com/ojs/index.php/pices/article/view/161

[38] Gupta, Ritu, and Anchal Jain, "A new image encryption algorithm based on DNA approach," *International journal of computer applications*, vol. 85, no. 18, pp.27-31, Jan. 2014.

[39] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, Feb. 2019, doi: 10.1016/j.sigpro.2018.10.011.

[40] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and*

Communications, vol. 66, no. 10, pp. 806–816, Oct. 2012, doi: 10.1016/j.aeue.2012.01.015.

[41] K. Mirzaei Talarposhti and M. Khaki Jamei, "A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map," *Optics and Lasers in Engineering*, vol. 81, pp. 21–34, Jun. 2016, doi: 10.1016/j.optlaseng.2016.01.006.

[42] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "Optimizing chaos based image encryption," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25569–25590, Mar. 2018, doi: 10.1007/s11042-018-5807-x.

[43] S. Suri and R. Vijay, "A Bi-objective Genetic Algorithm Optimization of Chaos-DNA Based Hybrid Approach," *Journal of Intelligent Systems*, vol. 28, no. 2, pp. 333–346, Apr. 2019, doi: 10.1515/jisys-2017-0069.

[44] B. Mondal and T. Mandal, "A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator," *Multimedia Tools and Applications*, vol.77, pp.25569-25590, Feb. 2020, doi: 10.1007/s11042-019-08352-z.

[45] Y. Niu, Z. Zhou, and X. Zhang, "An image encryption approach based on chaotic maps and genetic operations," *Multimedia Tools and Applications*, vol. 79, no. 35–36, pp. 25613–25633, Jul. 2020, doi: 10.1007/s11042-020-09237-2.

[46] K. S. Khalaf, M. A. Sharif, and M. S. Wahhab, "Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map," *International Journal of Engineering*, vol. 35, no. 10, pp. 1981–1988, Oct. 2022, doi: 10.5829/ije.2022.35.10a.16.

[47] Zakaria, Seyedeh Bahareh, and Keivan Navi, "Image encryption and decryption using exclusive-OR based on ternary value logic," *Computers and Electrical Engineering*, vol. 101, pp. 108021, 2022.

[48] D. T. Dheepak, "Enhancing the Cloud Security with ECC based Key Generation Technique," *Annals of the Romanian Society for Cell Biology*, pp. 3874–3891, Mar. 2021, Accessed: Jan. 11, 2023. [Online]. Available: https://www.annalsofrscb.ro/index.php/journal/article/view/1394

[49] G. Pai, "Design of Stream Cipher for Text Encryption using Particle Swarm Optimization based Key Generation," *Journal of Information Assurance and Security*, vol. 4, pp. 30–41, 2009, [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e844e886ffc9616a9b48884942a0dda6bf5975e3

[50] G. Jaya Krishna, V. Ravi, and S. Nagesh Bhattu, “Key generation for plain text in stream cipher via bi-objective evolutionary computing,” *Applied Soft Computing*, vol. 70, pp. 301–317, Sep. 2018, doi: 10.1016/j.asoc.2018.05.025.

[51] H. R. Kanan and B. Nazeri, “A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm,” *Expert Systems with Applications*, vol. 41, no. 14, pp. 6123–6130, Oct. 2014, doi: 10.1016/j.eswa.2014.04.022.

[52] P. D. Shah and R. S. Bichkar, “Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure,” *Engineering Science and Technology, an International Journal*, vol. 24, no. 3, pp. 782–794, Jun. 2021, doi: 10.1016/j.jestch.2020.11.008.

[53] P. Bedi, R. Bansal, and P. Sehgal, “Using PSO in a spatial domain based image hiding scheme with distortion tolerance,” *Computers & Electrical Engineering*, vol. 39, no. 2, pp. 640–654, Feb. 2013, doi: 10.1016/j.compeleceng.2012.12.021.

[54] Z.-H. Wang, C.-C. Chang, and M.-C. Li, “Optimizing least-significant-bit substitution using cat swarm optimization strategy,” *Information Sciences*, vol. 192, pp. 98–108, Jun. 2012, doi: 10.1016/j.ins.2010.07.011.

[55] R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud, and A. Alhindi, “An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms,” *IEEE Access*, vol. 7, pp. 133496–133508, 2019, doi: 10.1109/ACCESS.2019.2941440.

[56] A. Banharnsakun, “Artificial bee colony approach for enhancing LSB based image steganography,” *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 27491–27504, Apr. 2018, doi: 10.1007/s11042-018-5933-5.

[57] P. D. Shah and R. S. Bichkar, “Genetic Algorithm based Approach to Select Suitable Cover Image for Image Steganography,” *IEEE Xplore*, Jun. 01, 2020. https://ieeexplore.ieee.org/document/9154032 (accessed Dec. 22, 2022).

[58] P. D. Shah and R. S. Bichkar, “A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator,” *Advances in Intelligent Systems and Computing*, pp. 119–129, Dec. 2017, doi: 10.1007/978-981-10-5520-1_12.

[59] P. D. Shah and R. S. Bichkar, “Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure,” *Engineering Science and Technology an International Journal*, vol. 24, no. 3, pp. 782–794, Jun. 2021, doi: 10.1016/j.jestch.2020.11.008.

[60] M. A. Hameed, O. A. Abdel-Aleem, and M. Hassaballah, “A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 4639–4657, Sep. 2022, doi: 10.1007/s12652-022-04366-y.

[61] S. Kamil, M. Ayob, S. N. H. Sheikh Abdullah, and Z. Ahmad, “Optimized Data Hiding in Complemented or Non-Complemented Form in Video Steganography,” *2018 Cyber Resilience Conference*, Putrajaya, Malaysia, 2018.

[62] S. Gupta and N. K. Garg, “Optimized Data Hiding for the Image Steganography Using HVS Characteristics,” *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences*, pp. 275–285, 2021, doi: 10.1007/978-981-15-7533-4_21.

[63] M. N, N. Siddiqa, and T. H. Sardar, “Multi-Layered Security System Using Cryptography and Steganography,” *International Journal of Innovative Research in Computer Science & Technology*, vol. 7, no. 2, pp. 8–11, Mar. 2019, doi: 10.21276/ijircst.2019.7.2.1.

[64] H. E. Rostam, H. Motameni, and R. Enayatifar, “Privacy-preserving in the Internet of Things based on steganography and chaotic functions,” *Optik*, vol. 258, p. 168864, May 2022, doi: 10.1016/j.ijleo.2022.168864.

[65] T. Jambhale and M. Sudha, “A Privacy Preserving Hybrid Neural-Crypto Computing-Based Image Steganography for Medical Images,” *Intelligent Data Communication Technologies and Internet of Things*, pp. 277–290, 2021, doi: 10.1007/978-981-15-9509-7_24.

[66] A. Danlami Mohammed, O. A. Ojerinde, M. Folorunsho Victor, And M. Ogbuka Kenneth, “Privacy Preservation in Big Data Application using Advanced Encryption Standard and Least Significant Bit Steganography,” *i-manager’s Journal on Information Technology*, vol. 9, no. 2, p. 1, 2020, doi: 10.26634/jit.9.2.17550.

[67] O. Hosam and M. H. Ahmad, “Hybrid design for cloud data security using combination of AES, ECC and LSB steganography,” *International Journal of Computational Science and Engineering*, vol. 19, no. 2, p. 153, 2019, doi: 10.1504/ijcse.2019.100236.

[68] “Exhaustive Search - an overview | ScienceDirect Topics,” *www.sciencedirect.com*. https://www.sciencedirect.com/topics/engineering/exhaustive-search (accessed Jan. 12, 2023).

[69] B. Zolfaghari and T. Koshiba, "Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap," *Applied System Innovation*, vol. 5, no. 3, p. 57, Jun. 2022, doi: 10.3390/asi5030057.

[70] "SIPI Image Database," *sipi.usc.edu*. https://sipi.usc.edu/database/

[71] "MATLAB - Overview - Tutorialspoint," *Tutorialspoint.com*, 2019. https://www.tutorialspoint.com/matlab/matlab_overview.htm

[72] Y. Alghamdi, A. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, p. 1344, Sep. 2022, doi: 10.3390/e24101344.

[73] C. Sur, S. Sharma, and A. Shukla, "Solving Travelling Salesman Problem Using Egyptian Vulture Optimization Algorithm – A New Approach," *Language Processing and Intelligent Information Systems*, pp. 254–267, 2013, doi: 10.1007/978-3-642-38634-3_28.

[74] C. Sur, S. Sharma, and A. Shukla, "Egyptian Vulture Optimization Algorithm – A New Nature Inspired Meta-heuristics for Knapsack Problem," *The 9th International Conference on Computing and InformationTechnology (IC2IT2013)*, pp. 227–237, 2013, doi: 10.1007/978-3-642-37371-8_26.

[75] C. Sur and A. Shukla, "Road Traffic Management Using Egyptian Vulture Optimization Algorithm: A New Graph Agent-Based Optimization Meta-Heuristic Algorithm," *Lecture Notes in Electrical Engineering*, pp. 107–122, 2014, doi: 10.1007/978-3-319-03692-2_9.

[76] C. Sur and A. Shukla, "Green Heron Swarm Optimization Algorithm - State-of-the-Art of a New Nature Inspired Discrete Meta-Heuristics," *arXiv:1310.3805 [cs]*, Oct. 2013, Accessed: Jan. 11, 2023. [Online]. Available: https://arxiv.org/abs/1310.3805

[77] C. Sur and A. Shukla, "New Bio-inspired Meta-Heuristics - Green Herons Optimization Algorithm - for Optimization of Travelling Salesman Problem and Road Network," *Swarm, Evolutionary, and Memetic Computing*, pp. 168–179, 2013, doi: 10.1007/978-3-319-03756-1_15.

[78] C. Sur and A. Shukla, "Dealing QAP & KSP with Green Heron optimization algorithm — A new bio-inspired meta-heuristic," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Jul. 2013, doi: 10.1109/icccnt.2013.6726799.

[79] V. Hayyolalam and A. A. Pourhaji Kazem, "Black Widow Optimization Algorithm: A novel meta-heuristic approach for solving engineering optimization

problems," *Engineering Applications of Artificial Intelligence*, vol. 87, p. 103249, Jan. 2020, doi: 10.1016/j.engappai.2019.103249.

[80] Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie, "A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm," *IEEE Transactions on Multimedia*, vol. 12, no. 5, pp. 345–357, Aug. 2010, doi: 10.1109/tmm.2010.2051243.

[81] Vikhar, Pradnya A, "Evolutionary algorithms: A critical review and its future prospects," In *2016 International conference on global trends in signal processing, information computing and communication (ICGTSPICC)*, pp. 261-265, 2016.

[82] Bansal, J.C., Singh, P.K. and Pal, N.R. eds., "Evolutionary and swarm intelligence algorithms*," Cham: Springer*, vol. 779, 2019.

[83] S. Katoch, S. S. Chauhan, and V. Kumar, "A review on genetic algorithm: past, present, and future," *Multimedia Tools and Applications*, Oct. 2020, doi: 10.1007/s11042-020-10139-6.

[84] S. Das and P. N. Suganthan, "Differential Evolution: A Survey of the State-of-the-Art," *IEEE Transactions on Evolutionary Computation*, vol. 15, no. 1, pp. 4–31, Feb. 2011, doi: 10.1109/tevc.2010.2059031.

[85] A. Rajagopalan, D. R. Modale, and R. Senthilkumar, "Optimal Scheduling of Tasks in Cloud Computing Using Hybrid Firefly-Genetic Algorithm," *Learning and Analytics in Intelligent Systems*, pp. 678–687, Jul. 2019, doi: 10.1007/978-3-030-24318-0_77.

[86] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, Jun. 2020, doi: 10.1016/j.future.2020.02.029.

[87] C. Liu and J. Qiu, "Study on a Secure Wireless Data Communication in Internet of Things Applications," *IJCSNS International Journal of Computer Science and Network Security*, vol. 15, no. 2, p. 18, 2015, Accessed: Jan. 16, 2023. [Online]. Available: http://cloud.politala.ac.id/politala/1.%20Jurusan/Teknik%20Informatika/19.%20e-journal/Jurnal%20Internasional%20TI/IJCSNS/2015%20Vol.%2015%20No.%2002/20150204_Study%20on%20a%20Secure%20Wireless%20Data%20Communication%20in%20Internet%20of%20Things%20Applications.pdf

[88] J. Jin, "An image encryption based on elementary cellular automata," *Optics and Lasers in Engineering*, vol. 50, no. 12, pp. 1836–1843, Dec. 2012, doi: 10.1016/j.optlaseng.2012.06.002.

[89] Al-Utaibi, Khaled A., and El-Sayed M. El-Alfy, "A bio-inspired image encryption algorithm based on chaotic maps," In *IEEE Congress on Evolutionary Computation*, pp. 1-6, 2010.

[90] J. R. Nechvatal *et al.*, "Report on the Development of the Advanced Encryption Standard (AES)," *NIST*, vol. 106 No. 3, Jun. 2001, [Online]. Available: https://www.nist.gov/publications/report-development-advanced-encryption-standard-aes

[91] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.020.

[92] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity," *Multimedia Tools and Applications*, Jan. 2021, doi: 10.1007/s11042-020-10224-w.

[93] K. Z. Mohd Azmi, A. S. Abdul Ghani, Z. Md Yusof, and Z. Ibrahim, "Natural-based underwater image color enhancement through fusion of swarm-intelligence algorithm," *Applied Soft Computing*, vol. 85, p. 105810, Dec. 2019, doi: 10.1016/j.asoc.2019.105810.

[94] "Bio-Medical-Image-Analysis-with-DICOMs/images at main · sauravmishra1710/Bio-Medical-Image-Analysis-with-DICOMs," *GitHub*. https://github.com/sauravmishra1710/Bio-Medical-Image-Analysis-with-DICOMs/tree/main/images (accessed Jan. 12, 2023).