



REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

**AN EFFECT IMAGE STEGANOGRAPHY SYSTEM
BASED ON PIXELS DISPARITY VALUE AND
SECRET MESSAGE COMPRESSION**

Maryam Shamil MUSTAFA

Master's Thesis

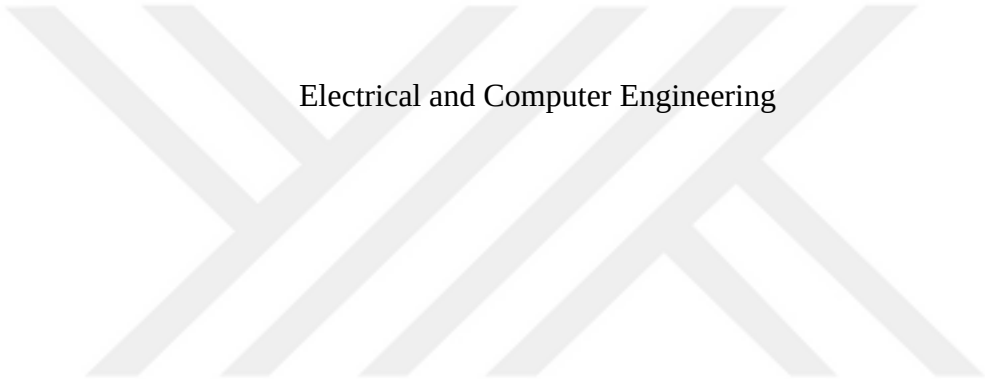
Supervisor

Prof. Dr. Galip CANSEVER

Istanbul, 2022

AN EFFECT IMAGE STEGANOGRAPHY SYSTEM BASED ON PIXELS DISPARITY VALUE AND SECRET MESSAGE COMPRESSION

Maryam Shamil MUSTAFA



Electrical and Computer Engineering

Master's Thesis

ALTINBAS UNIVERSITY

2022

The thesis titled AN EFFECT IMAGE STEGANOGRAPHY SYSTEM BASED ON PIXELS DISPARITY VALUE AND SECRET MESSAGE COMPRESSION prepared by MARYAM SHAMIL MUSTAFA and submitted on 13/06/2022 has been accepted **by unanimously** for the degree of Master of Electrical and Computer Engineering.

Prof. Dr. Galip CANSEVER

Supervisor

Thesis Defense Committee Members:

Prof. Dr. Galip CANSEVER

Faculty of Engineering and
Natural Sciences,
Altinbas University

Asst. Prof. Dr. Sefer KURNAZ

Faculty of Engineering and
Natural Sciences,
Altinbas University

Asst. Prof. Dr. Yavuz EREN

Faculty of Electrical and
Electronics,
Yildiz Technical University

I hereby declare that this thesis meets all format and submission requirements of a Master`s Thesis.

Submission date of the thesis to Institute of Graduate Studies: ____/____/____

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Maryam Shamil MUSTAFA



Signature

DEDICATION

I devote and pledge this research work to my supervisor who is salient for guiding me throughwhole research work as well as my family for always assisting me in my hard time



PREFACE

First of all, gratefulness of thanks to our Creator, “ALLAH”, who enabled us to complete this study. Special thanks go to Prof. Dr. Galip CANSEVER, for giving this opportunity to work under his supervision and for sharing his great knowledge and experience with me.

Finally, special thanks to my family, my brothers and all my lovely friends for their continuous encouragement and support throughout the time taken to write this thesis.



ABSTRACT

AN EFFECT IMAGE STEGANOGRAPHY SYSTEM BASED ON PIXELS DISPARITY VALUE AND SECRET MESSAGE COMPRESSION

Mustafa, Maryam

M.Sc. Electrical and Computer Engineering, Altınbaş University,

Supervisor: Prof. Dr. Galip CANSEVER

Date: 06/2022

Pages: 103

The first priority in the technology and modern communication is improving an effective and delicate steganography scheme when considering data hiding. Developing such a scheme for hiding a secret message should ideally disguise the hidden data well within transmission media. Pressing challenges in the context of a steganography system include security, imperceptibility, and capacity issues. Enhancing these issues must be done by enhancing the Peak-Signal to Noise Ratio in the steganography method to concretize it. Furthermore, imperceptibility and robustness enhancement are required, this thesis is proposed an enhanced steganography system made by $Pixel_s / Pixel_d$ method. An enhanced proposed system gives evidence towards overcoming the aforementioned issues. The main contribution utilized in this research starting with image and text preparation passing by embedding stage and ending with the evaluation stage, which is suffering huge challenges and underscored in this research. Finally, the evaluation stage which gives tremendous attention due to the responsible for the evaluation of the system. For implementing the system, standard datasets (USC-SIPI) are used. Excellent results in terms of Peak Signal-to-Noise Ratio (77.203 dB) achieved by this study. Based on the findings, the proposed scheme gives evidence to increase capacity, imperceptibility, and security to overcome existing issues. Superior imperceptibility achieved compare with

previous methods in the literature.

Keywords: Image Steganography, Security, PSNR, Payload Capacity, Imperceptibility.



TABLE OF CONTENTS

	<u>Pages</u>
ABSTRACT	vii
LIST OF TABLES	xiii
LIST OF FIGURES.....	xiv
LIST OF CHARTS.....	xvii
ABBREVIATIONS.....	xviii
1. INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 PROBLEM BACKGROUND	3
1.3 PROBLEM STATEMENT.....	7
1.4 RESEARCH GOAL	8
1.5 RESEARCH OBJECTIVES.....	8
1.6 RESEARCH SCOPE.....	8
1.7 MOTIVATION.....	9
1.8 SIGNIFICANCE OF PROPOSED METHOD.....	9
1.9 THESIS OUTLINE	10
2. LITERATURE REVIEW	11
2.1 INTRODUCTION	11
2.4 STEGANOGRAPHY CLASSIFICATION	13
2.4.1 Cover Medium Classification Based	14
2.4.1.1 Text-based steganography	15
2.4.1.2 Image-based steganography	15
2.4.1.3 Audio-based steganography	16
2.4.1.4 Video-based steganography	16
2.4.1.5 Protocol-based steganography	16

2.4.2 Dna Based Steganography	16
2.4.3 Key Types- Classification Based.....	17
2.4.3.1 Pure key steganography	17
2.4.3.2 Secret key steganography	17
2.4.3.3 Public key steganography	17
2.4.4 Embedding Procedures- Classification Based	18
2.4.4.1 Insertion-based technique	18
2.4.4.2 Substitution-based technique	18
2.4.4.3 Generation-based technique	18
2.4.4.4 Cover look-up-based technique	19
2.4.5 Extraction Function Classification Based.....	19
2.4.5.1 Blind steganographic scheme	19
2.4.5.2 Non-Blind steganographic scheme.....	19
2.5 APPLICATION OF STEGANOGRAPHY	20
2.6 PROPERTIES OF STEGANOGRAPHY	20
2.6.1 Imperceptibility.....	21
2.6.2 Robustness	21
2.6.3 Payload Capacity	22
2.7 Embedding Domains of Image Steganography	22
2.7.1 SPATIAL or Map Domain	23
2.7.2 Frequency Domain.....	23
2.7.3 Adaptive Domain	24
2.8 STEGANALYSIS METHODS	24
2.8.1 Human Visual System (HVS) Attack	25
2.8.2 Chi-Square Attack (χ^2)	25
2.9 DATA PREPARATION.....	26
2.10 STEGANOGRAPHY VS CRYPTOGRAPHY	27
2.11 SUMMARY OF WORKS OF LITERATURE REVIEW (2015-2022).....	28

2.12 SUMMARY	32
3. METHODOLOGY	33
3.1 INTRODUCTION	33
3.2 FRAMEWORK	34
3.2.1 Proposed Method	36
3.2.1.1 Least significant bit (LSB) steganography	36
3.2.1.2 Pixel indicator	37
3.2.2 Data Pre-Processing	37
3.2.2.1 Secret data preparation	38
3.2.2.2 Cover image preparation	44
3.2.2.3 Stego key in steganography	52
3.2.3 Embedding Part	54
3.2.4 Evaluation Stage	58
3.2.5 Extracting Stage	59
3.2.6 The Usc-Sipi Image Database	61
3.3 SOFTWARE IMPLEMENTATION	62
3.4 SUMMARY	67
4. RESULTS OF THE PROPOSED SYSTEM	68
4.1 INTRODUCTION	68
4.2 RESULTS AND DISCUSSIONS	68
4.2.1 Imperceptibility	68
4.2.2 Robustness	72
4.2.3 Human Visual System Attack	78
4.3 SUMMARY	80
5. CONCLUSION AND FUTURE WORK	81
5.1 INTRODUCTION	81
5.2 CONCLUSION	81
5.3 CONTRIBUTION	82

5.4 FUTURE WORK	82
REFERENCES	84



LIST OF TABLES

	<u>Pages</u>
Table 1.1: The PC utilized in various steganography method.....	6
Table 2.1: An overall comparison of spatial and transform domains with adaptive embedding methods.....	23
Table 2.2: Data proration of the proposed study.	27
Table 2.3: Differences Between Steganography and cryptography	28
Table 2.4: Summary of Related Work from 2015 – 2022	29
Table 2.4: Summary of Related Work from 2015 – 2022 “Tables continued”	30
Table 2.4: Summary of Related Work from 2015 – 2022 “Tables continued”	31
Table 3.1: The Binary Bit-plane within the Image.....	47
Table 4.1: Computing PSNR for Cameraman gray-scale image.....	69
Table 4.2: Computing PSNR for Zelda gray-scale image	70
Table 4.3: Computing PSNR for House Gray-scale image	70

LIST OF FIGURES

	<u>Pages</u>
Figure 1.1: Three main performance criteria concerning the existing steganography schemes.....	2
Figure 2.1: General structure of steganography scheme [60].....	13
Figure 2.2: A comprehensive taxanomy of digital steganography [21]	14
Figure 2.3: Properties of the steganographic system.....	20
Figure 2.4: Types of steganalysis attacks [12]	24
Figure 2.5: Model for both types of HVS and Chi-square attacks [22].....	26
Figure 3.1: Research framework	35
Figure 3.2: The basic mechanism for the 1-bit LSB embedding.....	37
Figure 3.3: Secret Text Preparation in Proposed Method	39
Figure 3.4: Huffman coding and text frequency reducing.....	39
Figure 3.5: Flowchart of Huffman coding.....	40
Figure 3.6: Huffman coding tree	41
Figure 3.7: Bits stream Fragmentation in proposed method	43
Figure 3.8: Generating key by two stages	43
Figure 3.9: Bit value weight based on LSB and MSB.....	45
Figure 3.10: Pixels of colour and gray image.....	46
Figure 3.11: 8-bitplane distribution in gray image	46
Figure 3.12: The Fibonacci sequence number.....	47

Figure 3.13: Decomposition for Lena image in (a) 8-bit-plane and (b) 12-bitplane in proposed work.	48
Figure 3.14: The principle of image steganography	53
Figure 3.15: The principle of asymmetric cryptography	54
Figure 3.16: Principles of stego key and image.....	55
Figure 3.17: A general embedding process	56
Figure 3.18: Explains the proposed theory	58
Figure 3.19: The evaluation criteria with the proposed system.....	59
Figure 3.20: Embedding and extracting processes	60
Figure 3.21: USC-SIPI dataset images used in the proposed system.....	61
Figure 3.22: The main menu of the demo system	62
Figure 3.23: The embedding process within proposed system.....	63
Figure 3.24: Selecting a cover image for embedding selected a secret text.....	64
Figure 3.25: Different payload capacities used in the proposed system	65
Figure 3.26: Shows resulted images after embedding process	66
Figure 3.27: The Extracting process within proposed system.....	67
Figure 4.1: Compute PSNR values along with different payload capacity (PC).	71
Figure 4.2: PSNR test for different colour images.	72
Figure 4.3: Binary versus Fibonacci pixels	73
Figure 4.4: The difference between Fibonacci and binary decomposition.....	74
Figure 4.5: The χ^2 -test for the original Tiffany image	75
Figure 4.6: The χ^2 -test for the simple LSB method with embedded 16384 pixels	76

Figure 4.7: The χ^2 performance test after concealment 16384 dB.....	76
Figure 4.8: The embedment using the proposed system for the baboon image with (a) 49152 and (b) 32768 bytes	77
Figure 4.9: The demonstration of the visual attacks with different bit planes for the peppers image	78
Figure 4.10: The performance of the present methods against HVS attack for the original Tiffany image	79
Figure 4.11: The bit plane (1) of the camera man and gold hill images with the proposed <i>Pixels /Pixeld</i> method.....	80

LIST OF CHARTS

	<u>Pages</u>
Chart 3.1: Huffman coding.....	42
Chart 3.2: Recursive bit stream function	44
Chart 3.3: Fibonacci sequence number	51
Chart 3.4: Embedding Algorithm	57



ABBREVIATIONS

DCT	:	Discrete Cosine Transform
DE	:	Difference Expansion
DFT	:	Discrete Fourier Transform
EMD	:	Exploiting Modification Direction
FFT	:	Fractional Fourier Transform
GA	:	Genetic Algorithm
HDWT	:	Haar Discrete Wavelet Transform
HVS	:	Human Visual System
JPEG	:	Joint Photographic Experts Group
LSB	:	Least Significant Bit
MSB	:	Most Significant Bit
OPAP	:	Optimal Pixels Adjustment Process
PDF	:	Partial difference equation
POV	:	Pairs of Values
PSNR	:	Peak Signal-to-Noise Ratio
PVD	:	Pixel Value Differencing
RGB	:	Red, Green and Blue
RPE	:	Random Pixel Embedding
SIS	:	Skeletonography Image System
TCP/IP	:	Transmission Control Protocol Internet Protocol
WFFT	:	Weight Fractional Fourier Transform

1. INTRODUCTION

1.1 INTRODUCTION

In recent times, the fast development of the information and communication technology enabled the free and easy transfer of the vast amount of data over the open internet. This free flow of massive data over the internet network in turn posed severe threat towards the privacy preserved sensitive data transfer where the intruders/attackers are constantly faced. Although the transfer (sending or receiving) of the data information ((such as the text, image, video, and audio) became very easy, securing the sensitive information over the insecure public network posed new challenges. For secured information transfer from the sender to received end, diverse information hiding techniques including the steganography, cryptography and watermarking have been introduced. Using the steganography scheme, the secret or private data can be hidden within different media including the colour or grayscale image [1]. The steganography technique can be divided into various categorizes based on the cover media such as the image, audio, text or video [1] wherein every such cover media has its own merits and demerits [2][3]. Over the past decades, intensive studies have been performed to develop some highly robust and secured image steganography schemes (ISSs). Essentially, these ISSs became promising owing to their easy transmission capacity of the multimedia contents via social media application platforms such as the WhatsApp, Twitter, Facebook and LinkedIn [3]. Despite the popularity and robustness of these ISSs, various issues related to the security and concealment of the private message (secret text) for the safe information transfer remains unresolved. In addition, a better understanding of the private message hiding processes in an image is vital for development of an outperforming ISS [4]. Generally, the steganography schemes are attained in the spatial and transform domains [5]. Two important concepts are involved in the steganography technique so called stego and cover image. A stego image hosts the secret information with certain quality, whereas the cover media (image) is the pure image (original) without containing any secret data within it and is ready to host the secret information. The significance of the steganography scheme relies on the security of the secret message that is embedded within the image. However, the problems arise when the

illegal messages or data embedded by the unauthorized users become expansive [6] [7]. In the steganography technique, the sender and receiver work together to hide the data needs to be transferred and then extracted. In this process, the sender hides the message and delivers, while the receiver extracts the information hidden in the stego image using a stego key [8]. The steganography technique has been applied in the field of medical diagnoses [9] [10], military and defense [11], multimedia biometric data security [12] and cloud computing [13]. The fundamental issues and difficulties concerning the performance of the existing state-of-the-art steganography schemes are related to the payload capacity, imperceptibility, and security [14] as indicated in Figure 1.1.

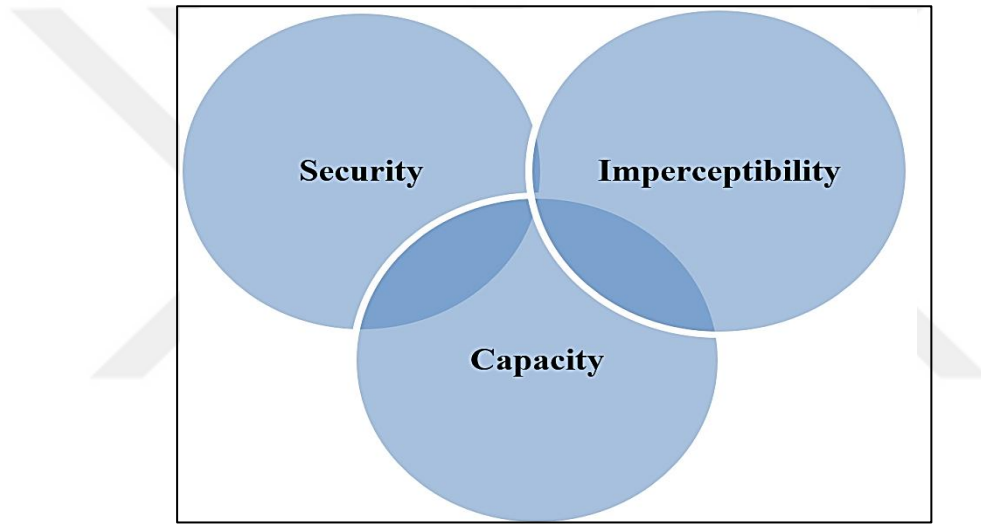


Figure 0.1: Three main performance criteria concerning the existing steganography schemes.

The Payload Capacity (PC) of the steganography method is defined as maximum amount of secret data that can be concealment into the image media [15]. The maximum payload refers to the highest limit of the secret data that can be embedded into the image. The imperceptibility of a steganography system signifies the carrier media quality that can be used for hiding the secret message following the algorithm embedment [16]. The security of a steganography system [17] refers to its robustness against various statistical tests like the chi-square test, human visual system and histogram analysis. The present work intends to resolve various issues related to the existing steganography system and improve its robustness in terms of high security, high payload capacity, and imperceptibility [18].

1.2 PROBLEM BACKGROUND

Intensive efforts have recently been made to secure the secret data by hiding it within the transmitting image media, making the secret data unnoticeable to the intruders [19] [20]. Consequently, the steganography approach for the data hiding in the image media received immense attention in the field of security and privacy preserved information communications [21]. Conversely, the use of other transmission media such as the protocols and text are quite sparse [22]. As aforementioned, the imperceptibility (embedding method), security and payload capacity being the main concerns related to the steganography system's performance need further improvement [23] [24]. It is important to mention that several studies in the image steganography and steganalysis focused on the improvement of the imperceptibility (embedding method). Based on this fact, the performance of the developed image steganography system was assessed in terms of the measures including the Structural-Similarity-Index (SSIM) and Peak-Signal-to-Noise-Ratio (PSNR) and [25] [26]. Actually, the enhancement of the PSNR and SSIM became one of the main challenges in the steganography techniques. The payload capacity being a trade-off between the PSNR and SSIM, different approaches have been proposed to enhance the PSNR and SSIM values. Despite the accomplishment of some encouraging results, only a few investigations have been conducted on the payload capacity [27] [28]. In-depth literature survey indicated that the studies on the trade-off between the steganography performance criteria are unbalanced [29]. Some researchers used a low payload capacity in order to increase PSNR and SSIM values. It has been observed that the use of the high payload capacity can affect the image quality, reducing the PSNR plus SSIM and vice versa. The PSNR is considered as low if it is less than equal to 45 dB. Conversely, the PSNR is acceptable if it is less than equal to 59 dB, otherwise, PSNR is regarded as high [30]. In the case of SSIM, two images are said to be similar to each other if the value of SSIM is equal to 1. Otherwise, the images are considered to be noisy [31] [32]. To achieve the improved security in the steganography method different strategies have been adopted. Amongst all these approaches, the pixel randomization was shown to be the most suitable one because it shares the same pixel features [40]. Several approaches have recently been introduced to increase the security including the image partitioning and pixel randomization. Although these proposed approaches are promising, each of them encounters different limitations during the performance evaluation. For instance, Das et al. [40] proposed the improvement

to image steganography algorithm using the pixel intensity and randomization of different pixel values to achieve improved security. In this method, greater space and manipulation of the pixels order in the stego image were considered wherein the secret bits were hold in two bits of the LSB. The proposed algorithm was simple in terms of the embedding process and the performance was evaluated in terms of the PSNR and Chi-square attack. The issues concerning the security performance of the image steganography have widely been discussed in the recent state-of-the-art literatures. Despite the development of different approaches to resolve these issues, the weaknesses of the image steganography still persist. Due to easy access of the information, the attackers acquired enough knowledge and expertise in the field of security, thus can breach the secret codes and keys. The intruders/hackers/attackers can anticipate easily the greater security of the secret data in the images due to the abundance of the steganalysis methods and tools with improved performance. Therefore, finding the newer and powerful approaches for the secret data concealing became necessary. It is inferred that the new approaches may enable in securing the transmitted information between two parties [41]. The LSB is one of the spatial domain techniques that are used by different approaches. However, this technique has some weaknesses (low security and poor robustness) against the statistical attack. This weakness can be attributed to the direct embedding in the LSB part of the pixel. The statistical attack is based on analyzing the LSB directly because of the presence of the secret data in this part. In order to enhance the security, some researchers have worked on the frequency domain transformation. The use of DCT and discrete wavelength transform (DWT) was shown to produce better results [42]. These frequency-domain techniques indicated stronger security than the LSB-based technique when applied against the Human Visual System (HVS) and Histogram analysis attacks. However, these methods have limitations when applied against other attacks such as the chi-square attack because this domain uses coefficients directly to embed the secret message. In addition, the chi-square is influenced by the slightest effects with the coefficients inside the image, thereby affecting the security. The existing steganography schemes use additional tools such as the the compression, noise removal or encryption in advance to increase the data security. However, the inclusion of such extra tools affects various other details of the developed steganography scheme, thereby increasing its complexity and execution time. Despite some intriguing applications of the steganography schemes in the biometric and medical fields, many issues involving these

applications require further improvement [43]. In addition, these applications suffer from the security problems which need to be enhanced [44]. To reduce the complexity of the image steganography system, the tunable visual image quality-based genetic algorithm (GA) was introduced by Kanan and Nazeri (2014), wherein the lossless data in the spatial domain was utilized for the problems optimization. Experimental results showed a high embedded capacity with enhanced PSNR. However, the system performance was poor against the statistical attacks which were due to the information hiding using a single randomized stage [45]. In an image steganography system, the word *security* is considered as a vital evaluation parameter. Indirectly, security refers to the undetectability or unnoticeability of the hidden data information. Therefore, any steganography system is regarded as highly secure if the secret information remains undetectable by the statistical analysis or attackers. In fact, the security issue needs to be resolved for avoiding the illegitimate data access by the intruders while transmitting through an insecure communication channel. Generally, the steganography systems may suffer from different types of the steganalysis detection attacks. The intruders are attracted to trace the existence or even to retrieve the secret information bits from the stego images. It is worth noting that no single steganography system is immune to all kinds of the statistical attacks. Thus, all steganography system used one or two statistical attacks during their performance evaluation [46]. Qian et al. (2018) suggested a better steganography approach to conceal the data for better security wherein the pixel difference histogram (PDH) was used during the data transmission. The performance of the proposed steganography approach was evaluated against chi-square attack only [47]. The maximum payload capacity (PC) of a steganography method related the highest the amount of the secret data to be embedment in the cover media file such as image best on to a specific condition. Therefore, it is desirable to enhance PC of a steganography system for getting better performance. A significant change in the multimedia file is observed when the maximum information limit is exceeded, causing a failure of the steganography algorithm. The steganography PC is measured using the Data Hiding Ratio (DHR) which is defined as the ratio between the maximum payload capacities to the original media size [34]. In [22] defined the hiding rate as the PC amount of data hidden (in bits) relative to the original image size. Thus, keeping the higher PC in a steganography system without sacrificing the image quality (imperceptibility) and security is a main challenge [48]. The size of the PC is characterized in terms of the bits per pixel

(Bpp), bytes and percentage (%). Table 1.1 shows the very low, regular, and very high PC used in different steganography method [49].

Table 1.1: The PC utilized in various steganography method

Types of capacity	Very low	Regular	Very High
Bytes	≤ 16384	≤ 49152	> 49152
Bpp	≤ 0.5	≤ 1.5	> 1.5
Percentage (%)	$\leq 6.25\%$	$\leq 18.75\%$	$> 18.75\%$

The noise level in the cover image increases with the increase of the payload capacity in the cover image, making it easy for the intruder to notice and analyze the secret message. Therefore, the approach used for the performance evaluation of any steganography system must aim to carry out the statistical analysis for the embedded data [50][33]. To achieve this goal, numerous approaches employ LSB for embedding the secret bit into a pixel [34][35]. However, the LSB is limited as insertion is restricted to one or two bits to host the data, leading to a major weakness of the steganography system. When the capacity of the stego images (images that hold the secret message) increases, the images become more susceptible to various types of attacks. The chi-square (χ^2) attack is very sensitive to the amount of data embedded into an image (capacity) [36][37][38]. The HVS attack is very sensitive to the LSB change in the image pixels that reveal the secret message position [39] [51] [52]. In [44] and [53] implement LSB methods in the image steganography. The regular capacity of 32768 dB and 32768 dB. During implement the proposed method, authors neglected the image quality (imperceptibility). Additionally, the payload capacity was based on the structure of the given image [32]. Unlike the previous study [54], [55] used some parts of the images like the edge. In [56], authors used high pixel contrast and [25] the special Region of Interest (ROI) position to obtain better result of the implementing the steganography. Overall, an increase in the payload capacity of the secret message involves very careful execution and constant monitoring to achieve a balance between the security and imperceptibility.

1.3 PROBLEM STATEMENT

The existing image steganography systems have various limitations that need to be surmounted. First, the challenging issue related to the payload capacity of the image needs to be resolved because any fault in the image steganography approach can affect the payload capacity. Commonly, the compression algorithms are used to reduce the secret message size via the condensation process. In addition, the compression approach changes the features of secret messages. The existing compression methods are easy to analyse using steganalysis and decompression tools. Therefore, changing the secret messages features and transform it into a new form is helpful to payload capacity and security as well. Second, the weak security performance of the existing steganography method against various statistical attacks is the major shortcoming that needs to be overcome. The security of the proposed scheme is related to the randomization of the blocks and pixels of a selected image that host the secret bits. The majority of the previous studies used an image partitioning strategy with the single randomization of the blocks and pixels to enhance the security performance for developed better steganography method. However, such the strategy produces the stego images that are easily detectable via statistical analysis such as the chi-square attack, thereby making the steganography system insecure against attacks. This clearly indicates that the challenges to re-arrange the image pixels inside a certain image to enhance the pixels' location integrity still an open problem that needs in-depth understanding. The Third challenging limitation in steganography is image quality (imperceptibility), which is compute via the PSNR equation. The high PSNR signifies better imperceptibility of the image, indicating a better steganography system [13]. The PSNR equation is depends on the altering MSE (short for Mean Square Error) values wherein the solutions suffer from a high rate of MSE that reduces the PSNR of the stego image [12][8]. Thus, it is essential to resolve this issue by reducing the MSE, thereby improving the imperceptibility of the stego image. In short, despite the substantial research efforts, the development of a robust steganography system that overcomes the problems involving the security, payload capacity, and imperceptibility of the stego image is still lacking.

1.4 RESEARCH GOAL

The main goal in present study is to introduce the enhanced image steganography scheme by expanding the payload capacity and increased imperceptibility for secures the secret data inside an image.

1.5 RESEARCH OBJECTIVES

Based on the aforementioned research gaps the following objectives are set:

- 1.To design a compression method of secret message for increasing the capacity and adding better security level.
- 2.To design a decomposition method that increase the steganography robustness while maintaining a visual quality of the stego image.
- 3.To design an enhance embedding method for concealment the secret data which improve a security of the steganography system

Because of widely used the internet with application that depends on the internet which needs the security issue; in addition to spread the image over the internet with its facility then developing steganography system of high security is needed. Developing such steganography secure method with sufficient capacity with maintains trusted media is much helpful.

1.6 RESEARCH SCOPE

This work intends to improve a highly secured image steganography system based on the $P_{\text{single}}/P_{\text{double}}$ method to achieve the strong imperceptibility, high PSNR and improved robustness. Some of the existing state-of-the-art techniques are used in the proposed system to further enhance its robustness. Based on these set objectives, the following scopes of study are emerged:

- i.The zooming, scaling, rotation, etc. is not considered within this work in addition to the time.
- ii.Embedment of the text file into an image was performed by considering the condition of the steganography system.

iii. Use of the colour and grey images (Tiffany, Lena, Lake, Zelda and Baboon with pixels size of 512×512 from the standard dataset (SIPI) for the evaluation of the proposed scheme.

iv. Testing the robustness of the proposed scheme against Chi-X2 and HVS tests.

1.7 MOTIVATION

The work develops a steganography approach in the image due to the images are excellent media that exhibit great redundancy in their representation. In addition, the usage of images is widespread in organizations to communicate among their members. Apart from that, images are also used extensively for communication between members of the military, intelligence operatives, agents of companies, and medical staff to hide sensitive or vital data. Moreover, a steady increase in malicious attacks on industrial applications, private applications, business, and sensitive government documents by adversaries of various kinds have motivated researchers and developers in the information security field to seek technical solutions to protect the privacy of documents sent over communication channels. The present work is motivated by the need for a more secure solution for protecting secret data that is being transmitted over communication channels so as to strengthen the privacy and integrity of the secret data.

1.8 SIGNIFICANCE OF PROPOSED METHOD

The proposed method could overcome some of the limitations associated with the existing steganography system. The newly developed system is anticipated to be more reliable in terms of security and capacity. Security of the steganography scheme is expected to be enhanced while keeping the PSNR score at a high level. This study anticipates challenges in the aspect of capacity and would attempt to lower its dependency. Limitations suffered by existing approaches in the embedding process are overcome by using the proposed scheme. Meanwhile, the performance evaluation results of the present steganography system are showed improved capacity and security. The designed steganography system may contribute to several applied fields of data communication such as the military, medical, cloud computing, and industry where high security and robustness are a priority.

Contributions of the study are not only limited to implementation in the field of image steganography, as the proposed scheme may also be used in other sections of steganography,

watermarking, and encryption fields. The proposed scheme proposes ideal quality in terms of randomness criteria, and this could make the proposed work applicable in fields that require randomness such as a complete randomised design, computer simulation, statistical sampling, and in fields where unpredictable sequences are desired.

1.9 THESIS OUTLINE

The proposed work is presented through this thesis and organized into seven chapters, which can be outlined as follows:

Chapter 1: An introduction to the proposed research is elaborated including problem formulation and a description of a research goal, objectives, scope, and significance.

Chapter 2: The chapter introduces hiding data approaches in a critical manner, research gaps, and principles in the classification of steganography are discussed in detail. The advantages and weaknesses of existing approaches were elaborated as well.

Chapter 3: General research framework, datasets used in the system testing and training, and the techniques used to evaluate the system are presented.

Chapter 4: Performance evaluation and security attacks of proposed scheme are explained in this chapter.

Chapter 5: Contributions and future works of the proposed research are elaborated in this chapter.

2. LITERATURE REVIEW

2.1 INTRODUCTION

This section presents a detailed comprehensive summary that aims at identifying all the objectives and questions raised in this research. As earlier mentioned, one of the definitions of the term, steganography, is the technique of concealing communication; a system for hiding of the secret data in the salient host image is referred to as a steganography system. So, there is no doubt if this media (image) carried the secret or not. Invisible ink or some time tattoos is used to transmit the hidden messages in the old steganography systems. Due to modern communication and its development, the transfer of the message has become easy via many hosting media. The emergence of the internet makes it necessary to spend effort on hiding the data and making it unseen or observed by the intruder [38]. Researchers have spent more effort trying to keep the message transfer secured and many methods have been suggested, each having its advantages and weaknesses [57][52]. The main issue in considering steganography as the art of invisible communication is the rise of the internet and the required security applications [58]. Information hiding has a long history, beginning when the nobleman was in need to contact his son; he devised the method of tattooed messages on chosen slaves and in their scalp after shaving; then, when the hair has grown again, he will send the slave to his son, with the tattooed message still hidden inside his scalp. This was the first attempt to steganography. Later, the Germans develop new techniques during the "Second World War " by using microdot to minimize periods of typing, making it difficult to find the message or detect it when sent via a secure channel [13][20]. Information hiding is an old idea, maybe older than communication itself. Information hiding consists of two major terms: the first one is steganography which will be considered in this study, while the second one is watermarking which is a different idea that was not considered in this study. The initial concept of steganography was confusing as messages were transferred manually and later developed step by step using horses, mail, and phones. In this case, when we need to hide the message, it should be kept in the mind of the messenger or hidden with the messenger himself. Despite the availability of sophisticated information techniques, however, it all dates back to the ancient Greece when information is hidden on the messenger's body. The Romans used invisible ink as steganography principles to write the secret message in between the original lines and to

reveal the secret message, they use a special material or heat it to be black [17]. During World War II, the famous method used to send secret message was invisible ink with variable extraction code technique. Invisible ink nowadays uses different techniques like Ultraviolet radiance this is employed with anti-counterfeit gadgets. The first attempt to secret message hiding into innocuous text started with the monk Johannes T. when he considered modern cryptography [59]. "Steganographia" is the title of the first book that considered steganography; it consists of 400 pages and was written by Gaspari Schott in 1665. This book includes the ideas almost took from the monk Trithemius. Cryptography on the other hand was first introduced in the book titled "Cryptographie Militaire" which was published by Auguste K in 1883. The book also mentioned the principles of steganography system that took must be considered when suggesting or designing any steganography system [36].

2.2 STEGANOGRAPHY

The term steganography can be defined as an intelligent technique for hiding secret data in reliable hosting cover in a manner which makes the media that carry the secret message non-detectible and unseen by the intruder or attacker. Even when the data is detected, it will be unreadable. In the context of digital world, the aim of both cryptography and steganography is to hold and save the secret data and protect it from hackers or intruder. These methods are useful when executed together. Many data formats are utilized with steganography recently, such as .bmp, .jpeg, .gif, .doc, .mp3 and etc... When considering this scope of steganography, it can be imagined that the necessary of modern steganography, especially with the internet, is for both security and capacity. Because of strict rules imposed by authorities and their impediments, the durability of cryptography system in the cyberspace group has been weakened. This is the reason why we needful to steganography where the sent message is secure and cannot be extracted by an intruder or attacker from the cover media except with the appropriate key [14][17].

2.3 TERMINOLOGIES OF STEGANOGRAPHY

Requirements that needed in every steganography system to hide information within trusted media are:

- a) For holding message Cover image (C).
- b) Any type of text called Secret Message (M).
- c) For embedding Stego Function (Fe) for extraction (Fe^{-1})
- d) For revealing secret, we use Stego Key (K) or called password.

For more understanding, assuming secret message (M) will store in the cover image (C) using the in embedding procedure (Fe) to produce the stego image (S). All the information on the embedding process is stored in the stego key (K) to use in the extracting process. The extract the secret messages from stego image (S) in the receiver side as shown in Figure 2. [60][61].

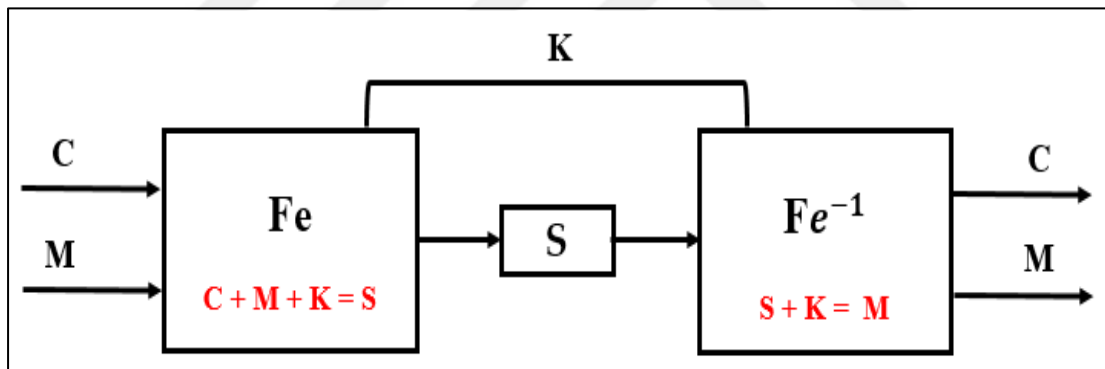


Figure 2.1: General structure of steganography scheme [60].

2.4 STEGANOGRAPHY CLASSIFICATION

This section presents the a comperhensive taxanonmy of digital steganography. This classification may be based on the type of cover medium employed, the key utilized to conceal and extricate masked messages, the hiding procedure, or the extracting function [61][22] as shown in Figure 2.3.

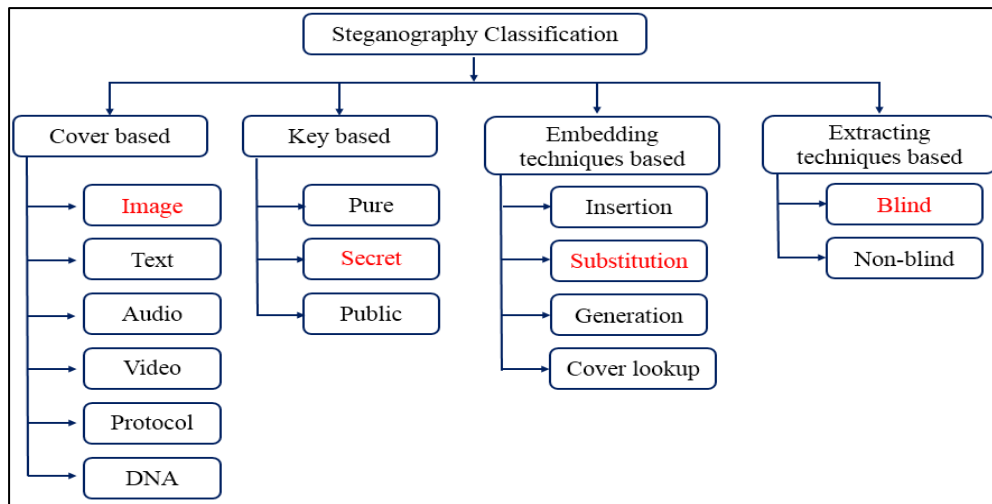


Figure 2.2: A comprehensive taxonomy of digital steganography [21]

As shown in Figure 2.2, this study selects the image file as a cover medium and embeds the hidden message by using a secret stego key . The different classifications of steganography are described in nest subsections.

2.4.1 Cover Medium Classification Based

The initial aspect to be clarified in this subsection is the definition of the cover media or the container of the concolment details or secret data. The properties of the carrier media or some of its areas can be changed, updated, or influenced to conceal vital details. Nevertheless, the influence taking place throughout the embedding activity must stay undetected to everyone except for the purposed message recipients. Therefore, the setup or visual facet of the carrier documents must remain intact after masking the secret data. Hence, secret information can be embedment into different kinds of cover media. Although the characteristics of cover files have differences depending on the redundancy in the digital depiction and distinctive cover file format, the mentioned elements persist in managing the procedures of embedding secret data into the digital specification of cover files. To this end, the cover (carrier) image is a foundational constituent of the steganographic arrangement. Figure 2.3, explain various steganographic techniques based on cover medium types are described as follows.

2.4.1.1 Text-based steganography

In this form of steganography, the cover medium used is text file; it is among the most problematic steganography techniques [18][24] as a result of the absence of unnecessary data in text files to hide the message [61][62]. This technique is also facing the problem of susceptibility to interception by a third party which can be achieved by just replacing or reformatting the text file itself into another form (such as .txt to .pdf). Over the years, several text-based steganography methods have been proposed, such as line shift, open spaces, word shift, and semantic. However, text-based steganography remains a commonly used technique due to various motivations. Among these motivation is the fact that the secret message can easily bypass the attention of attackers by encoding the secret message within an email message or Internet article. Detection may also be prevented by classifying the text as a spam message. Artificial messages may be produced via propagation steganography and such message are similar to spam messages; hence, they merely receive attention due to their frequent occurrence. Being that the “mimic algorithm” or “mimicry,” can be utilized for artificial spam messages generation, it has been classified as a propagation steganographic procedure. Such details may be linguistically wrong and could deceive spam filters statistically. Mimic texts, upon investigation, can easily be detected by humans while retaining the basic features of spam messages.

2.4.1.2 Image-based steganography

Concerning image steganography, the bearer enshrouding requisite details is an image. The general image steganography depiction is exhibited in Fig. 2.2. In Fig. 2.2., the concept “cover image” indicates the image that is employed to conceal the concealed details as a PC or “secret message”. This “Embedding procedure” is literally the algorithm or procedure employed to conceal the “secret data” internal to the “cover image” termed as “stego-image” or electively “stego-key”. Every party must possedd the electively “stego-key”. The “stego-image” indicates the ultimate outcome identity which obscures the vital details. In parallel, the equivalent of embedding has the possibility of extricating vital details, where the “extraction procedure” entails the technique to retrieve the “secret message” amidst “stegoimage” with optional “stego-key”.

2.4.1.3 Audio-based steganography

Here, audio files are used as the cover medium during stenographic processes [63]. The embedded messages in the audio-based steganographic techniques cannot be easily intercepted by intruders as they are hidden in a manner that made them imperceptible to the human ear [34]. It may be hard for some people to listen to tones that immediately follows a louder tone; hence, the secret data may be concealed through such scarcely distinct noises to conquer audio compression and to keep it from the human hearing system. Secret data can also be hidden in faint echo to delay their interception. Audio files for audio steganography can come in different formats, such as .wav, .midi, and .avi [23]. There are other available audio-based steganography techniques in the literature, such as parity, phase coding, echo hiding, and spread spectrum [64].

2.4.1.4 Video-based steganography

Video-based steganography uses videos as cover media. Given that videos are fundamentally several images in a sequence within a specific frame rate, they can hide information in ways similar to images. Discrete Cosine Transform (DCT) changes the estimates (such as 8.667 to 9) that are exerted when inserting data at the interiors of the images in a video. The mentioned approach typically ensures that the details are imperceptible by the human eye. Regular file formats for video-based steganography include .mp4, H.264, .avi, and .mpeg [65].

2.4.1.5 Protocol-based steganography

Here, network protocols are used as carriers during steganography. Typical protocols used include UDP, ICMP, TCP, and IP. In some hidden channels within OSI network layer models, steganography is applied in unutilized header bits at the interior of TCP and IP fields [66] .

2.4.2 Dna Based Steganography

DNA based steganography employs the randomness characteristics in DNA for secret data embedment; a contemporary technique used the numerical mapping table for DNA sequence mapping during secret data embedment [44].

2.4.3 Key Types- Classification Based

Three kinds of steganographic protocols were identified in [67]. Namely, pure steganography, secret key (SK) steganography, and public key (PK) steganography. Each of these protocols is described in the following manner.

2.4.3.1 Pure key steganography

This is a steganographic system that requires no stego key as a cipher; hence, it provides minimal security due to the reliance of the transmitter and receiver solely on random guessing and presumptions regarding the pattern of behavior of every individual to encipher the message. Such message may be restricted from sharing on social platforms or over the Internet [43].

2.4.3.2 Secret key steganography

Regarding secret key steganography, it is a steganographic system that works with a stego key; cover images are used in this technique and the stego key is kept masked. The details have the possibility of being deciphered by individuals with the private key. Being that secret key steganography relies heavily on the stego keys, attackers have the possibility to realize and react to the message with ease but despite this setback, the message can only be extracted by parties with the secret key [50].

2.4.3.3 Public key steganography

This form of steganography exploits the concept of public key cryptography; it utilizes both public and private keys to propagate hidden messages. The message sender may encode the message using the public key and provide the receiver with the private key to decode the message. Therefore, this may not be a secure approach for steganographic systems since several studies have focused on public key cryptography and several levels of security have been employed to address the concerns of parties that are not participating in the communication. But as soon as the attackers are aware of the communication and are alerted to this steganographic procedure, they may strive to crack the framework that holds the public key for interception of the hidden message [34].

2.4.4 Embedding Procedures- Classification Based

Three techniques for hiding information within cover media have been proposed in the literature, including insertion-based, substitution-based, generation-based and Cover look-up based techniques [67].

2.4.4.1 Insertion-based technique

The insertion-based procedure identifies locations in cover media prone to be disregarded by executing applications that can read the cover file and by choosing appropriate locations inside the media for embedding hidden messages. Given that this technique adds secret messages to the interior of the cover files, one usefulness of the insertion-based technique is preserving the original contents of the cover media. However, as one of its major limitations, the large size of the stego file may trigger suspicion. Therefore, the primary aim of the algorithms is to add secret messages without arousing the suspicion of attackers. An embedding element of most files is that they have a possibility of possessing a mark in either EOF or HTML[68].

2.4.4.2 Substitution-based technique

The substitution-based technique depends on interchanging the component of a carrier file with the secret message in a way that cannot be detected by attackers. This technique works by substituting some bits of information or by deliberately modifying the cover file while producing the least amount of distortion to the cover file. Consequently, the sizes of both the stego object and cover object become similar. To avoid suspicion, a suitable replacement process must be applied, thereby making it of necessity to select and restore just the unnecessary elements of the carrier file [13].

2.4.4.3 Generation-based technique

The generation-based technique disregards the use of a cover file and instead applies a generation engine that uses the secret message as an input to generate a file that appears to be regular and may be presented in text, music, or graphics format [11] .

2.4.4.4 Cover look-up-based technique

This technique looks for a pre-existing cover media so as the secret information embedment does not need to maintain anything within cover object. It supposes that it can find the appropriate cover object that already holds the desired secret data. Therefore, as the size of secret data increases, this solution becomes unusable very quickly. For example, if sending (20-bits) of secret information requires a million cover files, then (30-bits) requires a billion cover files [69].

2.4.5 Extraction Function Classification Based

Another classification of steganographic systems is based on whether the original cover media is utilized or not by the extraction procedure; on this note, they are classified into blind and non-blind schemes, respectively. However, this classification is not receiving much attention in steganographic literature [70].

2.4.5.1 Blind steganographic scheme

In these steganographic systems, it is assumed that the use of cover medium is not important for the recipient to extract the information. Hence, the original cover media is not required during the extraction process and the hidden information can be extracted from the stego media [5]. Consequently, it gives the sender party the opportunity to use any cover media even when it may not be accessible to the receiver party.

2.4.5.2 Non-Blind steganographic scheme

Here, the original cover medium must be available during the extraction process as the hidden content cannot be retrieved without it. Regrettably, this steganographic scheme has not received the attention of steganographers, despite its potential practical application. For instance, if the sender and receiver accept to utilize the same set of cover images, the informed extraction procedure would be helpful in embedding the hidden content in a less stressful manner. Hence, the detection probability would be reduced compared to blind embedding techniques.[69].

2.5 APPLICATION OF STEGANOGRAPHY

In the image steganography domain, many kinds of application exist, each based on their contributions, like protection of copyrighting, feature tagging, secure money transfer and security of communication [17][23]. Embedding in both copyright and watermarking happens within special areas of the image, such as intellectual property. For this reason, using the image becomes easy without permission via proving from the author. Modern stamping will be intelligent and may be involved within an image and other types of security as well, such as tagging, captions and elements of descriptive. During copy or transfer of the stego image, the factors of the identity have the chance to remain attached through transforming. Stego key implicit or explicit also keeps the information regarding the embedding within it during copying [20]. since all the secret data may not be included during the communication by steganography. Anyway, double checking is necessary before embedding to avoid hacking the system In the medical domain, crucial private data is hidden in the medical data itself. and the sequence of DNA and propagated. This will help to avert the leakage of private information in unauthorized hands [71][72].

2.6 PROPERTIES OF STEGANOGRAPHY

Every steganography system is evaluated in terms of its imperceptibility, robustness, payload capacity and security [74][75]. For the same reason, in the proposed study, we will solve the problem regarding these issues. Figure 2.4 illustrates the three essential properties for designing a steganographic system, which will be discussed in the following subsections.

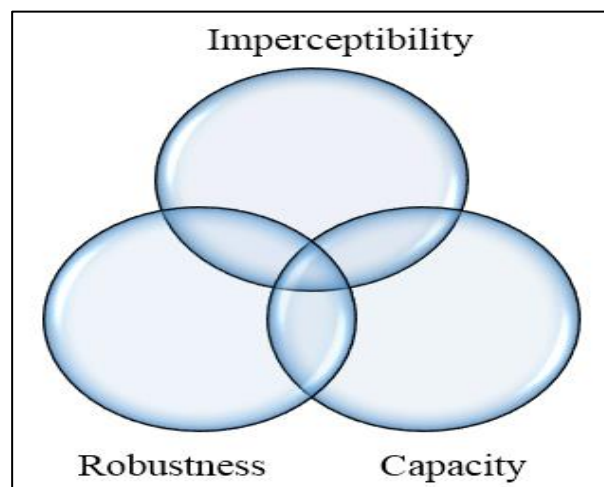


Figure 2.3: Properties of the steganographic system

2.6.1 Imperceptibility

The Human Audio System (HAS) and Human Visual System (HVS) is an invisibility attribute, so, no evident artefact should be abandoned when individuals fail to distinguish carriers possessing or lacking disguised messages [33][77]. The method for image quality evaluation is determined by peak signal to noise ratio (PSNR), which is calculated after the process of embedding to compare between stego image (result image) and the original image. The process of embedding message is obtained as image quality to Human Visual System (HVS) if the obtained result of (PSNR) calculation is equal or greater than 30db [54]. By applying the following equations, PSNR can be calculated.

$$PSNR = 10 \log_{10}(255^2 / MSE) \quad 2.1$$

where, MSE is the mean square error which is calculated by the following equation.

$$MSE = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (x_{ij} - y_{ij})^2 \quad 2.2$$

where, m and n are the images' sizes while x and y are the cover and stego images separately.

2.6.2 Robustness

In the secure embedded algorithm, the embedded secret message fails to be extracted after a genuine recognition happened by target censures, depending on complete comprehension of the embedded algorithm (omit knowing the secret key), [77]. The following is the list of different known approaches to the practical steganalysis.

- i. Visual detection.
- ii. Detection based on first order statistics (histogram analysis).
- iii. Dual statistics methods that use spatial correlation in images.
- iv. Higher-order statistics (RS Steganalysis).
- v. Universal blinded detection schemes.

- vi. JPEG compatibility steganalysis.
- vii. Some other special cases

2.6.3 Payload Capacity

Payload capacity is the portion of embedded data having the possibility of being masked into the enfold media as compared to the area of this cover. There is a trade-off between the size of the embedded secret and the cover signal distortion (Hussain et al., 2018). The techniques for data embedding process are either with high embedding rate or with high resistance with the modification, but not all of them. If one of them is increased, the other will decrease(Jain et al., 2012). The bitplane tool technique uses Least Significant Bit (LSB) insertion and manipulation of noise. The mentioned steganography approaches are commonly used and are easy to apply for images or audio. The LSB substitution mechanism is used for embedding data with high payload capacity while keeping the high imperceptibility of the stego-image [78].

2.7 Embedding Domains of Image Steganography

Embedding domains in steganography systems can be categorized into three classes depending on the hosting places and nature of the embedding process (Spatial domain, frequency domain and adaptive domain, which is essentially interlinked to spatial and transform domain, where each of these categories has its advantages and disadvantages. The comprehensive differences between these domains are shown in Table 2.1 [12][19].

Table 2.1: An overall comparison of spatial and transform domains with adaptive embedding methods

Characteristics	Properties	Domains		
		Spatial	Frequency	Adaptive
System type	Complexity	Simple	Complex	Depends on adaptive algorithm
Pixel Manipulation	Embedding	Direct	Indirect (transformed coefficient)	Depends on adaptive technique
Embedding Capacity	Payload	High payload	Limited payload	Varied payload
Visual Quality	Imperceptibility	High	Less controllable	Highly controllable
Robustness	Compression, Noise, Cropping, Rotating, Filtering	Highly prone	Less prone	Depends on adaptive algorithm
Security	Attacks	Vulnerable to attacks	Resistant to attacks	Hard to attacks
Statistical detection Attacks/analysis	RS, Histogram	Easy to detect	Hard to expose/unsuccessful	Hard to expose/unsuccessful

2.7.1 SPATIAL or Map Domain

Pixels intensity is used here to insert or embed the secret message. This type or class has many advantages for embedding; for instance, it increases the capacity (no limitation), reduces complexity, therefore, imperceptibility of the hidden message is ensured [54].

2.7.2 Frequency Domain

In this regard, the given image will be changed or transformed into frequency class (domain) before embedding the secret message in the coefficient factors. The benefit of using frequency domain is robustness against statistical attacks but in other hand, it suffers from very low capacity. In literature, spatial domain is widely used because of its simplicity and more efficiency [13].

2.7.3 Adaptive Domain

While revisiting the contributions of image steganography studies, the study fails to overtake the impact of adaptive techniques. It is a particular case of spatial and transforms domains. Adaptive *steganography* is sometimes termed as “Model-Based”.or “Statistics-aware embedding” or “Masking” [11][13]. Many of the previous work in steganography lies under this section. Adaptive nature can be introduced in the information hiding methods in different ways: in choosing the target pixels in the cover image, nature of modification to be made, number of bits embedded in a pixel, etc. Based on the nature and mode of adaptiveness offered by these methods, they can be dividing into a few sections. This includes Region-based Steganography, HVS based the Steganography, Artificial Intelligence and Machine Learning Techniques based Steganography.

2.8 STEGANALYSIS METHODS

Among the attack types listed in the above table, the known message attack may be surmised from an algorithm that produces a stego file with a hidden message. Therefore, this algorithm has chance of being utilized for detecting and extracting hidden messages. In a certain message strike, the striker inputs varying messages to the interior of the cover media into numerous algorithms with an aim to check whether the stego file possesses certain elements that resemble the unitary objective of the employed algorithms. All the aforementioned attacks may be categorized into visual attack (Human Visual System), structural attack, or statistical attacks (Chi-Square, Histogram, RS attacks) [13][29] as condensed in Figure 2.5.

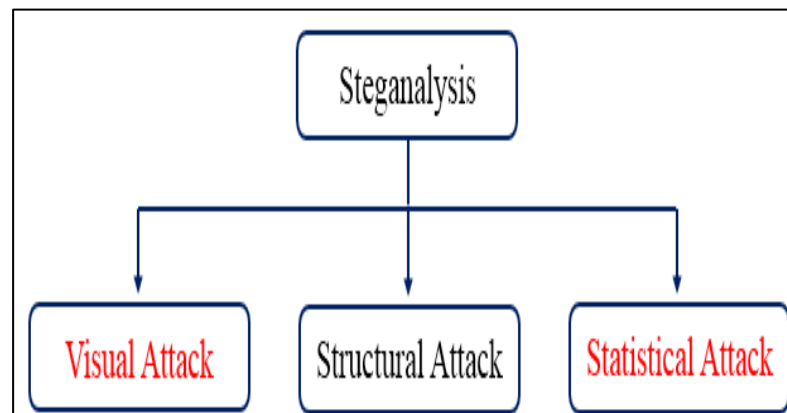


Figure 2.4: Types of steganalysis attacks [12]

2.8.1 Human Visual System (HVS) Attack

One of the famous attacks in both steganography and watermarking structure is Human Visual System Attack (HVS). The mentioned attack is working under the condition of checking the frequency of pixel bits within the identity, which is visible to the human eye. During the embedding of secret message within the process of steganography, it is either done sequentially or randomly. The bits of the secret message are embedded inside the image independently. Decomposition of the stego image allows the user to check bitplanes of the image and the secret message is always hidden in the first bitplane; however, individuals have the possibility of recognizing the hidden message in this layer. In the relayed identity, the LSB of the pixel represents the first bitplane and it is out of the question to recognise between stego image and noised image. In spite of the ordinary technique used in this attack, it is not easy to distinguish the distribution of bits spread out of the image, therefore leading to the same difficulties of distinguishing between random bits in the LSB of the pixels.

2.8.2 Chi-Square Attack (X^2)

Chi-Square (X^2) is statistical attack; it evaluates stego images before sending through the channel. This type of attack applies mathematical formulas on the image; this attack is more effective than HVS attack. To measure the perceptibility of the hidden data, Chi-square attack is used. Pairs of Values (PoV) frequencies are compared inside the image concurrently; the observed frequencies of the hidden details are also checked. The sequence of PoV values located in LSB is changed and transferred to the other location, and vice versa. Chi-square attack is always used when the original media is unknown; unfortunately, the amount of data hidden in the image cannot be determined. Chi-square attack works by finding the frequencies of bits in LSB (or bitplane (1)), then, Pair of Values (PoVs) will be checked. In spatial domain, most of the embedding methods apply on the LSB part of the pixels in the picture to conceal the secret details. In case the bits in LSB are overwritten and disseminated over the cover image, thereafter, PoV in Chi-square becomes equal [79]. The main idea here is to check and compare the observed distributed bits of the sample with the expected distributed frequencies. By taking the summation of both the expected and observed frequencies, Chi-square can take the action. For the entire image, Chi-square shows the difference of between the observed and expected values. This type of attack

illustrates the probability of embedding in certain areas, but the result does not show whether the results are correct or not. This is theoretically explained thus:

$$X^2 = \sum_{for\ all\ images} \frac{(Observed-Expected)^2}{Expected} \quad 2.3$$

Most of the time, Chi-square comes when other attacks, such as HVS strike does not locate concealed messages within the carrier. Figure 2.6 shows two types of attacks.

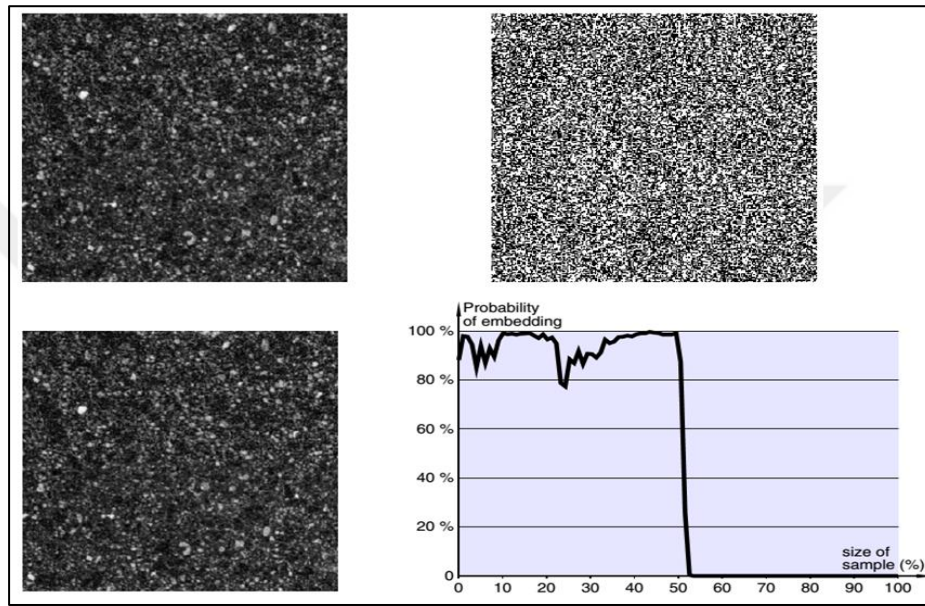


Figure 2.5: Model for both types of HVS and Chi-square attacks [22].

The images in Figure 2.12 shows how the HVS attack fail to establish whether the image contain the secret message or not (because there is no pattern in bitplane (1)); HVS attack considers the LSB part of the pixels because it contains the secret data while the MSB part is removed. HVS checks Layer (1) and draw the pixels to see if there's a pattern or not via human eye. However, chi-square strike discovers that 50% of the image possesses concealed details having greater chance because this attack considers the frequencies of the data embedded in LSB part of the pixel by adding pair of values to the pixels to check the probability; if more than 25%, that means there is a secret data hidden inside these pixels.

2.9 DATA PREPARATION

In term of preparation, both the secret text and the cover image to be embedded needs to be prepared before embedding. The image needs to be suitable for hosting the secret message in a way that will rearrange the priority of the pixels inside, while the secret text needs some

manipulation to be ready for hiding inside certain images. Table 2.2 explain the data preparation in the proposed study.

Table 2.2: Data proration of the proposed study.

Text Preparation	a. Prepare the secret text using Huffman coding, to decrease the size of the secret text (original message) to achieve a high payload capacity which is one of the main objectives of the proposed study.
	b. Image Normalization.
Image Preparation	c. Fibonacci Decomposition: To change the biplane of the given image from 8 bits to 12 bits to achieve a high robustness, which is one of the main objective of the proposed study

2.10 STEGANOGRAPHY VS CRYPTOGRAPHY

Cryptography or secret writing is a method where a secret method is converted into the ciphertext and sent to another person who then decrypts the ciphertext into plain text. Cryptography can be classified as Symmetric key cryptography or Asymmetric key cryptography. While steganography is the practice art of hiding data (in any form — text, image, etc.) in plain sight within another object. This process allows you to transmit information undetected, without arousing any suspicion. At the same time, the first recorded use of steganography can be traced back to ancient Greece, Johannes Trithemius 1499 [5] who, with his book Steganographia, officially gave it a name. Over the years, and as a result of technological advances, digital steganography has gained popularity. Following are some of the important differences between Steganography and Cryptography.

Table 2.3: Differences Between Steganography and cryptography

No.	Key	Steganography	Cryptography
1	Type	Steganography refers to Cover Writing.	Cryptography refers to Secret Writing.
2	Integrity	Structure of data remains same.	Structure of data can be altered.
3	Attack	Attack in Steganography is termed as Steganalysis.	Attack in Cryptography is termed as Cryptanalysis.
4	Security Principles	Steganography supports Confidentiality and Authentication.	Cryptography supports Confidentiality, Authentication, Data integrity and non-repudiation.
5	Parameter	Steganography requires a parameter like key call stego key.	Cryptography needs any key used with method.

2.11 SUMMARY OF WORKS OF LITERATURE REVIEW (2015-2022)

Over the decades, numerous traditional image steganography techniques have been introduced for secure data transmission over the WWW which are briefly summarized in this section. In addition, the salient features of the full steganography frameworks are presented. These study summaries the spatial domain only. Several recent studies related to the steganography in terms of the capacity and the corresponding PSNR are listed in Table 2.5 (between the years 2015 to 2022).

Table 2.4: Summary of Related Work from 2015 – 2022

Domain	References	Method	Remarks	Performance
Spatial Domain	[40]	LSB- MBP: Block-based multi bit-plane adaptive LSB embedding method.	-AES and RSA key maintenance dependency for encryption. -No robustness against compression, filtering and cropping.	46 dB 1.5 BPP
	[55]	MF-PVD:	-Weak against statistical steganalysis. -Low embedding capacity	36 dB 1.03 BPP
	[64]	LSB - MLEA: Multi-level encryption applied on stego-key as well as secret data.	-Limited embedding capacity (EC). -Limited robustness.	> 45dB 1BPP
	[24]	PVD-TPVD:	-Lack of security -Weak against statistical attacks	38.33 dB 2.14 BPP
	[74]	LSB: CM LSB method that used chaotic map-based ISS. Chaotic sequence is generated using a 1-D logistic map and the secret bits embedding is based on this generated sequence	- Low payload capacity. -The robustness of the presented system is suspicious as the secret bits get scrambled while undergoing any lossy compression or geometrical attacks	44.53 dB 2 BPP

Table 2.4: Summary of Related Work from 2015 – 2022 “Tables continued”

Domain	References	Method	Remarks	Performance
	[47]	Bit plane + Histogram The pixel intensity values are divided into 2 based on the bit-plane values and histogram-shifting based embedding is used over the histogram bins separately.	Lack of defense against an intruder (statistical) attack	40 dB 5.0 BPP (High EP)
	[61]	PVD: Adjusting the Tri-way PVD by finding the best value of each pixel pairs where their difference affords the extreme information without dropping any	-Low robustness against compression and statistical attacks -Lack of Security -Less visual quality	37.63 dB 2.7 BPP
	[7]	LSB- Edge Area Canny and Sobel detectors are combined to get a wider edge area to increase the payload capacity	-Low robustness against compression, filtering and statistical attacks.	50.21 dB 1.03 BPP
	[60]	PVD: An enhance the Tri-way PVD technique by getting an optimal pixel value for each pixel pair.	-Less visual quality -Lack of Security	37.81 dB 2.41 BPP

Table 2.4: Summary of Related Work from 2015 – 2022 “Tables continued”

Domain	References	Method	Remarks	Performance
Spatial Domain	[4]	PVD: PVD method with 1×2-pixel blocks in overlapped fashion	-Less visual quality -Lack of Security	42.96 dB 2.96 BPP
	[9]	PVD- MF ISS based on PVD and modulus function (PVD) to enhance the peak signal-to-noise ratio (PSNR) and embedding payload (EP).	-Low embedding capacity -Less visual quality	42.04 dB 1.5 BPP
	[1]	PVD: A pixel value difference-based text encryption and random pixel section.	-Low visual quality - Lack robustness against filtering and scaling	41.59 dB 2.94 BPP
	[3]	LSB: Least significant bit-based secret map techniques via applying 3D chaotic maps, namely, 3D Chebyshev, and 3D logistic maps	-Low visual quality - Low embedding capacity.	46.15 dB BPP

2.12 SUMMARY

Nowadays, the term steganography has become important in research as different methods have been suggested to address the issues of steganography using various embedding methods. In the past decade, information hiding witnessed rapid development. Some explanations on the techniques related to the spatial domain descriptor used in literature are based on their embedding techniques. In the current thesis, many studies that are based on different embedding methods with varying message preparation techniques were reviewed. Reliable embedding methods such as edge detection, LSB substitution, and histogram were reviewed as well. Detailed literature survey on the strength of the proposed idea was also conducted. In the end, brief notes were provided in chronological order regarding the relevant studies reviewed in this research.

3. METHODOLOGY

3.1 INTRODUCTION

This chapter goal is to demonstrate the proposed research methodologies to execute the research objectives. To perform an image steganography system, there are four main stages used to accomplish the task of concealment starting from data pre-processing which includes secret bits in addition to the cover image that will be hosting the secret bits. The generating framework of the proposed system was discussed in detail with illustrated figures. The researchers competed to suggest several methods and software for concealing information that is appropriate to the complexity of the great revolution that arose in the field of communications technology. The current study showed two active contributions, through which the gap that was achieved through previous studies can be reduced. The first contribution relates to the first stage of the image steganography system (pre-processing), where secret text and cover image preparation will be accomplished in this stage. To improve the payload capacity and the enhance the security level of the secret text the Huffman coding algorithm is used to compress and fragment the secret text before the embedding stage and backtracking fragments of the secret text to reduce the change in pixels of the image. To improve the robustness of the proposed steganography system Fibonacci decomposition is logically converted to the number of image pixels from 8 to 12 bits, as this tool adds a better level of robustness to the proposed system as the intruders are not familiar with this tool [40]. The second, contribution is used with embedding stage, where embedding the secret data by sorting the bits of the secret message (as 0s and 1s) for matching with the pixels, to avoid changing in pixels' value. Four main stages are considered in this methodology, starting with the preparation stage which prepares data and images before embedding. Then embedding secret data within selected pixels in image, the third stage is the evaluation stage, where the stego image will be compute utilising the PSNR, as well as attacking the hosted image using two types of attacks Human Visual System (HVS) attack and Chi-square attack (X2). The last stage includes extracting stage which extracts the secret bits from the steg image. A comprehensive explanation will discuss later.

3.2 FRAMEWORK

The goal in this study is to enhance Image Steganography specially in term of payload capacity using many secret message sizes. A secret message is analyzed and prepared to embed with image. The major objective is shown in the embedding process that makes concealment of the secret data or message to pixels with Fibonacci decomposition while less different in value. As a result of this stage is stego-image is looked like an original image that conforms to a high imperceptibility. The evaluation stage contains three main types of evaluation, PSNR is related to distortion of the image, better PSNR means better image quality. Finally extracting stage to extract the secret message from stego-image this process is located in the receiver part. As shown in Figure 3.1.



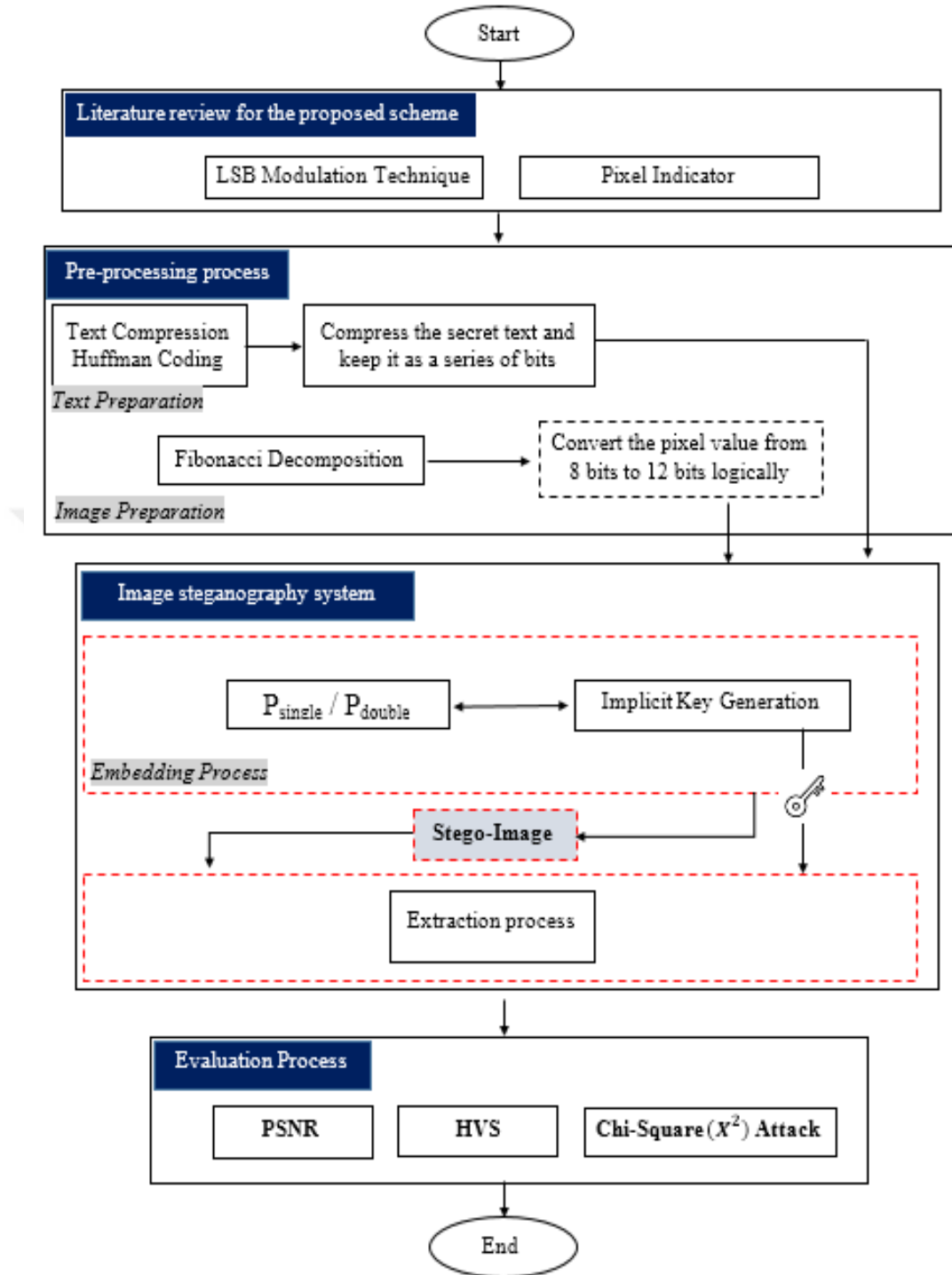


Figure 3.1: Research framework

3.2.1 Proposed Method

In this section, we will cover the state of arts that were studied during the stage of exploring the research gap related to the information hiding system. Least significant bits (LSB) and pixels indicator are the most important method which we have to discuss in the following sub-sections.

3.2.1.1 Least significant bit (LSB) steganography

Most of the steganography systems use the LSB substitution for the secret message embedding. Huang et al. [34] proposed a new system using the LSB substitution for the message embedding via the “Optimal Pixels Adjustment Process (OPAP).” The main aim was to improve the quality of the stego image containing the secret data and minimize the computational complexity wherein four LSB bits were changed to hide the information. The achieved PSNR value was 51 dB. Another method based on the adaptive LSB substitution steganography was suggested (Bharti et al., 2019). In this method, the image was divided into non-sensitive and sensitive parts based on the texture analysis. The majority of the bits in the non-sensitive area were used for bearing the secret message and other bits in the sensitive area. The main supremacy of this procedure was to achieve greater payload magnitude with imperceptibility. In [25] introduced new steganography based on the LSB method for embedding the secret message by normal LSB bit position in the cover image. Inversion of the pixels before embedding was the main contribution of this method which achieved high capacity and PSNR. Recently, an robust color image LSB steganography method has been presented by Pak et al. (2020) using the improved 1D chaotic map. The proposed study confirmed a high accuracy and better performance than the standard LSB embedding. The results revealed improved robustness against statistical analysis attacks. The existing methods based on the LSB are simple due to the variation of the LSB bits of the pixels, but they lack capacity and security. Figure 3.2 shows the basic mechanism for the 1-bit LSB embedding technique.

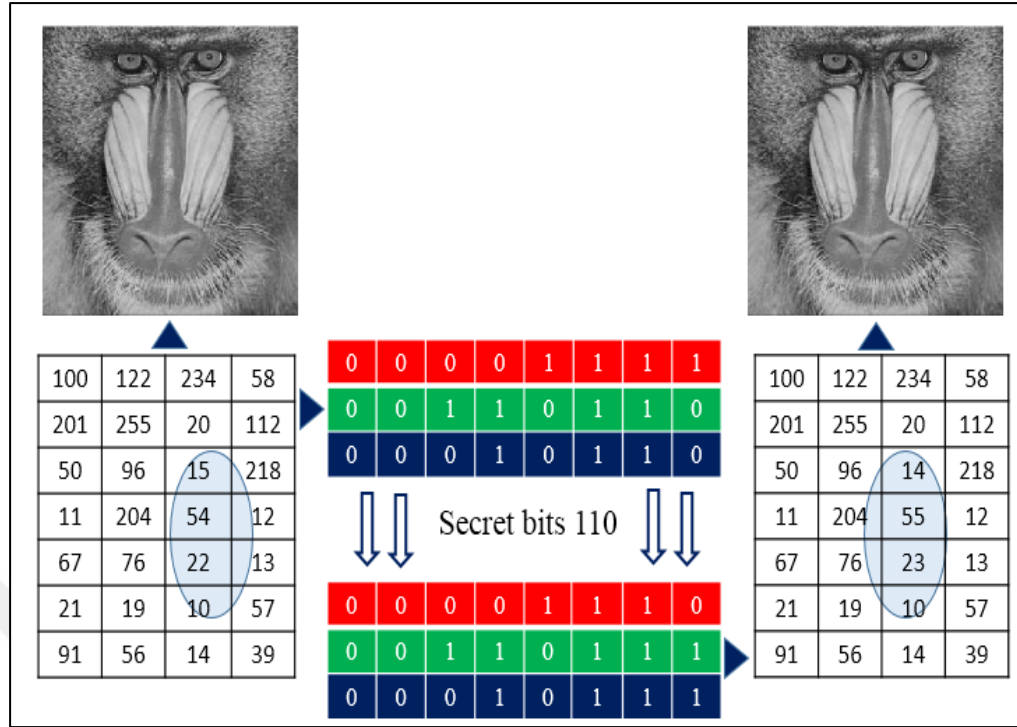


Figure 3.2: The basic mechanism for the 1-bit LSB embedding

3.2.1.2 Pixel indicator

The pixel indicator refers to addressing pixels index within the image, where this index is stored as mapping to be used further [39]. The index processes the pixels in the group due to the presence of a distribution of the pixels over the image. This is because each pixel has a special address in the image and cannot change it without mapping the pixels into the special table or vector. The pixel in general has two main things such as the address and value, wherein the pixel indicator deals with the address and cancels the value until the embedment is completed.

3.2.2 Data Pre-Processing

The proposed method two stages used preparation (pre-processing). Firstly, preparation of the image and then preparation of secret data as well image normalization. The procedure of image normalization is used in the case that the secret message is hidden in a non-standard image (an image taken by digital cameras), while this procedure considers useless by researchers who deal with the image steganography system in the case that the secret message

is hidden in the standard images (USC-SIPI database). Equation 3.1 explains the image normalization process.

$$Image_{(N)} = (Image - Min) \frac{new\ Max - new\ Min}{old\ Max - old\ Min} + new\ Min \quad (3.1)$$

Where $Image_{(N)}$: Normalized Image.

Image: Original image.

Min: Minimum Range.

Max: Maximum Range.

Where this normalization should be used in the case we use non-standard images, an image captured from (smartphone or digital camera), in the current study, SIPI dataset standard color, and gray images were used, so no need for image normalization. The Fibonacci technique was used to convert the value of image pixels from 8 to 12 bits, as this indicates the increase of robustness and payload capacity [36]. This chapter includes a detailed explanation of the tools that have been used in the proposed system that help the P_{Pixel_s}/P_{Pixel_d} method to increase payload capacity while maintaining the other key issues like (Security and imperceptibility).

3.2.2.1 Secret data preparation

The secret text preparation related into three parts such as compression, change the form of secret text bits instead of the binary form (0, 1) and secret bits fragmentation. The secret text was generated randomly in different lengths using all the alphabet letters where the length of the shortest one had 5500 letters and the longest one composed of 56428 letters (Sun 2016). The secret message was first compressed and then transformed into the new form streams of bits. The Huffman algorithm will be applied to the secret text before the embedment and before changing the form of the secret text. This algorithm will be used to compress the secret text of the steganography scheme. The compression of the secret message enabled the reduction of the message size that will be hidden inside the cover image.

The process of the Huffman algorithm has a secret code via the Huffman dictionary and the results achieved after the compression process is the vector of the secret codes. In this stage,

three different processes are obtained as seen at figure 3.3. It is important to make the sequence for this stage to get better performance results.



Figure 3.3: Secret Text Preparation in Proposed Method

The main objective of the Huffman coding method is to minimize the size of the secret data before concealment process (embedding) it into the given image. Figure 3.4. is demonstrated Huffman coding process using the Huffman tree.

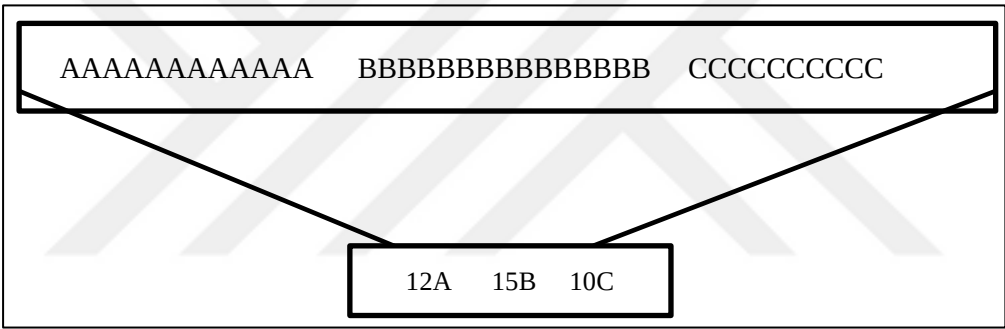


Figure 3.4: Huffman coding and text frequency reducing

The PC is an important concept in the steganography system to make the system more acceptable, such as a better system that can hold a high amount of data inside the hosting images while maintaining the quality of the image represented by (PSNR). For the concept of data management and transfer protocol compression of information transferred from sender side to receiver side is very useful besides other techniques used in this research. Figure 3.5 shows a simple flowchart of Huffman coding implemented in this work.

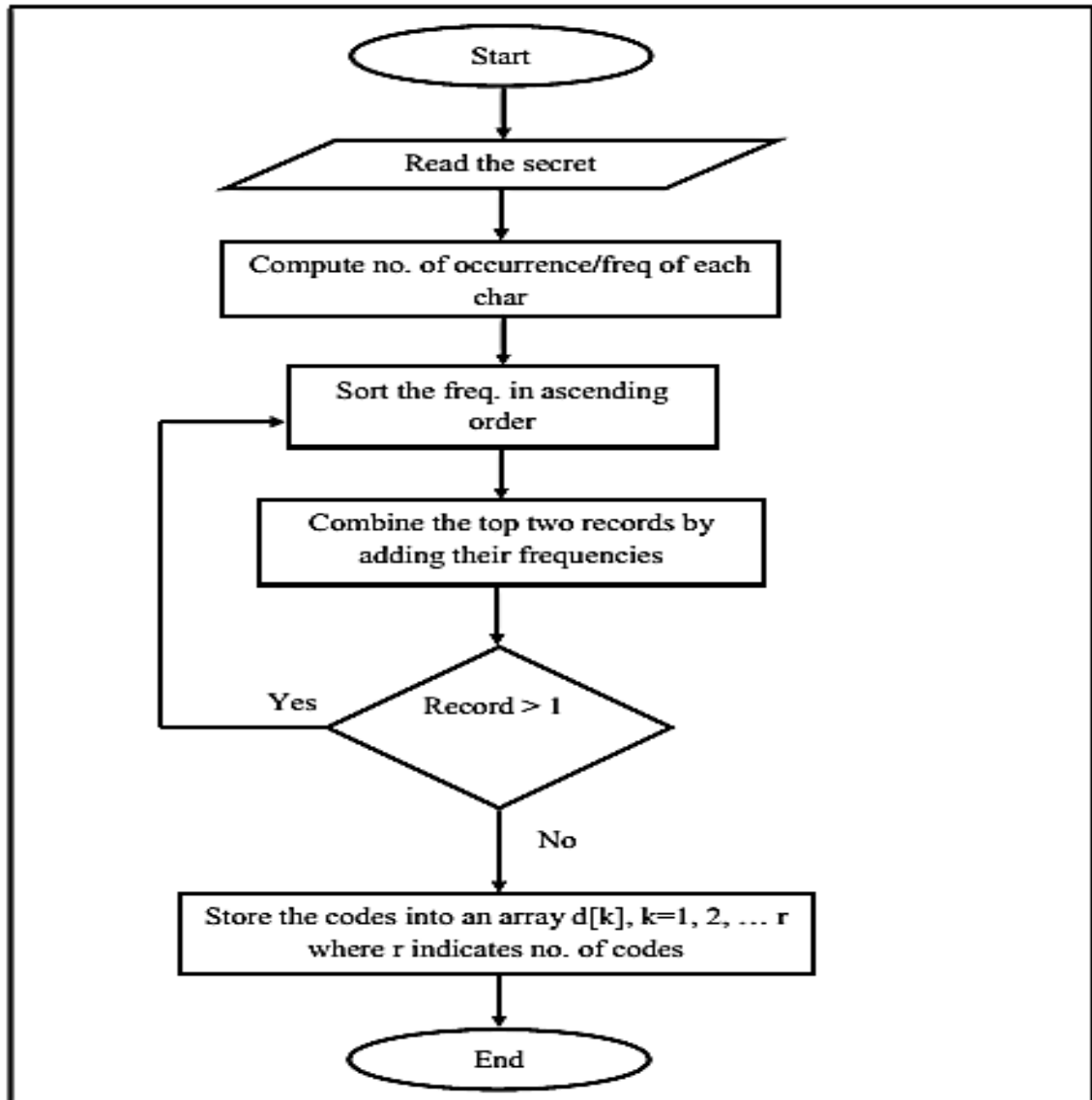


Figure 3.5: Flowchart of Huffman coding

For more illustration numerical example will be provided to explain how Huffman will work within the proposed system. This example uses five different symbols as:

Symbol	frequency
F	22
G	10
H	8
I	6
J	6

Starting with "J" and "I" for the less frequency to build tree structure for the first branch and follow by "G" and "H" at the same level. These parent nodes have the frequency of 12 and 18 respectively. Each parent node accumulates the frequency of their children in the tree. For our example, the high-frequency letter "F" will be created at a high level to construct the final tree that will connect both children in one-parent with frequency 52. As illustrated in Figure 3.6.

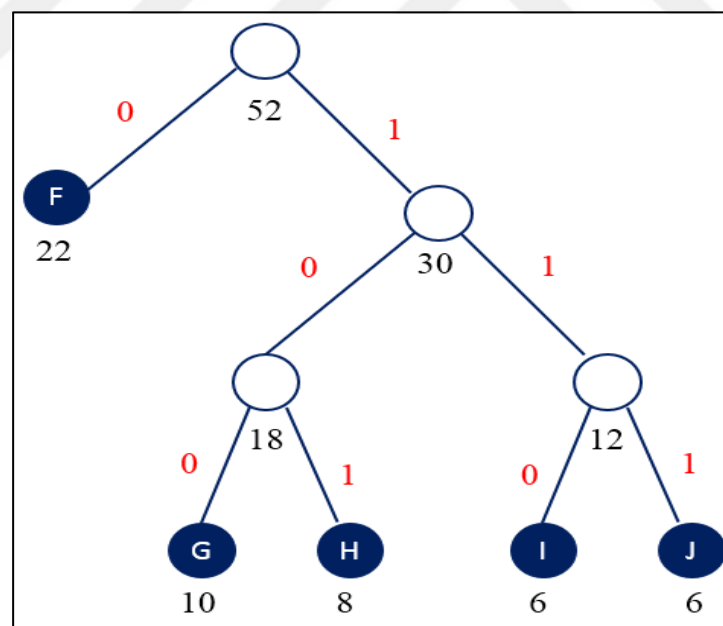


Figure 3.6: Huffman coding tree

The frequency will be reduced and the compression for this example getting off to the 42% from original text. (If the same frequency of letters).

Symbol	Frequency	code	length
-----	-----	-----	-----
F	22	0	1
G	10	100	3
H	8	101	3
I	6	110	3
J	6	111	3

Chart 3.1: Huffman coding

Input: Array $f[1...n]$ of numerical frequencies or probabilities

Output: Binary coding tree with n leaves that has minimum expected code length for f .

`huffman( $f[1...n]$ )`

T = empty binary tree

Q = priority queue of pairs $(i, f[i])$, $i = 1...n$, with f as comparison key

For each $k = 1...n - 1$

$i = \text{extractMin}(Q)$

$j = \text{extractMin}(Q)$

$f[n + k] = f[i] + f[j]$

`insertNode( $T, n + k$ )` with children i, j

`insertRear( $Q, (n + k, f[n + k])$ )`

Return T

Due to the secret bits in the steganography method is always in the form of text, thus Huffman algorithm is useful in terms of compression and increases the payload capacity. Three conditions should be taken into our consideration to get a better steganography method which is: maximum payload capacity, imperceptibility (visual quality of the image that includes the secret), and robustness (Akhtar, 2016). So that to achieve the first condition Huffman coding is used.

In compression theory and computer science, Huffman coding considers lossless data

compression. In Figure 3.7 the second process is the fragmentation of the bitstream, after the Huffman coding process the text produced will convert into a digital form of 0,1. The process of stream bits depends on how long of bits provided to the embedding stage, manipulate the bits before embedding it gives the reliability to the method. The data hiding to the image especially when a down payment of bits should be processed as one packet and break from original bitstream Figure 3.7.

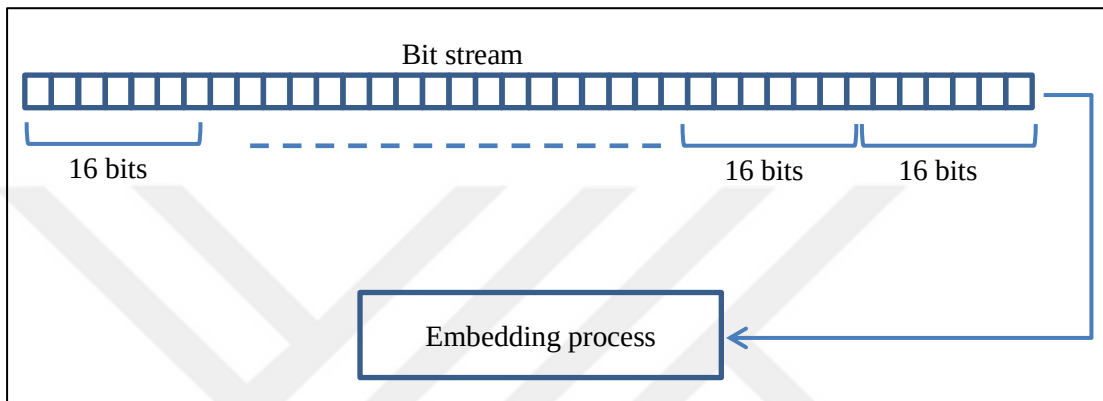


Figure 3.7: Bits stream Fragmentation in proposed method

There are different disadvantages and advantages to selecting fragments as large or small fragments. The small one makes concealment (embedding) easy but leads to reducing the image quality (imperceptibility) at the same time. For large one is hard to concealment (embed) but will get better PSNR (better imperceptibility). All the data collected will store in the key that will generate during the process in two stages preparation and embedding stages as shown in Figure 3.8.

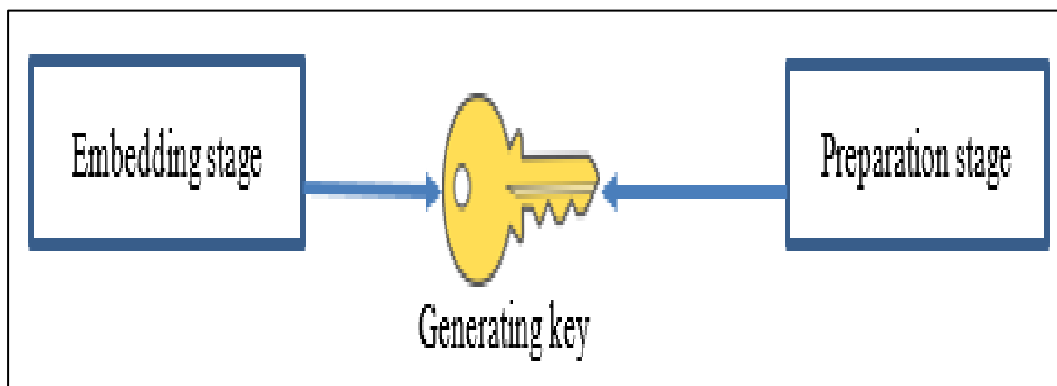


Figure 3.8: Generating key by two stages

The last process in the secret text preparation phase is the backtracking check (Figure 3.2) which is responsible for checking the match between bits of a given text message and LSB pixels value. In this regard, checking should be managed by results that come from comparing the values of pixels with secret message bits. Two important things in this process, are the first condition of a stopping point in the bitstream and how long of bits should go back to satisfy the next point. The recursive moving may be static or dynamic according to returns of this function as shown in algorithm 3.2.

Chart 3.2: Recursive bit stream function

```

Input:  $n$  is the length of bit stream and same function when recursive
Output: null that is the same previous output
Function recursive{
    For (  $i=1$  to  $n$ ) do
        {   If   place  $a(n)$  then
             $n=n+1$ ;
            return ( $n$ );
        Else   recursive;
        } return (null);
}

```

Every action taken by these processes achieve two objective capacity and security that are needed in the steganography system. The main objective in this stage (secret text preparation) is capacity and Huffman coding algorithm achieves this objective perfectly.

3.2.2.2 Cover image preparation

The least significant bits (LSB) steganography method considers one of the easiest spatial domain techniques that are able to embed highly secret bits directly into the LSB plane bit of the hosted image without noticeable visual distortions [80]. Change in the data on LSB is not recognized by human eyes as the amplitude of such change is very small. Every embedding method has its own pros and cons, and LSB also has weaknesses in filtering or any manipulation which occurs to the image [13]. Most effort for embedding method goes to keep

the image with high PSNR (Peak Signal to Noise Ratio) to prevent the attacker from noticing if there is a secret in an image. This is because if the pursuer detects any secret in an image, and even if he cannot extract the secret message, he can delete the secret by deleting the LSB plane of the image. The importance of LSB is less than Most Significant Bit (MSB) because changing of LSB does not affect the quality of the image as shown in Figure 3.9.

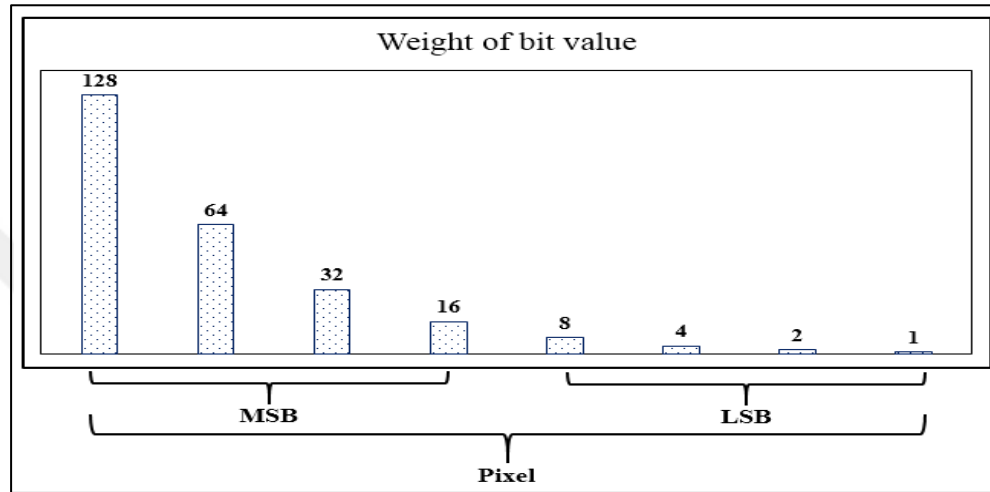


Figure 3.9: Bit value weight based on LSB and MSB

Most of the previous spatial domain studies used the LSB technique, each of which has its own contribution to agreeing to the development or design of an embedding method but not the location of embedding. Obviously, hiding the secret data will be in the LSB part of the image, image before embedding is called cover image while after insertion the secret message is named stego image. It is very important that the stego image should not contain detectable artifacts because of message insertion. The Colour image consists of three channels, Red, Green, and Blue [7]. While gray images consist of just one channel [17]. The embedding process with a gray image is better than the color image as it is less detected by Human Visual System (HVS) but a good method can embed the secret with two types of images with the same robustness. For color pixels, three LSBs channels are used for embedding data, and one LSB channel is used for grayscale pixel as shown in Figure 3.10.

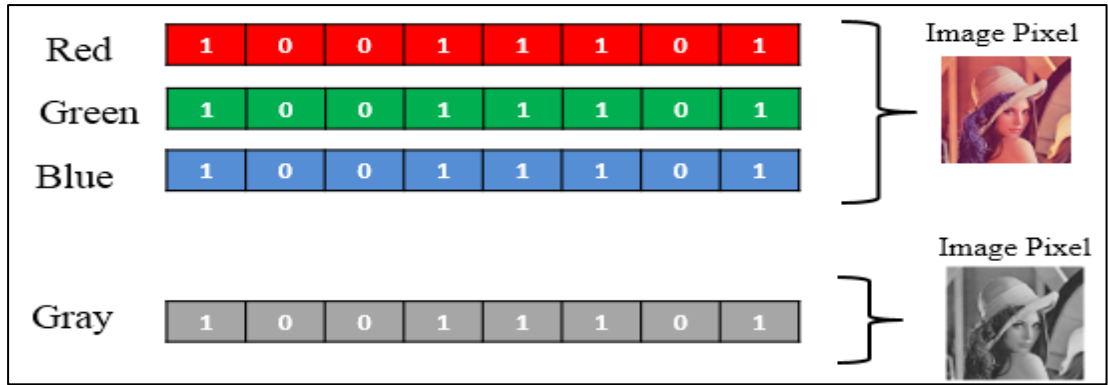


Figure 3.10: Pixels of colour and gray image

The normal distribution of most previous studies for binary images is 8-bit plane and the embedding will be in the LSB bit plane 0 of each plane as illustrated in Figure 3.11. While in the present study Fibonacci decomposition is used to transfer the 8-bit planes of image pixels to 12-bit planes logically. This section will provide a detailed explanation of the Fibonacci decomposition technique.

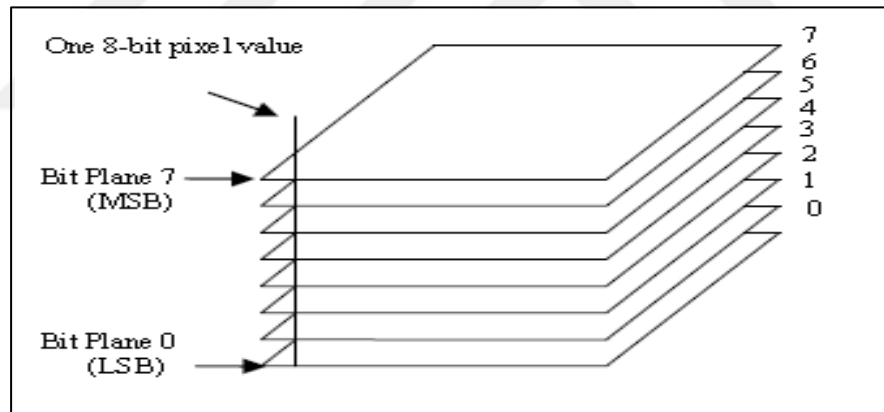


Figure 3.11: 8-bitplane distribution in gray image

Fibonacci decomposition [43] is a logical sequence number utilized to present the decimal number of the pixel values that consists of two previous numbers summation. It is utilized here to increase the robustness and security of the method. With Fibonacci decomposition, the proposed system that will be based on pixels' grade value will be more secure and robust. Fibonacci is the summation of the previous two numbers in the sequence except for *the first* and *second numbers*. The Fibonacci analysis and decomposition works, and the procedure are shown within Figure 3.12.

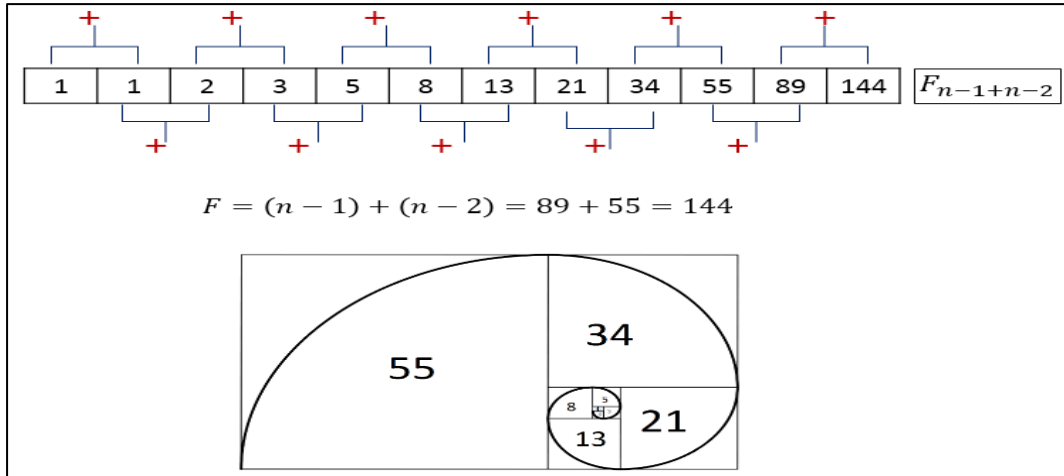


Figure 3.12: The Fibonacci sequence number

To enhance the efficiency of embedment the privet message, the Fibonacci technique was used [81]. The bit-plane of the cover image is 8-bit-planes because to binary presentation. Thus, implementation Fibonacci decomposition will become 12-bit-planes to make it better for the embedment procedure in consideration of the image quality (*imperceptibility*) of embedding result (*Stego Image*). With Fibonacci number, the impact value of each bitplane of binary representation is equal to (2^k) , where k present the bitplane order (ex: ($k=3$) for bit-plane number 3, ($k=7$) for bit-plane number 7 and etc.). Table 3. 1 present the impact value of each layer in the binary presentation.

Table 3.1: The Binary Bit-plane within the Image

Biplane No.	1	2	3	4	5	6	7	8
Impact value on image luminance	1	2	4	8	16	32	64	128

The difference among 8-bit-plane and 12-bit-plane is that the hiding procedure will become in LSB as 12-bitplane is more efficient and robust. The difference among these two bit-planes was presented in Figure 3.13.

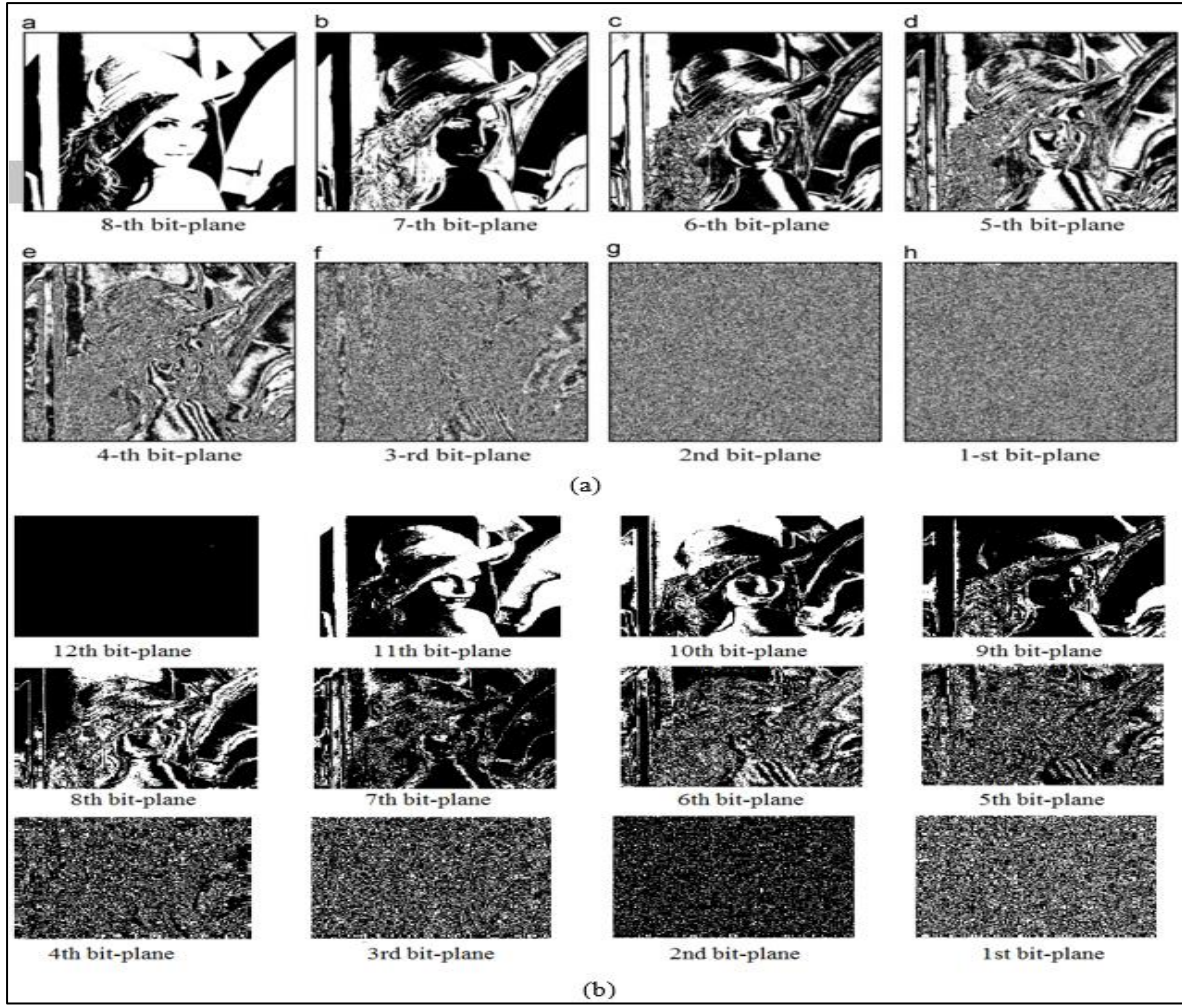


Figure 3.13: Decomposition for Lena image in (a) 8-bit-plane and (b) 12-bitplane in proposed work.

For the bitplane (1), we considered the difference in the result, where Fibonacci decomposition process darker images than with binary presentation, that means the number of zeros is greater than with Fibonacci analysis. To illustrate the technique of analysis of any pixel value from decimal representation to Fibonacci presentation utilizing Fibonacci number sequence and applying Zeckendorf's theorem on this sequence. The general equation of the Fibonacci number sequence is given as [36]:

$$F_1=1, F_2=1, F_3=1+1=2, F_4=2+1=3, F_5=3+2=5 \dots, F_n=F_{n-1}+F_{n-2}.$$

In general,

$$F(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F(n-1) + F(n-2) & \text{if } n > 1 \end{cases} \quad 3.2$$

For more detail, a numerical example is provided. Zeckendorf's theory [42], addressed the variety between Fibonacci and decimal values. Whereas Fibonacci consisted of twelve stages, the last stage of Fibonacci's series is zero. If the Fibonacci value was greater than the value of converted decimal, then Fibonacci is zero. But, if the Fibonacci value equaled the value of converted decimal, Fibonacci is equal to zero. However, when the Fibonacci value was less than the value of converted decimal, the value of Fibonacci equals one, and the value of the decimal number should be subtracted from Fibonacci's value. Therefore, the next Fibonacci value will be zero. To illustrate Zeckendorf's theory, the example below is to analyze decimal numbers according to Fibonacci decomposition analysis: the decimal number (150), when analyzed with Fibonacci numbers follows the underneath procedures:

233 144 89 55 34 21 13 8 5 3 2 1

- 1- 150 < 233 → F=0.
- 2- 150 > 144 → F=1.

According to the Zeckendorf's theory [82], when Fibonacci value was less than the value of converted decimal, the value of Fibonacci equals one, and the value of the decimal number should be subtracted from Fibonacci's value.

150 – 144 = 6 The modified decimal value.

According to the Zeckendorf's theory [82], the next Fibonacci value will be zero.

- 3- F=0.

- 4- $6 < 55 \rightarrow F=0.$
- 5- $6 < 34 \rightarrow F=0.$
- 6- $6 < 21 \rightarrow F=0.$
- 7- $6 < 13 \rightarrow F=0.$
- 8- $6 < 8 \rightarrow F=0.$
- 9- $6 > 5 \rightarrow F=1.$

According to the Zeckendorf's theory (Bower et al., 2015), when Fibonacci value was less than the value of converted decimal, the value of Fibonacci equals one, and the value of the decimal number should be subtracted from Fibonacci's value.

$$6 - 5 = 1 \text{ The modified decimal value.}$$

According to the Zeckendorf's theory [43], the next Fibonacci value will be zero.

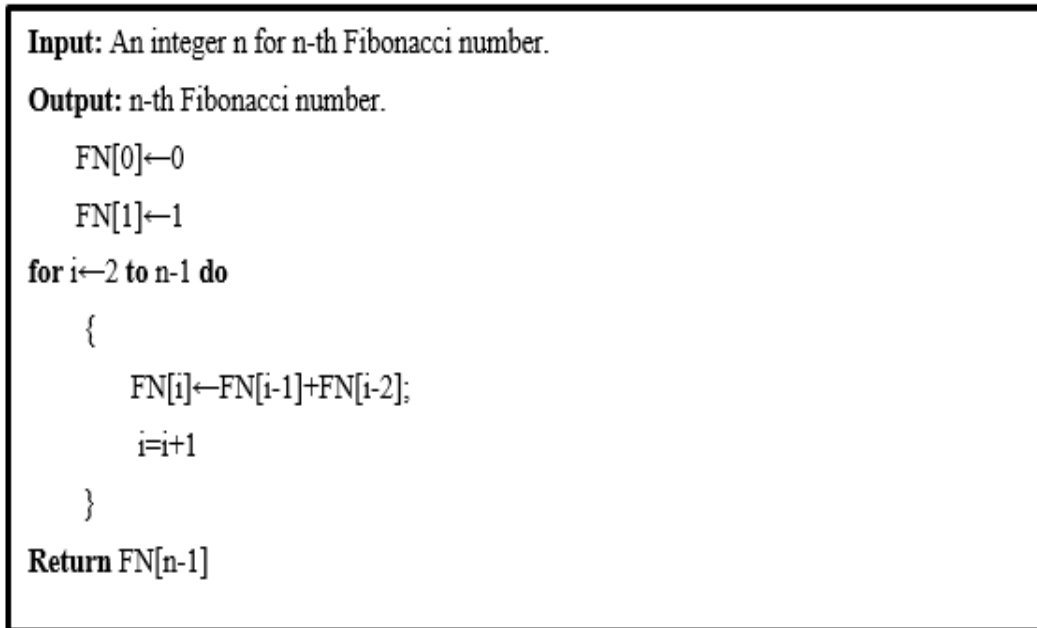
- 10- $F=0.$
- 11- $1 < 2 \rightarrow F=0.$

According to the Zeckendorf's theory (Bower et al., 2015), , the last stage of Fibonacci's series is zero.

- 12- $F=0.$

In comparison between the Fibonacci analysis and the binary system, the decimal number 150 will be as follows: (10010110), if a binary system analysis is performed. While it is in the following form: (000100000010), if it is analyzed by the Fibonacci system, as the outcome of the analysis looks completely different. According to the previous studies, the Fibonacci decomposition gives the embedding method more robustness, which is one of the goals of building any steganography system. In general, in the Fibonacci number sequence, each number is the summation of the previous two numbers. Fibonacci number began the sequence not with (0, 1, 1, 2), as modern mathematical do but with (1,1, 2), etc. Fibonacci number carried the computation up to the thirteenth place (fourteenth in modern counting), that is (233), though another manuscript carries it to the next position: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377. Fibonacci number did not speak about the golden ratio as the limit of the ratio of consecutive numbers in this sequence. The algorithm 3.3 is shown the procedure for any Fibonacci number sequence.

Chart 3.3: Fibonacci sequence number



Three main reasons for using Fibonacci decomposition are:

- i. Changing to Fibonacci decomposition improves the security due to difficulty in estimating the secret information by attacker.
- ii. Increase the robustness of the method due to using (12) bit-planes.
- iii. Difficult to recognize by Human visual attack due to heterogeneous information.

With Fibonacci decomposition, the proposed work that is based on $Pixel_s/Pixel_d$ method will be more secure. Simply, the Fibonacci is the summation is shown in the simple procedure below.

```
"public int Fibonacci (int x) {  
    if (x==1) {  
        return 1;}  
    else if (x==2) {  
        return 1;}  
    else {  
        return Fibonacci(x-1) + Fibonacci(x-2)}  
}"
```

Embedding the data with Fibonacci 12 bitplane is different from the original image of 8 bitplanes because the two LSB bits in Fibonacci are special from other bits, and when embedding, the condition of Fibonacci decomposition should be considered to avoid two ones in series which mean there are no two bits (of 1 value) contiguous as illustrated in the example below:

128 64 32 16 8 4 2 1		233 144 89 55 34 21 13 8 5 3 2 1	
1 1 0 0 0 1 0 1 = 197		0 1 0 1 0 0 0 0 0 0 1 0 = 197	
1 1 0 0 0 1 0 1 = 197		0 1 0 1 0 0 0 0 0 0 0 1 = 196	
Add a secret bit to the pixel P = 72			
0 1 0 0 1 0 0 0 = 72		0 0 0 1 0 0 1 0 0 1 0 1 = 72	
0 1 0 0 1 0 0 1 = 73		0 0 0 1 0 0 1 0 0 1 0 1 = 72	
Add a secret bit to the pixel P = 198			
1 1 0 0 0 1 1 0 = 198		0 1 0 0 1 0 1 0 1 0 1 0 = 198	
1 1 0 0 0 1 1 1 = 199		0 1 0 0 1 0 0 0 1 0 0 1 = 197	

This procedure of preparing cover image is done simultaneously with secret message preparation that will be discussed in the next section.

3.2.2.3 Stego key in steganography

Steganography refers to the problem of sending messages hidden in “innocent-looking” communications over a public channel so that an adversary eavesdropping on the channel cannot even detect the presence of the hidden messages. Simmons [19] gave the most popular formulation of the problem: two prisoners, Alice and Bob, wish to plan an escape from jail. However, the prison warden, Ward, can monitor any communication between Alice and Bob, and if he detects any hint of “unusual” communications, he throws them both in solitary confinement. Alice and Bob must then transmit their secret plans so that nothing in their communication seems “unusual” to Ward. Therefore, Alice and Bob need the key which is the method to share their information. This key is called the stego key as seen in figure 3.14[50].

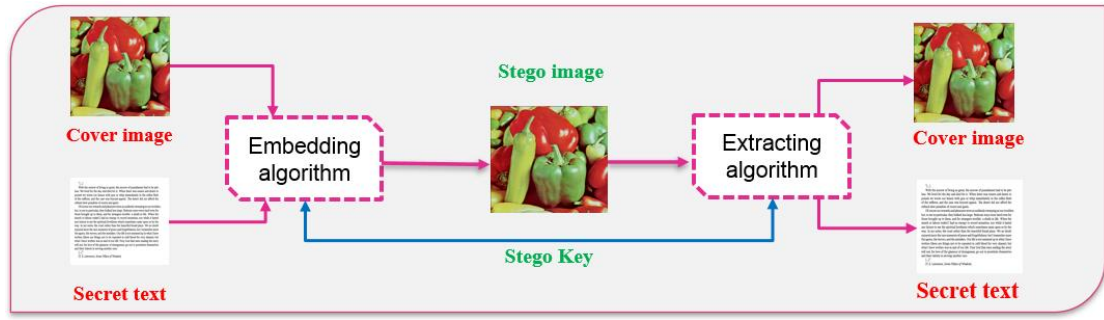


Figure 3.14: The principle of image steganography

In image steganography, the stego key is used to select the pixels where the data will be hidden. An attacker without the key does not know what pixels he has to read. Therefore, the stego key is related to the embedding method that has been used with the steganography techniques or algorithms such as the LSB technique [26] as seen in figure 3.14

There have been many proposed solutions to this problem, ranging from rudimentary schemes using invisible ink to a protocol that is provably secure assuming that one-way functions exist [37]. However, the majority of these protocols have focused on the case where Alice and Bob share a secret or private key. If Alice and Bob were incarcerated before the need for steganography arose, these protocols would not help them. In contrast, public-key steganography allows parties to communicate steganographically with no prior exchange of secrets [41]. As with public-key encryption, the sender of a message still needs to know the recipient's public key or otherwise participate in a key exchange protocol. While it is true that if there is no global PKI, the use of public keys might raise suspicion, in many cases it is the sender of a message who is interested in concealing his communication and there is no need for him to publish any keys [22]. A key in cryptography is a piece of information, usually, a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data [21]. Based on the used method, the key can be of different sizes and varieties, but in all cases, the strength of the encryption relies on the security of the key is maintained. A key's security strength is dependent on its algorithm, the size of the key, the generation of the key, and the process of key exchange [23] as seen in figure 3.15

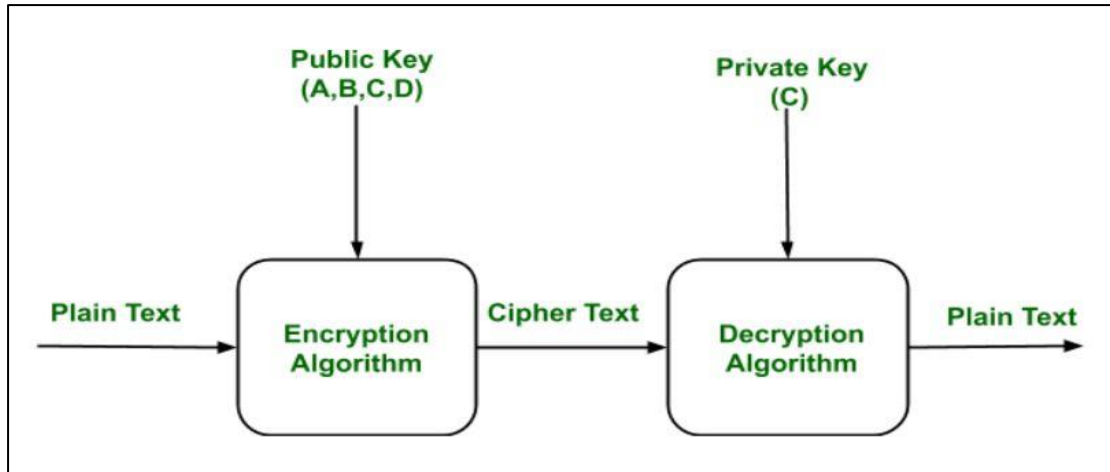


Figure 3.15: The principle of asymmetric cryptography

3.2.3 Embedding Part

The proposed algorithm is designed to host secret data into given image. The essence of any steganography system is to hide a secret message in a certain image and transfer it from the sender to the authorized receiver side without any suspicion. The resulting images should satisfy the imperceptibility of maintaining high PSNR. The basic concept of embedding secret data inside the image depends on generating the key to select the position of pixels of the given image. All the procedures inside the embedding process should represent in this key. A finding of the best key is necessary for the steganography method to achieve high security which is called the stego key that is used in both sender and receiver side, this key carries the procedures of embedding methods which the receiver side should be aware of it to reveal back the secret text. Two types of stego key are implicit and explicit stego key, As shown in Figure 3.14

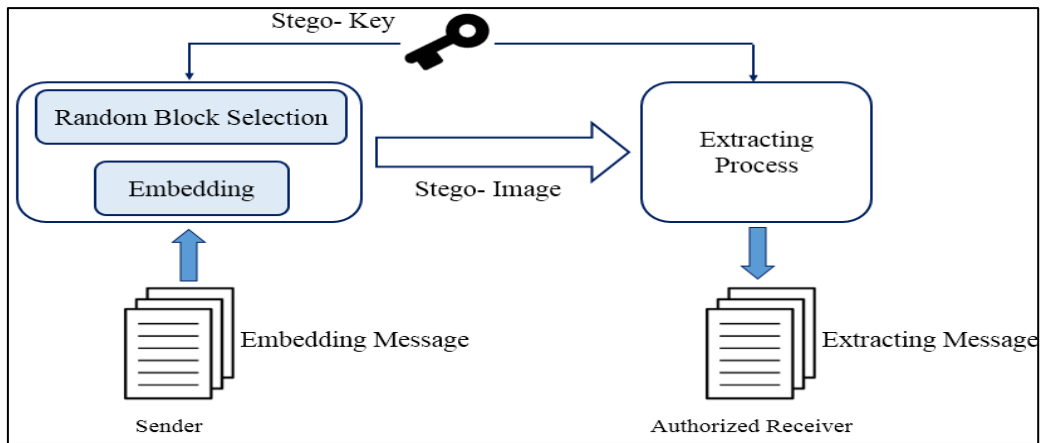


Figure 3.16: Principles of stego key and image

To obtain a high percentage of PSNR, the researchers are working on keeping the pixel's value after embedding the same as original as possible, this is done by keeping the LSB value because of in the steganography system the changing specified in LSB which is unseen place. The reason for using LSB is low impact value of bit weight which equal to one as maximum due to the impact value of the binary format of the pixel value (2^0), so the maximum change of the pixel, in this case, is 1 or keep it as the same when it is changing with the same value. A general embedding process illustrates in Figure 3.15 When embedding with the proposed method just LSB of bitplane (0) will affect that's mean like standard embedding of the first bit in LSB du to our case are increasing, decreasing, or stay the same.

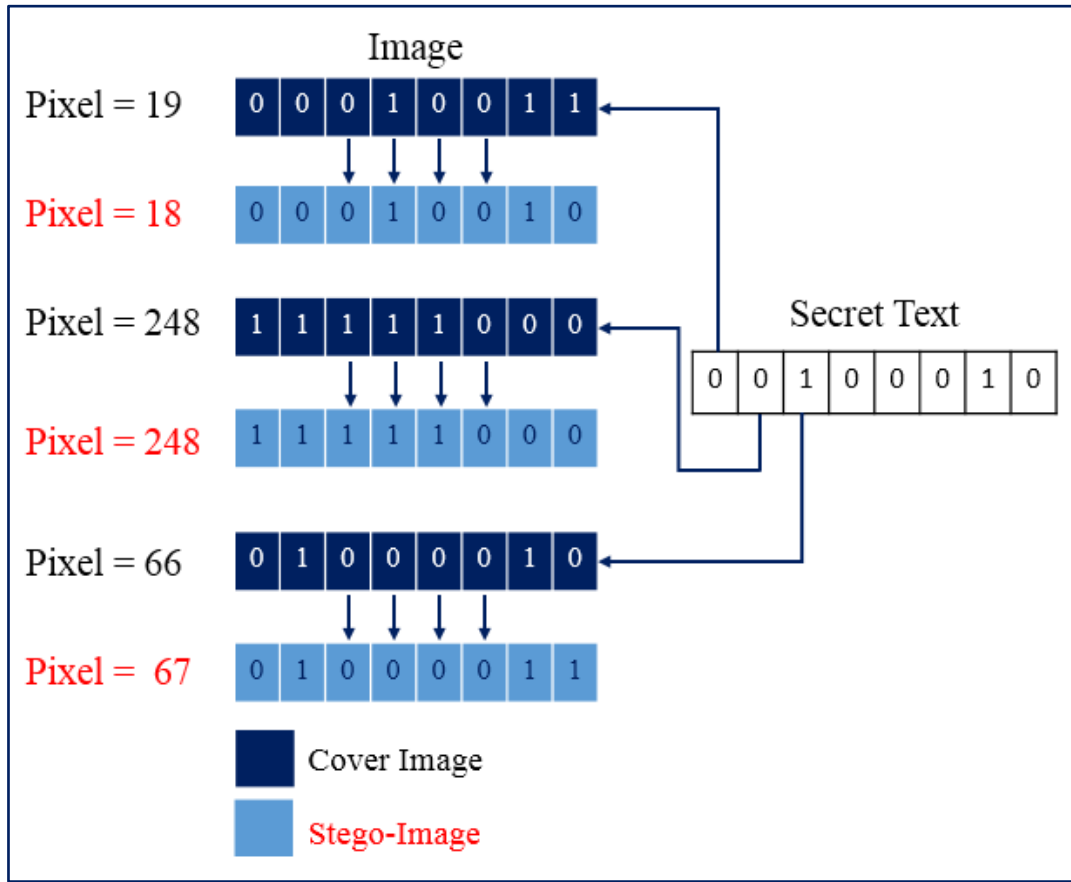


Figure 3.17: A general embedding process

The proposed embedding procedure contains three stages with stego-key. Start with these are pixel selection, P_{sel}/P_{da} system and end with secret key (stego-key). All bits are computed in same way. Each bit from the private data (secret data) is searching for one pixel adaptively in the given image, then, checking the condition of embedding. So, if it is satisfied, put the bits into the pixel and store all the data into the stego key. This process can be discussed in detail in algorithm 3.4.

Chart 3.4: Embedding Algorithm

Input: Cover Image (CI) of size 512×512 , Secret Message (SM). Output: Stego Image (SI).
1. Read the SM and convert it into series of bits with binary system.
2. Read the CI and convert the pixel's value form binary to the Fibonacci decomposition.
3. Apply the Huffman coding on the SM.
4. Calculate the size of the SM (the number of characters or bytes).
5. Let L =length of SM in bits.
6. Select a given CI (512×512).
7. Select the aim pixels according to P_{Single} and P_{double} strategy.
8. Create V vector and arrange it according to to P_{Single} and P_{double} .
9. Mark the LSB of each pixel.
10. Then make loop from $I=1: N$.
11. Get SM bit (0 or 1).
12. If SM is 0 and pixel value is P_{double} do no change.
13. If SM is 0 and pixel value is P_{Single} , replace, the LSB layer value by 1.
14. If SM is 1 and pixel value is P_{double} ,replace, the LSB layer value by 1.
15. If SM is 1 and pixel is P_{Single} , do no change.
16. $I = I+1$.
17. Return the SI.
18. End

Double pixel value consists of 0 within LSB position because of binary impact value (IV), while the value 1 of the LSB position reflects as a single pixel value. As discussed in the previous algorithm 3.1, embedding the value 1 of the privet data to P single of the hosted image result in the same value of the LSB as no change will happen and the same case for hiding the value 0 of the select message to the p double of the given image. While hiding the value 1 of the select text to the p double will increase the p double value by one and adding the value 0 of the chose text to the p single will decrease the p single value by one. In the Figure 3.16 depicts the hiding procedure of the present work.

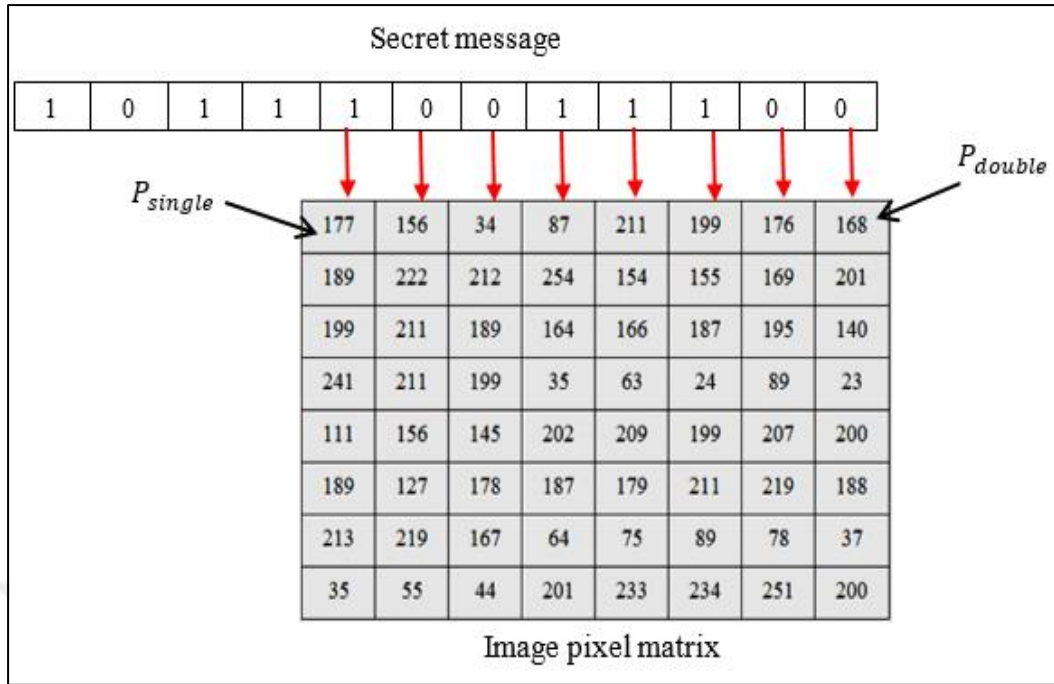


Figure 3.18: Explains the proposed theory

The information hiding procedure will be saved in key call the stego key (SK). The SK may store within the image or store outside the image in this called explicit stego key. There is an agreement between the parties regarding this key produced by the sender to be used by the receiver side to extract the secret data from an image. The image that contains the secret message called stego image, should be able to stand against the attacks, therefore many tests are applied to the image before sending it to the second part or receiver. These attacks (intruders) or evaluations happened in the sender part and will be discussed in detail in the next paragraph of the evaluation stage.

3.2.4 Evaluation Stage

The aim of any steganography system is to build a secure system that cannot be detected as much as possible. The attacker always uses statistical methods to detect the stego-image even if the cover image is unknown. During the embedding method, some statistical changes occur on the image and attackers catch this weak point and go through it to detect the stego-image. Recently, many kinds of steganalysis methods have been suggested in order to detect the stego-image and test the steganographic methods. Various methods have been proposed in the literature to detect steganography [13][17]. such as Chi-square (X2) which is related to

the objective attack, and Human Visual System (HVS) which is due to the subjective attack. Three crucial types of steganalysis methods have been used to test the result image (*Stego Image*) before transfer it into receiver side, which are Chi-square, Human Visual Pixel (HVS), and PSNR, the proposed method is designed to stand against these types of attacks and give good result in term of capacity, security, and imperceptibility. As shown in Figure 3.17.

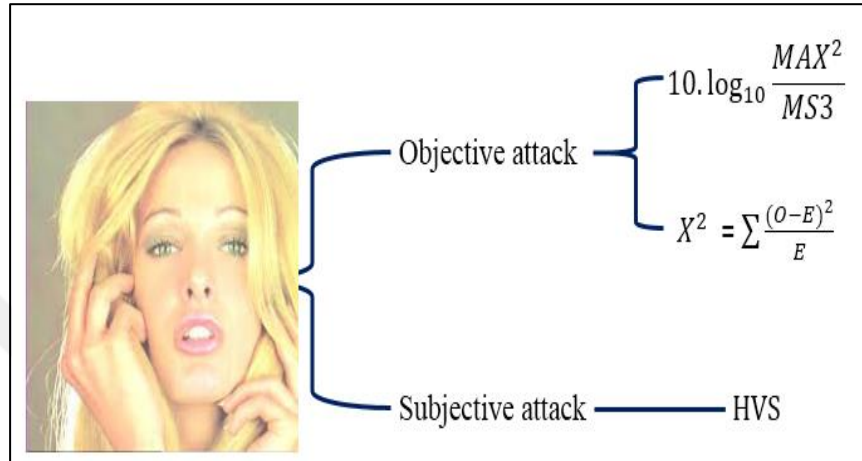


Figure 3.19: The evaluation criteria with the proposed system

3.2.5 Extracting Stage

The transmission media in the field of information hiding, steganography, in particular, can be video, audio, protocol or image, in the proposed study we consider the image as transmission media due to its availability and the ability to hold a large amount of data [41]. There is a certain possibility that the image may encounter different kinds of attacks when transferring from the sender side into the authorized receiver side. The whole procedures that occurred in the embedding stage are recorded in the implicit stego key as a sequence, once the receiver side receives the stego-image, he/she uses the same sequence of embedding process but in conversely action called extracting. The receiver side uses two kinds of information in the implicit stego key. The first kind of information is the procedures used by the embedding such as sequence operations of pixels' selection, and the mapping order of secret message which defragmented accordingly. The second information on stego key is the general information that agreed by the two parties in advance that may it change. The main goal of the extracting stage is to get the embedded data (secret bits) from LSB pixels at the same time should follow the procedure designed and build in the embedding stage. Most of

the information related to extracting stage made by agreement between the two parties (sender and receiver), rest information used by the implicit stego key which considered variable information and based on image nature and environment. The entire algorithm of embedding and extracting stages is known for the sender and the receiver parties but some information is needed to specify index pixels' location which is not agreed upon in advance; this extra information can be carried out by the stego key during the embedding process immediately. In this case, the stego key is still updated until finish the embedding process. Figure 3.18 depicts the embedding and extracting stages with security and imperceptibility goals.

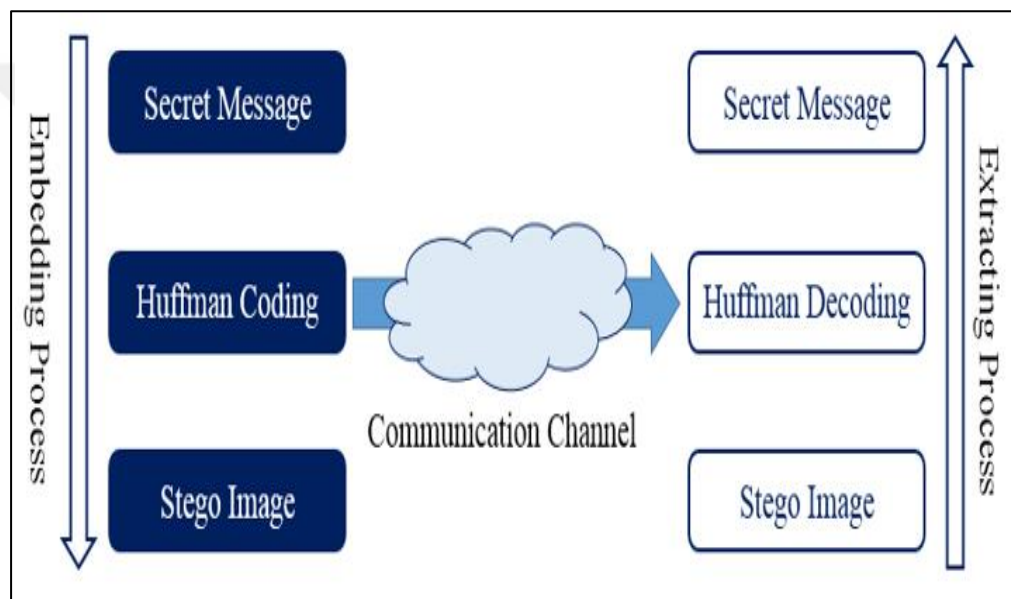


Figure 3.20: Embedding and extracting processes

The embedding and extracting stages are responsible for keeping image quality (imperceptibility) high as possible, on the other hand the pixel's selections of the image reflex the security of the steganography system. These consider the major objectives in the proposed system in addition to increasing the capacity achieved by the pre-processing or preparation stage. Cover images are supposed to host the secret bits selected from the standard USC- SIPI dataset which will discuss in the next section.

3.2.6 The Usc-Sipi Image Database

USC-SIPI dataset [83], which is used with the proposed system contains digitized images. The purpose of this dataset is to support studies in image processing, analysis of an image, and vision analysis. The first version of the USC-SIPI dataset was released in 1977 since that time many images have been added to this dataset to maintain it. In a steganography system, a dataset is defined as a set of images, which is used to benchmark the observation of the proposed study with existing literature. Many images are used as datasets in the literature, where each researcher achieved some results based on this dataset. The present thesis follows the same strategy to evaluate and benchmark realistically the experimental results obtained using the proposed method. Colour (red, green, and blue) and grayscale images are used. In these three major colours, each pixel in the image consists of 24 bits, in which 8 bits are allocated to each colour. The embedding method treated each part separately as new pixels because the illumination of each colour (part) is different from the other as well each colour possesses a different [13]. The embedment in LSB is direct because gray image pixels in the cover image consist of 8 bits. The worthiness of the proposed system is further demonstrated by selecting several images including Lena, Baboon, Cameraman, and Peppers as shown in Figure 3.19.



Figure 3.21: USC-SIPI dataset images used in the proposed system

Every image is normalized into (512 x 512) before starting the embedment, where they are divided into blocks and sub-blocks. Some images in the dataset are already normalized and others need to make it, size of the image affects the PSNR of the result due to it belonging to the component of the equation.

3.3 SOFTWARE IMPLEMENTATION

The embedding and extracting methods are the main issues within image steganography method. Where the embedding process is located within the sending process, while the extraction method is located within the reception process. Embedding and extracting methods are the core process in the proposed system. Proposed system reflected by software build in Matlab V. 18 program to simulate the process and results that given during the process. In this section user interfaces are introduced shown in Figure 3.20 for the whole system.

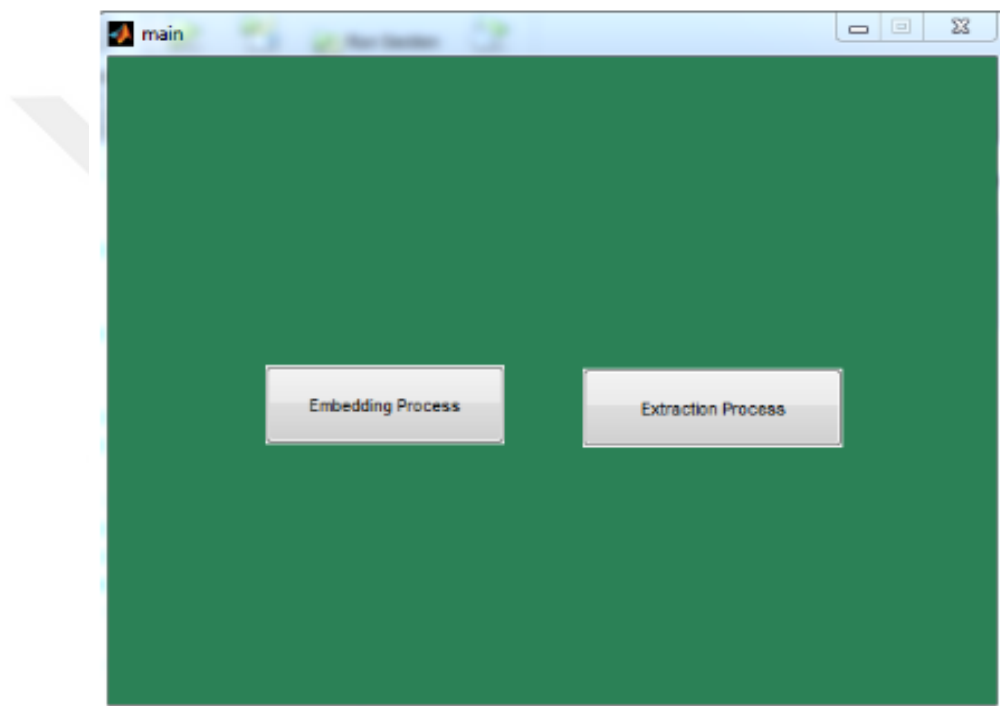


Figure 3.22: The main menu of the demo system

This program is compatible and works with the sender and receiver sides when the embedding process occurs in the sender side who is responsible for hiding a secret message into the digital media such as an image while extracting process follows the embedding in the other part of the system who needs to reveal the secret data from the result image (stego image). Two main sub-processes associated with the embedding process are selecting both secret data and media (image) as shown in Figure 3.21.

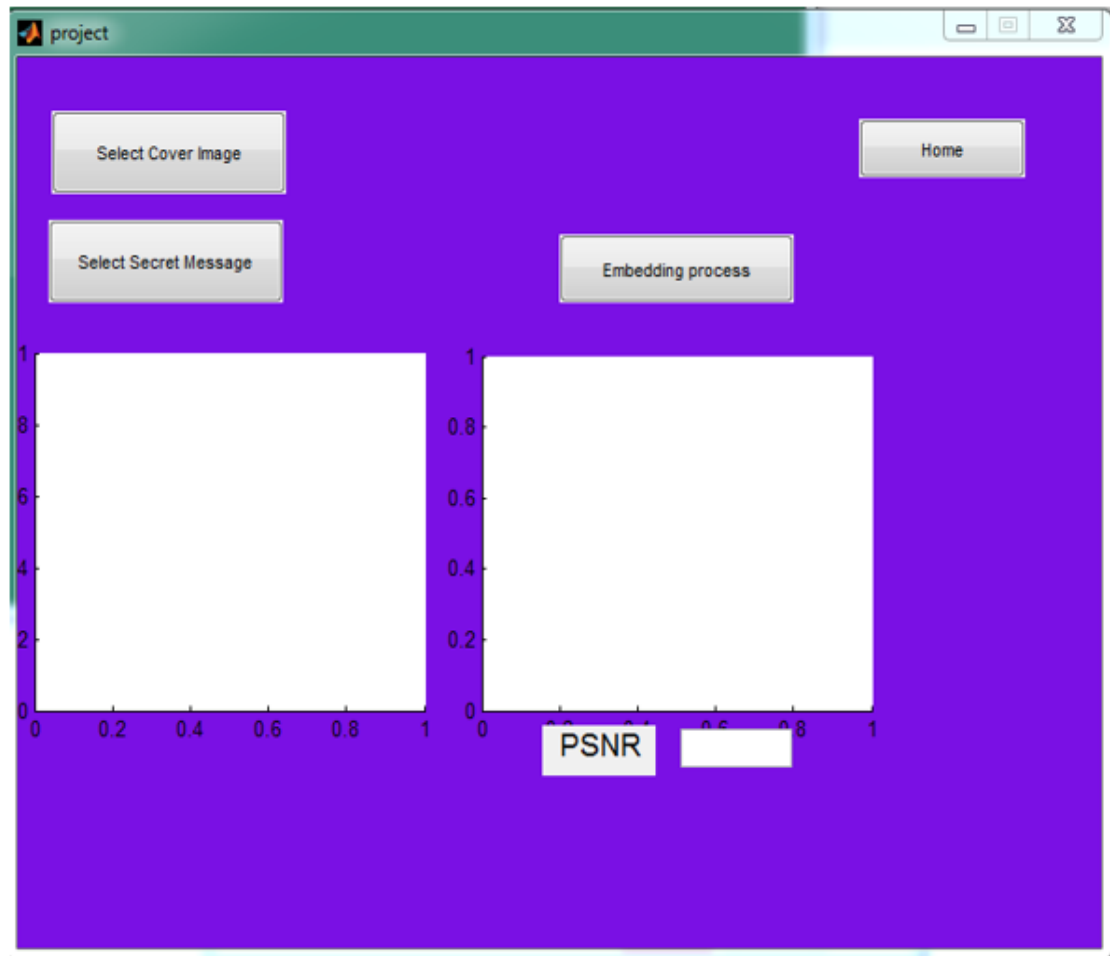


Figure 3.23: The embedding process within proposed system

The secret file is first selected to be ready for embedding in the image which was also selected at this stage. Before pressing the embedding button these two selective items must be ready as shown in Figure 3.22. The proposed system can handle both gray and color images with different types of SIPI database images.

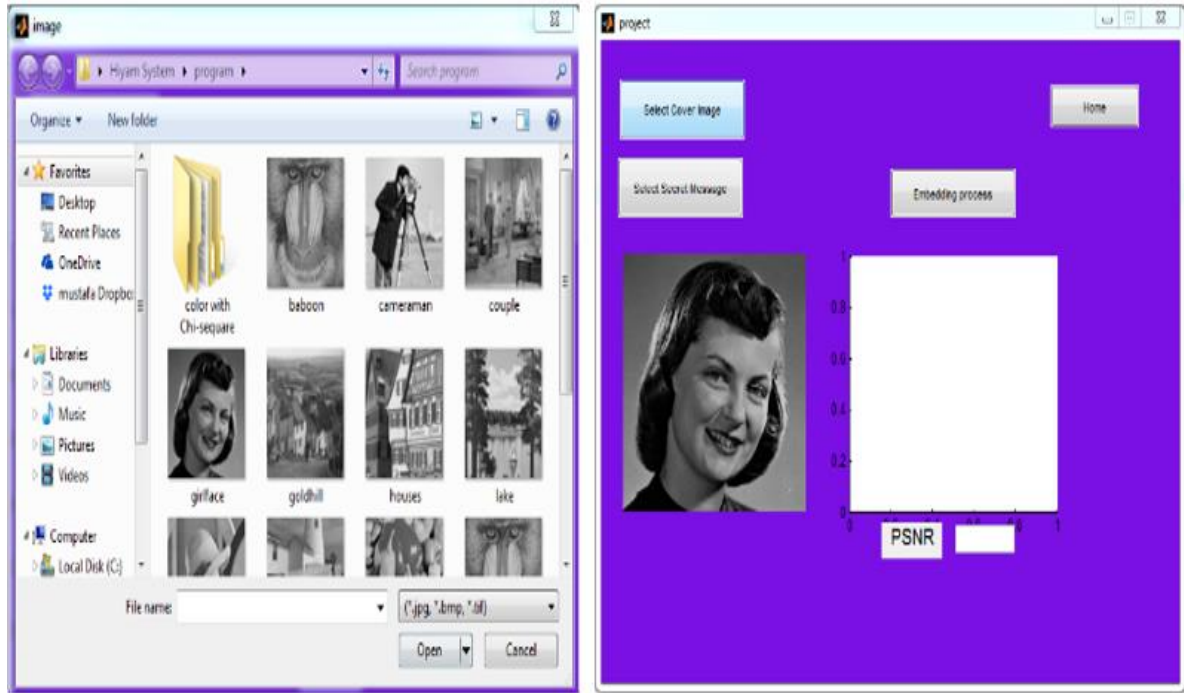


Figure 3.24: Selecting a cover image for embedding selected a secret text

In the previous studies, the methods were evaluated according to many criteria, the payload capacity (PC) is one of these criteria which we may achieve it from the following equation:

$$Ec(bpp) = \frac{\text{No.of embedding bits}}{W \times H} \quad 3.3$$

There are different standard sizes that researchers who work in the information hiding field use to evaluate their proposed steganography methods, which are 6.25%, 12.5%, 18.75%, 25 %, and others. Various payload capacities have been used with the proposed system and reflected as a percentage to correspond with the research in recent literature. For more clarifying when embedding. The percentage of 6.25% for the cover image 512×512 is equal to 16384 bytes, and the percentage of 12.5% for the cover image 512×512 is equal to 32768 bytes. While the percentage of 18.75% for the cover image 512×512 is equal to 49152 bytes. These percentages can be calculated by the number of secret bits embedded in each pixel of the cover image, where the ratio of 6.25% appear from embedding one secret bit in every 2 pixels of the cover image (2 pixels = 16 bits → 1/16 = 6.25%), and the ratio 12.5% came from embedding one secret bit in each pixel of the cover image (1 pixel = 8 bits → 1/8 = 12.5%).

The current study deals with different sizes that were mentioned in the section above and other sizes in order to benchmark the proposed method with those that were suggested in previous studies in order to evaluate the performance of the proposed system as shown in Figure 3.23.

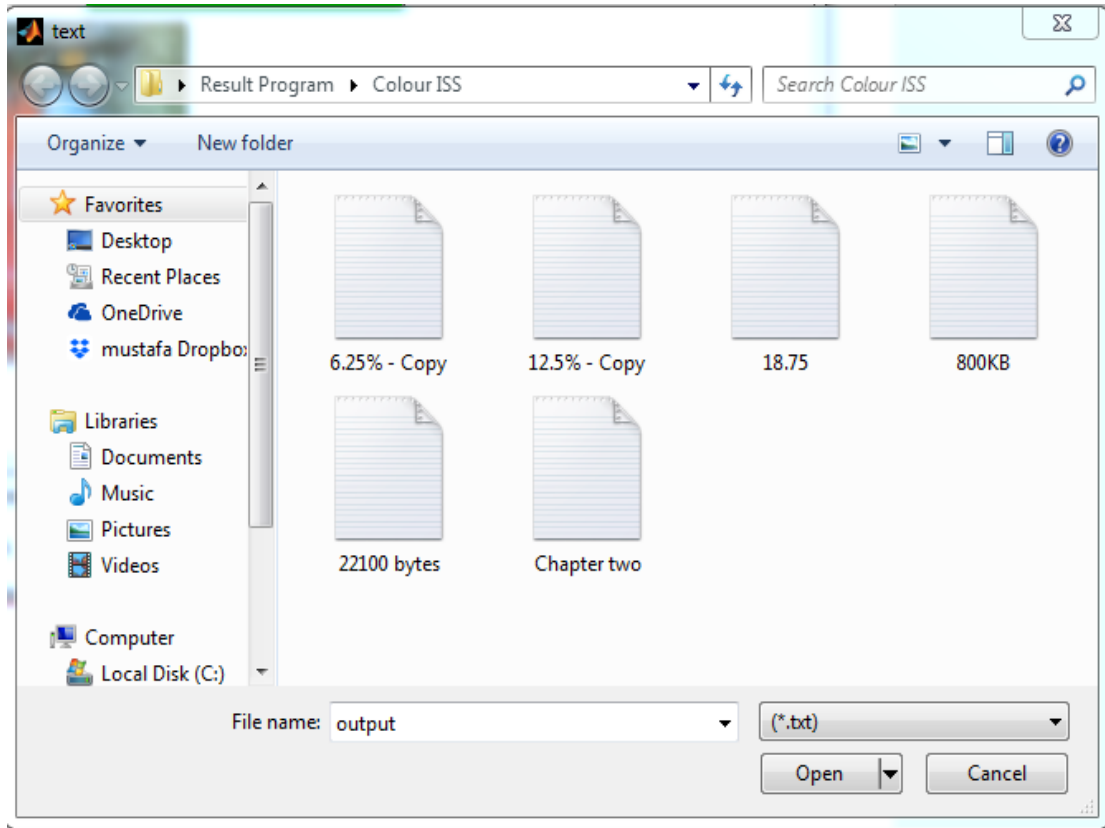


Figure 3.25: Different payload capacities used in the proposed system

After selecting the secret text and cover image (the original image), the embedding process will be ready for concealing. While embedding the secret bits within the proposed method, the suggested tools and method in chapter three (research methodology) are implemented by pre-processing the image and text as well as by using the proposed $Pixel_s/Pixel_d$ method to satisfy the proposed system. Two images will appear in the user interface after including the original image (cover) and stego image (image after embedding) as shown in Figure 3.24.

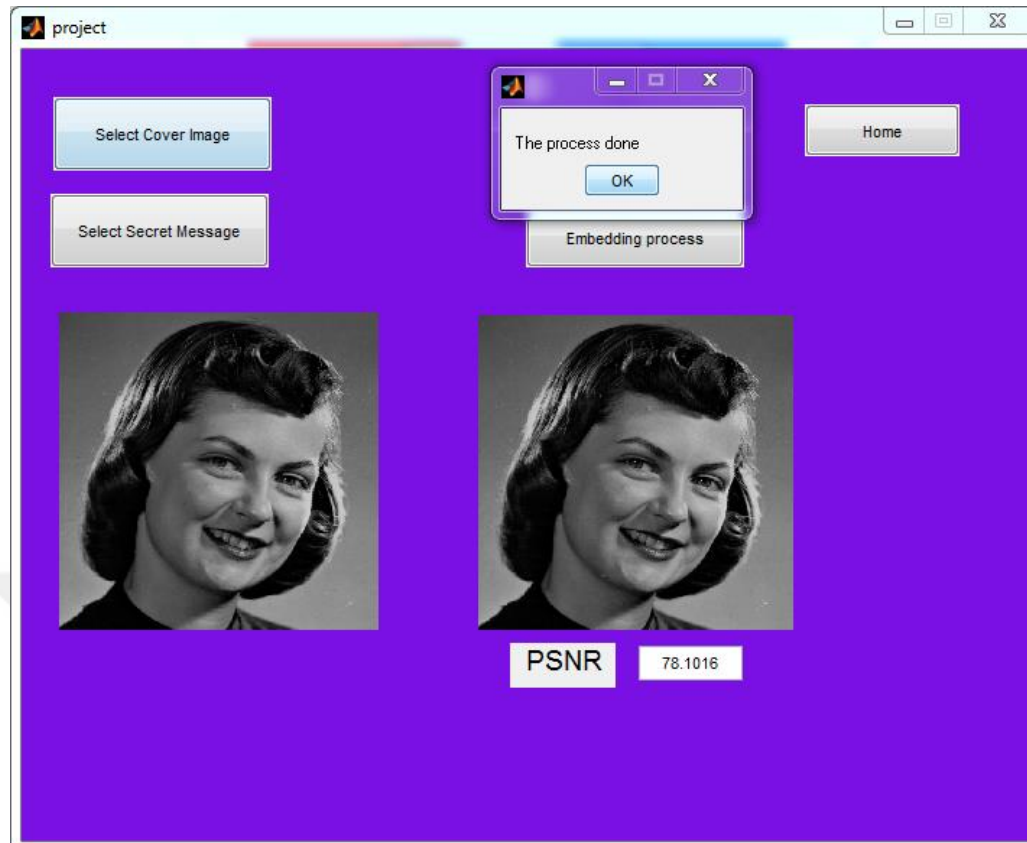


Figure 3.26: Shows resulted images after embedding process

The stego image is the result of the procedure of embedding the private text within selected image so that stego image looks like the cover image, or in another word, there is exactly a match between the two images. As shown in Figure 3.24, the image on the left looks like the image on the right, this is the purpose of steganography which is embedded image cannot distinguish by naked eyes. No one can recognize the image whether stego or cover but the problem with statistical evaluation like PSNR or HVS it's easy to recognize the difference between them. The amount of secret bits is limited and not free due to the limitation size of SIPI dataset images, in proposed system we took in our consideration 512×512 pixels. However, these pixels can hold certain amount of data but increasing this amount depends on $Pixel_s/Pixel_d$ method. The second part of the proposed system is the extracting process, when a receiver party receives the stego image with the key, he / she can extract the secret bits by using a certain algorithm and the key as a tool to get secret bits as shown in Figure 3.25.

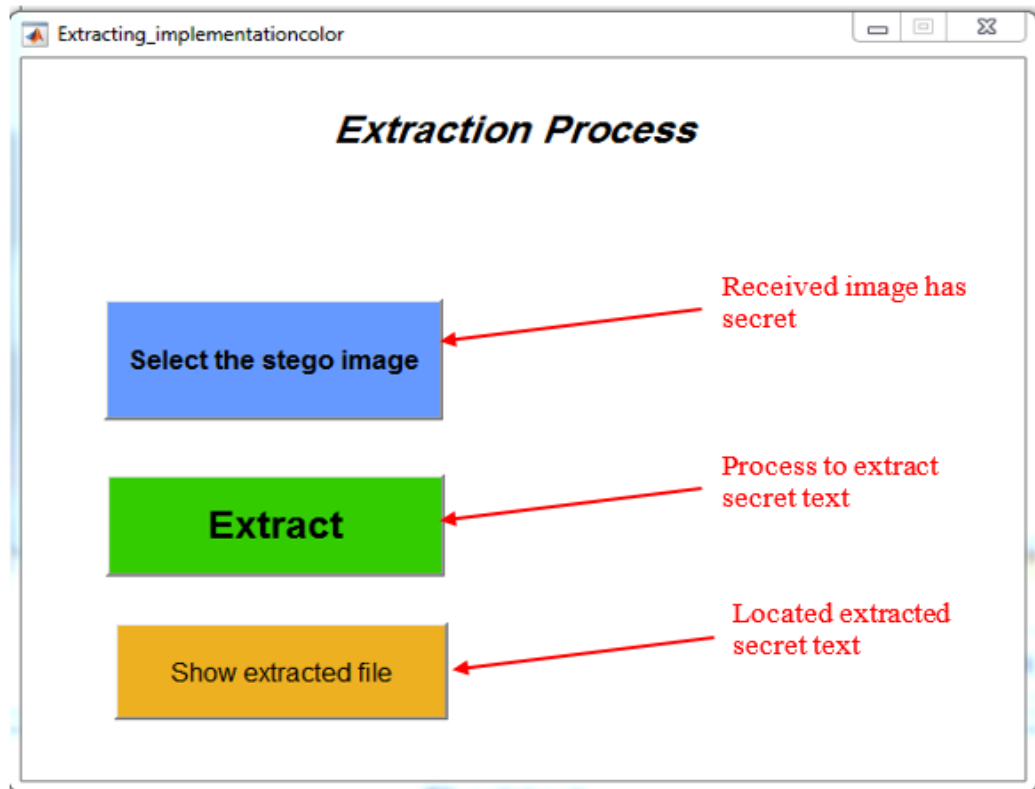


Figure 3.27: The Extracting process within proposed system

The evaluation process must be at the sender side when embedding the secret bits, in this case, imperceptibility is the main criteria measured as PSNR will calculate before sending stego image. Hackers always catch the stego image before receiving it by the receiver side, so we evaluate the stego image to avoid any missing in the system. Within the system menu, there is a field PSNR located after embedding to ensure the imperceptibility of the image.

3.4 SUMMARY

This chapter provided a detailed explanation of the mechanism for hiding the secret bits in an image while ensuring the security of the embedded secret bits. Four stages were used in the proposed study. This is preparation, embedding process, performance result of stego image, and finally extraction stage. The secret text was compressed using the Huffman coding technique, and the values of the given image pixels were converted to Fibonacci technology. All of these operations have been done during the preparation stage. The secret bits are embedded within the cover image pixels using Enhanced Method. The plan of the proposed system does not allow the disclosure of confidential data.

4. RESULTS OF THE PROPOSED SYSTEM

4.1 INTRODUCTION

This chapter is focused on the implementation to achieve the proposed research goal which is "increasing the payload capacity while preserving security, imperceptibility, and robustness as much as possible". Three important criteria help to maintain security in this study. The first is to find the position of each last pixel value embedded in which pixel in the cover given image with the Fibonacci technique. The second is splitting decomposition which increases the robustness and security of the system. Third, Huffman coding in order to increase the capacity and thus contribute to increasing security. Two types of attacks are used to evaluate the security in this chapter which are Human Visual System (HVS) and Chi-squared (X^2) attacks. The first one is based on human eye detection and the other one is fully based on the system. Evaluation is made by different amounts of capacity embedded in the system. The objective of security and robustness is underscored. First, an intelligent lossless compression method is performed using Huffman, and second, maintaining the robustness of the stego image is carried out using Fibonacci.

4.2 RESULTS AND DISCUSSIONS

The following sub-sections explain in detail the related criteria to the proposed system, supported by tables and figures. The present work has been benchmarked with the previous works and It has been proven by experimental that the proposed system is immune to any kind of attacks that would retrieve the embedded secret data

4.2.1 Imperceptibility

The main priority of any information embedding system is image quality (imperceptibility). It is any steganography feature. Therefore, it remains unrecognized via the naked human eye (HVS) or statistics test [13]. The peak signal to noise ratio (PSNR) can be defined as the ratio between a given maximum signal and the corrupted image after the embedding. After the embedding, the stego image can host the secret data and cause some distortions. However, this corruption is almost inconceivable, especially by the human eyes. This is aimed to keep the stego image similar to the original one. In the proposed system, the embedding process

used a special condition for embedding the secret bits in some single and double pixels which are calculated in such a way to make the place of embedment untraceable and to use the additional random techniques with reduced corruption. The hiding secret bits were applied by adding the adaptive pixels to the embedding condition to keep the order of the image pixels almost identical to the original. The image quality (Imperceptibility) is a statistical test that used the result of embedding method (stego image) from the original image before embedding. The PSNR measurement is utilized to compute the quality of the image after hiding and it is equation as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (4.1)$$

with

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (4.2)$$

where MAX is the maximum possible pixel value of the image; m and n are the dimensions of the image; I and K are the original and noisy pixel. The PSNR value is based on Mean Square Error (MSE) which has an adverse effect. The parameters of PSNR allow normalizing the equation for all methods and image types. Three types of embedding are utilized to compute the methods, LSB method, with the Fibonacci method and embedment utilizing P_{ixel_s}/P_{ixel_d} system within Tables 4.1, Tables 4.2 and Tables 4.3.

Table 4.1: Computing PSNR for Cameraman Gray-scale image

Percentage of Embedding	Capacity Byte	Compute by PSNR		
		LSB Method	LSB Method	LSB Method
6.25%(dB)	16001	62.83	75.31	78.158
12.5%(dB)	32001	61.24	62.62	75.133
18.75%(dB)	48001	55.77	65.14	71.961
25%(dB)	64001	50.84	62.93	68.372

Table 4.2: Computing PSNR for Zelda Gray-scale image

Percentage of Embedding	Capacity Byte	Compute by PSNR		
		LSB Method	LSB Method	LSB Method
6.25%(dB)	16001	61.25	75.26	78.153
12.5%(dB)	32001	62.09	62.28	75.129
18.75%(dB)	48001	55.36	65.42	71.964
25%(dB)	64001	50.12	62.80	68.174.

Table 4.3: Computing PSNR for House Gray-scale image

Percentage of Embedding	Capacity Byte	Compute by PSNR		
		LSB Method	Fibonacci Decomposition	Proposed Work
6.25%(dB)	16001	61.44	75.68	78.088
12.5%(dB)	32001	62.23	61.96	75.101
18.75%(dB)	48001	55.12	65.08	72.003
25%(dB)	64001	50.14	62.23	68.254

Results in the above Tables represent the PSNR performance of the proposed method in comparison to benchmark methods on different images. A secret message containing different bytes of payload capacity was embedded in the image. The other images of (SIPI) dataset are identical to the Zelda, Cameraman, and House images as seen in Tables 4.1, Tables 4.2 and Tables 4.3.

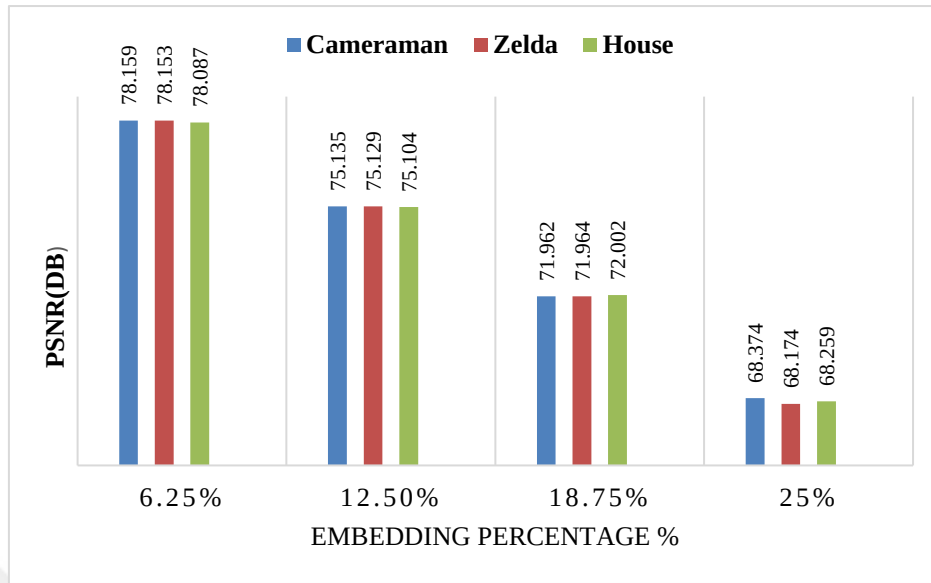


Figure 4.1: Compute PSNR values along with different payload capacity (PC).

In the proposed study we aim to reduce the difference between cover and stego image, since the PSNR (that measures the distortion of image) depends on MSE (Mean Square Error) this error comes from the difference of checking each pixel of cover image with corresponding pixels of stego image. While the difference located down the equation of the PSNR and power to (2) mean square which means is inversely proportional, this relation makes changing of pixels value is worthy and should be considered. The proposed method takes care of pixels change and made it as less as possible. Hackers always use statistical methods for checking the stego image so considering this issue is necessary and inevitable. During embedding with the proposed method (which aims to use the single and double pixels to keep the intensity of pixels value less changing in the frequency of the pixels during embedding the secret bits) increase the imperceptibility of the image represented by PSNR. however, existing methods look for a technique to reduce the change in an image while embedding a certain amount of data to it. We gain better imperceptibility by using Huffman compression for the secret message before embedding to make stego images carry enough amount of payload capacity. Even compression help to increase the PSNR so the Huffman coding technique used with the proposed method, when increasing the payload capacity and exceeding the limit effect the image by distortion it, thus a reasonable amount of data embedded should be allowed. Figure 4.2 is shown the better PSNR with diffrent payload capacity in a graphically shape.

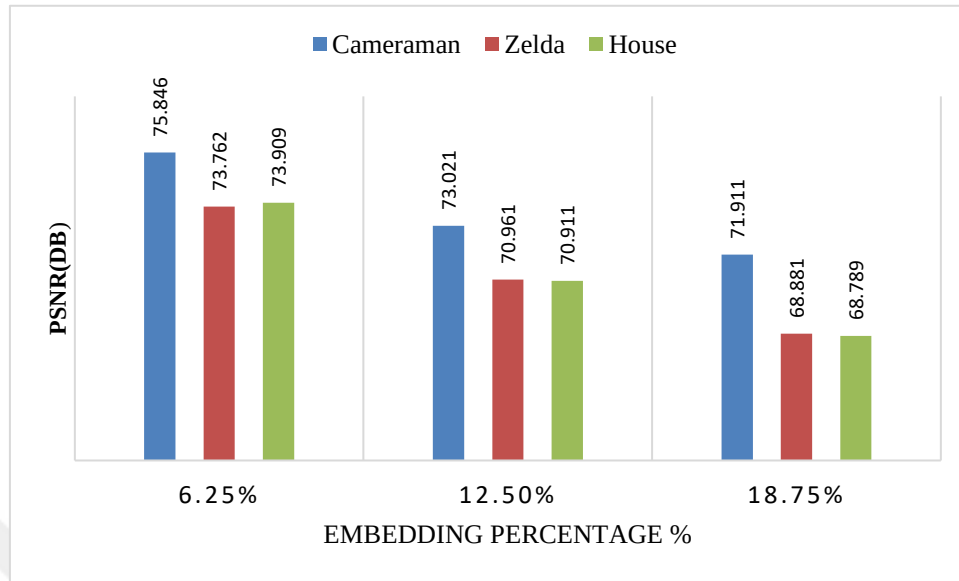


Figure 4.2: PSNR test for different colour images.

During compute the PSNR for the (SIPI) images, we can notice the result having different PSNR outcome and this can be present as is pixel density per image. We can notice that from figure 4.2.

4.2.2 Robustness

The robustness can be defined as the information hiding inside an image by keeping the host image unchanged without losing any secret data due to the attacks. The nature of the steganography system falls under different kinds of attacks such as the statistical or others. The proposed system tried to break the behaviour of the normal image structure that consists of pixels each of 8-bits where most of the embedding methods fall in the LSB of 8-bits. Due to the expected form of the pixels, many statistical attacks can predict the existence of a secret bit within the image. A new term called Fibonacci was used in the proposed study to enhance the robustness of the steganography system performance. The Fibonacci sequence can be used in the steganography techniques to resist attacks on the image because it depends on the pixels. Figure 4.3 depicts the difference between the Fibonacci decomposition and 8-bits decomposition called the binary decomposition.

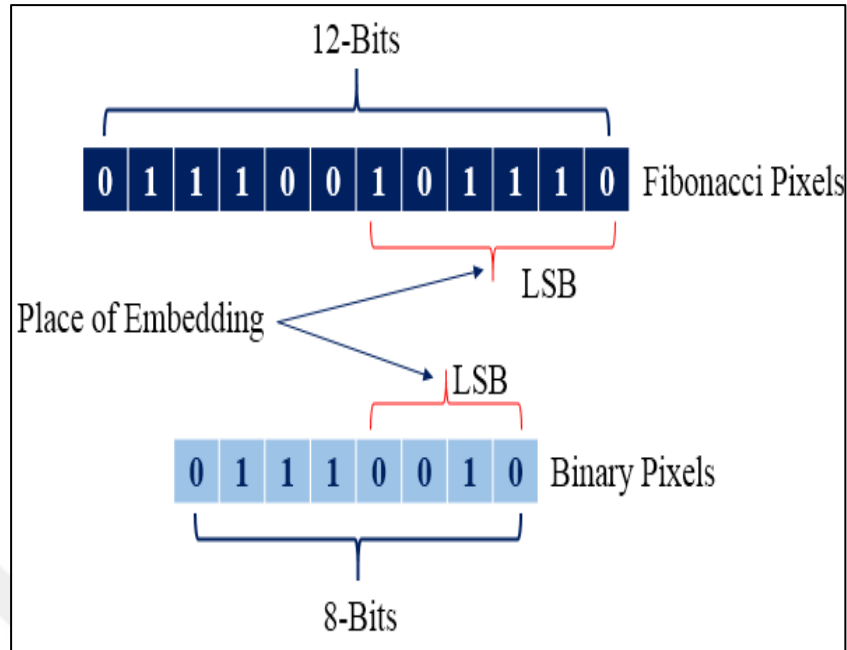


Figure 4.3: Binary versus Fibonacci pixels

The Fibonacci decomposition (12 bits within embedment) can be confused the statistical tests wherein the up-normal allocation for the pixels in the Fibonacci number structure also improve the steganography method. In this research, the bit-plane was utilized to review and check the imperceptibility where it reflected the degree of the image concealment within the first 2 bit-planes. Figure 4.4 discussed the distinction among the Fibonacci number and binary bit-plane analysis with the *Region of Interest* (ROI).

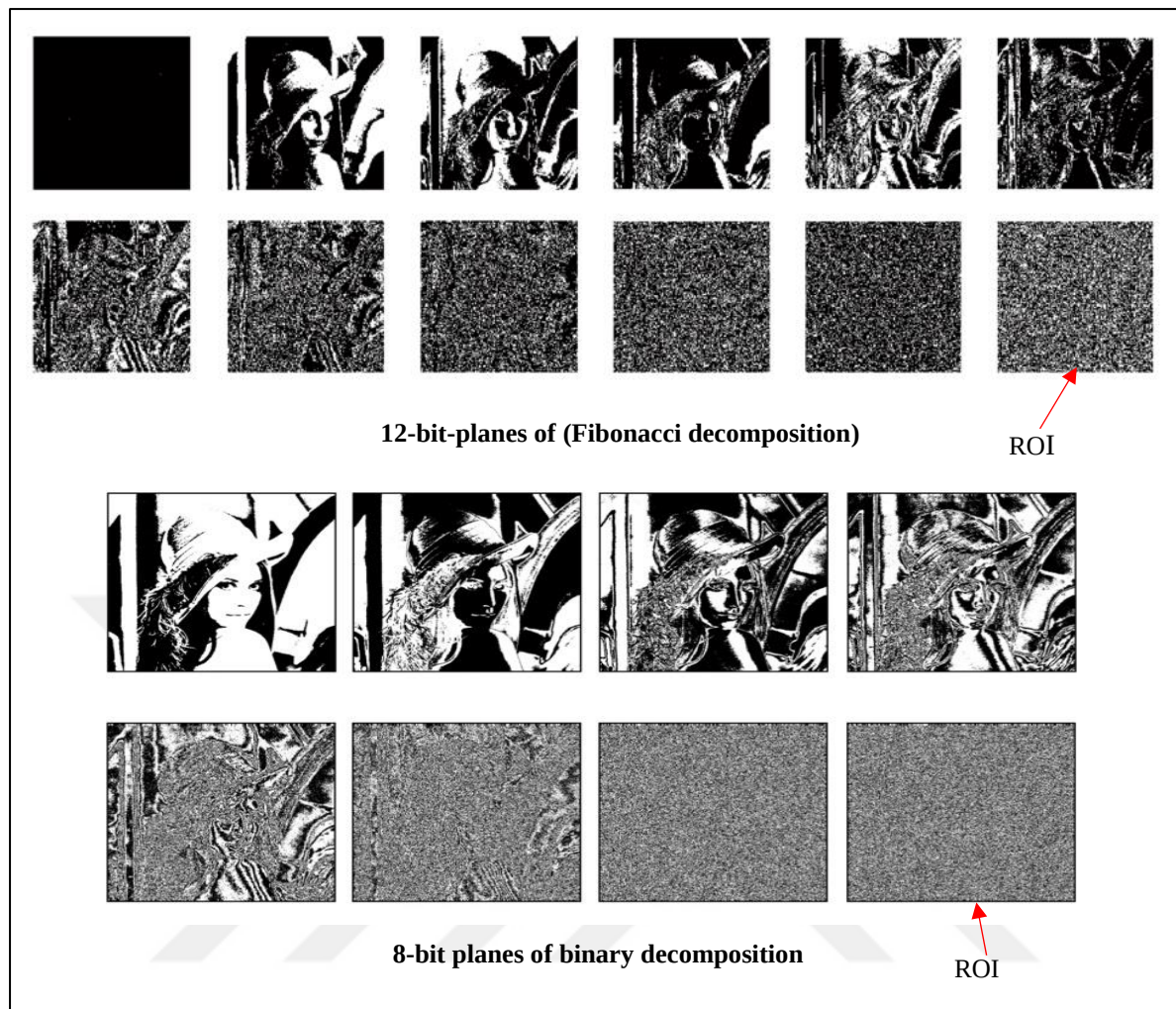


Figure 4.4: The difference between Fibonacci and binary decomposition

The Chi-square is a category of a statistical attack as it computes the theoretically expected frequency distribution of LSB in the stego image. Specifically, the attack observes certain sample distribution that is changed in the stego image. As the attacker does not have the original image or cover image to compare with the stego image, the attack compares the information that it is derived from instead. Thus, arithmetic means of the frequencies are used for this purpose. Embedding that occurs in LSB may be in odd or even value, which has no effect on the the sum frequency. Worthiness of the embedding approach is assessed in terms of the extent that the approach is able to retain the theoretically expected frequency distribution of a random sample. The chi-squared statistical attack shows the probability of embedding information into image by checking the frequency of the (LSB) in the result image (Stego Image). Chi-squared statistical test computes the probability of embedding hidden

information in an image by checking the frequency of LSB in the result image (Stego Image). In figure 4.5 shows the χ^2 tests for the original image before embedding.

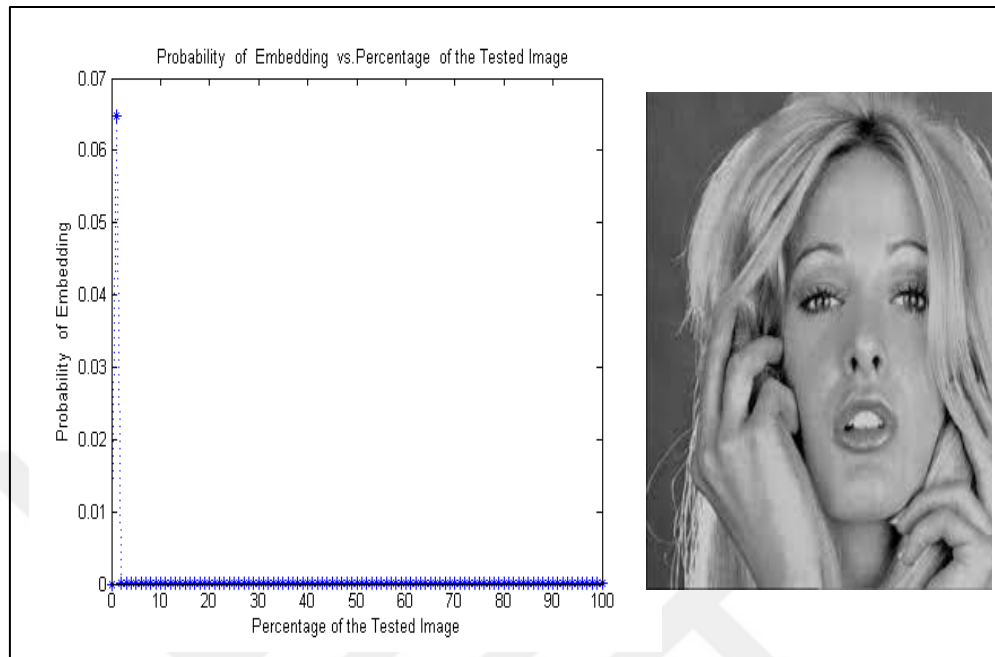


Figure 4.5: The χ^2 -test for the original Tiffany image

The x-axis represents the percentage of the whole image while the y-axis shows the probability of hiding the private message (secret data) in an image (Figure 4.6). In the first 10%, the probability is 0.065 because when the function checks the pixels most of the characters in the alphabet start with the same value of the frequent bits. Thus, the test detects this frequently and suggests these pixels as the embedded data. For the rest of the images, there is no detection for the embedding, and this is normal because the original image does not have any hidden data. Thus, after embedding the 16384 bytes to the image different methods generate different results. Figure 4.6 shows a simple LSB method where the χ^2 -test detects 50% (red arrow) of the image as the hidden data with a probability the reaching 1 (blue arrow).

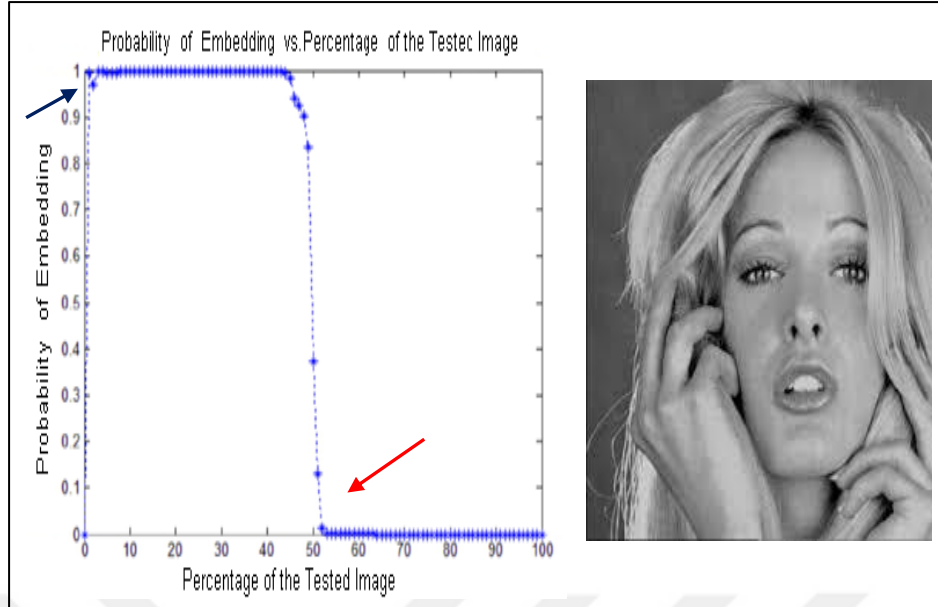


Figure 4.6: The χ^2 -test for the simple LSB method with embedded 16384 pixels

The simple LSB method is easy to detect by the χ^2 tests, where the image cannot be recognized by the naked eye. For this reason, the proposed system considered the statistical analysis to embed the secret bits. By checking the bits before embedding, the big change of the LSB can be lowered, thereby allowing the proposed system to withstand the χ^2 attacks as shown in Figure 4.7. It is clear from the behavior of the χ^2 curves (Figure 6.13) that it covers the entire image with a low probability even better than the original image (Figure 4.7). This is because the statistical distributions of the values in the LSB are good because the segments of the secret bits are chosen carefully. The payload also affects the χ^2 tests in the probability section.

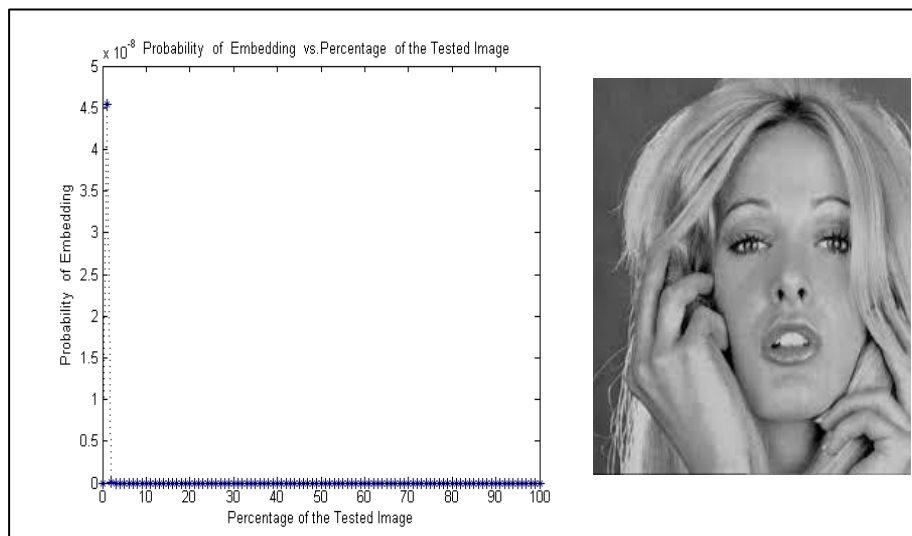


Figure 4.7: The χ^2 performance test after concealment 16384 dB.

With the increase in the payload, the degree of the probability is increased as well and vice versa when 32768 bytes and 49152 bytes are embedded in the Tiffany image (Figure 4.8). Figure 4.8 (a) shows the embedding of 49152 bytes that makes the probability 0.8. The payload of 32768 bytes in Figure 4.8 (b) produced a probability of 0.045. In this case, the increase in the payload capacity is affected very much by the χ^2 attacks. This is one of the advantages of the proposed method in addition to the security. The compression processes played a key role by preparing the secret data before embedding it. This in turn made the behavior of the χ^2 of the stego image identical to the χ^2 of the original image.

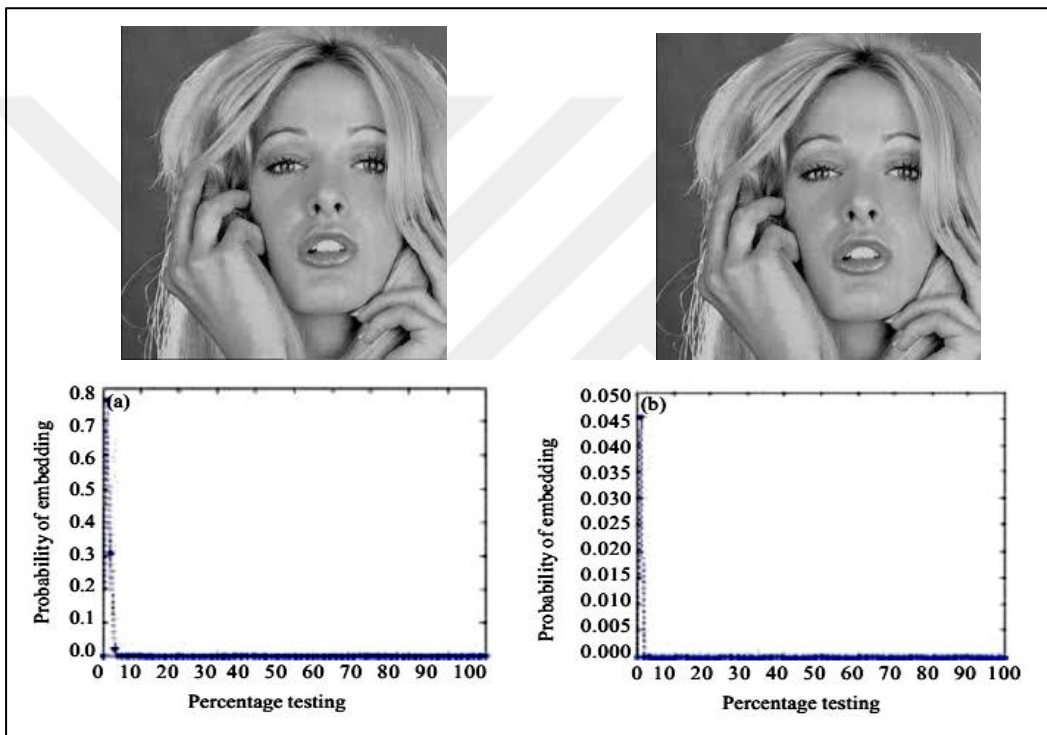


Figure 4.8: The embedment using the proposed system for the baboon image with (a) 49152 and (b) 32768 bytes

In conclusion, the χ^2 tests can detect the degree of security of the system where the results are based on the embedding method. If the statistical distribution of the pixel's value in the image is considered, then it is possible to accomplish good results. For the first part of the image, around 9% was embedded and the test behaved as if detecting the hidden data inside which was due to the identical frequency of all letters starting with the same bits' value. The χ^2 relation yields:

$$\chi^2 = \sum \frac{(\text{Observed} - \text{Expected})^2}{\text{Expected}} \quad 4.3$$

4.2.3 Human Visual System Attack

The most widely used embedding technique is the LSB method that can host the secret data because the LSB pixels are difficult for the human eyes to recognize. The replacement of the LSB values by the secret bits' values makes it difficult for the system to distinguish the LSB and randomize the bits. However, edges can be detected by a system when it becomes blurred or unclear. Consequently, the HVS attack can be detected by the LSB which is still ambiguous to the human sight because it is trained to recognize the known things. The idea behind the HVS attack is to remove the important information represented as the cloud formation. This information does not belong to the LSBs that are located in the MSBs. In this case, the human eye now can distinguish the presence or absence of the hidden data as shown in Figure 4.9.

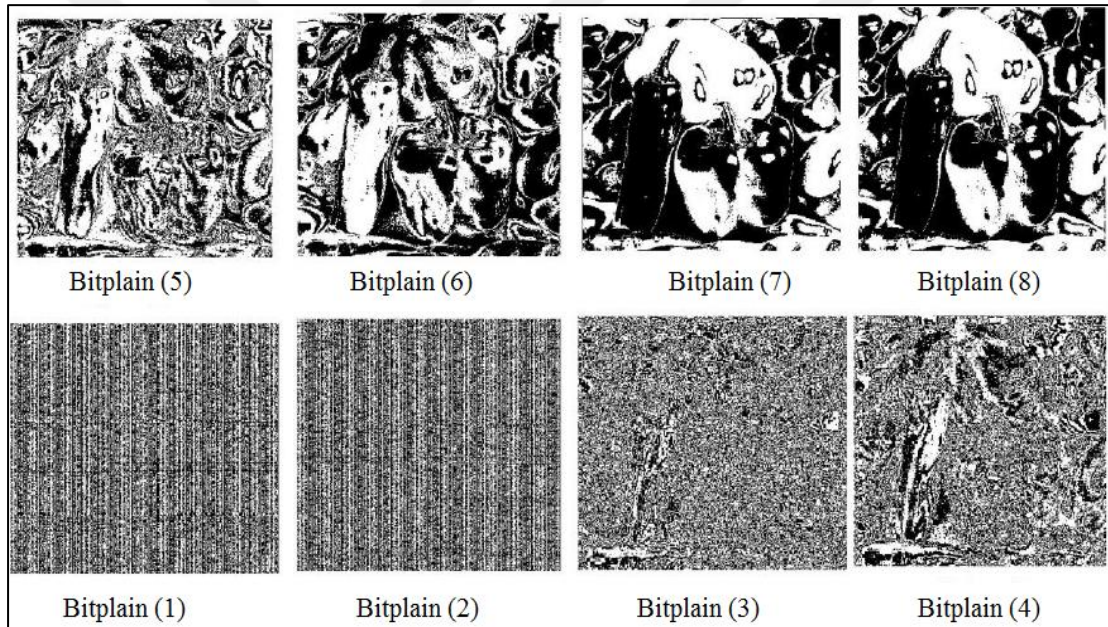


Figure 4.9: The demonstration of the visual attacks with different bit planes for the peppers image

The eight-bit planes HVS attack can detect only the LSBs, and the rest are ignored. In Figure 4.9 the embedding in the bit planes (1 and 2) is very clear where the vertical lines refer to the frequencies in their bits, implying that in this two-pixel hidden information is embedded. This type of detection is somewhat interactive between the system and humans because the system generates the pattern and human eyes detect it. Therefore, it is an example of the poor embedding method that illustrates the working principle of the HVS attack. To test the efficiency of the proposed system, three methods were applied to the images so that it was

easy to determine the differences when compared. Figure 4.10 depicts these three methods including the simple LSB, Fibonacci, and proposed P_{single} / P_{double} method.

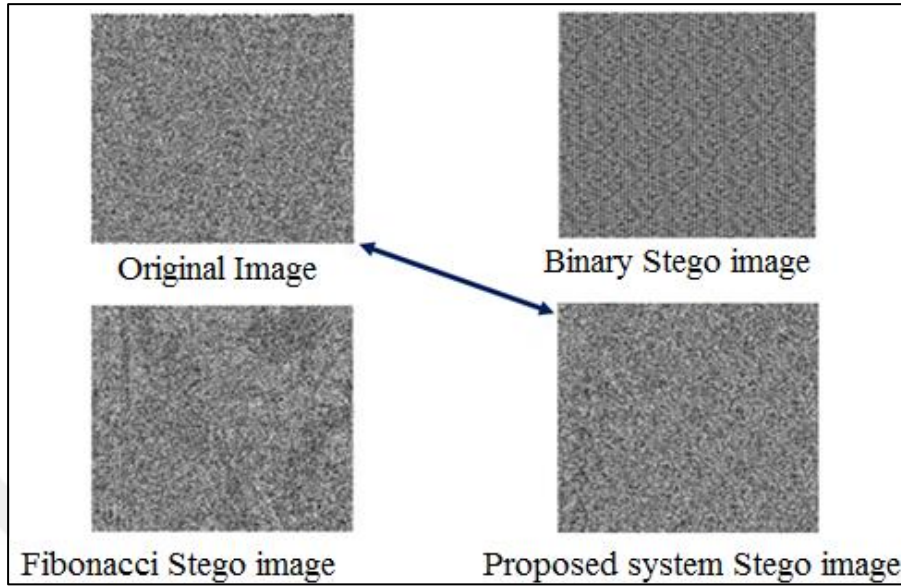


Figure 4.10: The performance of the present methods against HVS attack for the original Tiffany image

It is observed in Figure 4.10 that the embedment of the simple LSB images is not good because it can easily be detected by the human eyes due to the insertion of the secret bits directly without manipulation or choosing the bit position. For the Fibonacci method, the values of the bits are changed already during the embedding. Thus, when the pixel values are stored again in the image it is changed over to binary, which is worthy in terms of the HVS and robustness. This was precisely the reason for combining the Fibonacci with the proposed method, where the robustness was reflected in the security of the system. The worthiness of the system can also be evidenced by the results that are very close to the original image. In short, the proposed system (Figure 6.10 produced a more similar outcome (after embedding) to the original image (before embedding) than other methods due to the arbitrary distribution of the bits. Moreover, it kept the values of the original image bits identical by mapping the secret bits before embedding them. For the training of the system, the new images from the dataset were used in the current research. The results were convincing as displayed in Figure 4.11. This training was for the bit plane (1) of the LSBs, and the results were almost identical to the original image. The HVS attack is of two categories where the first one is the filter working in the frequency domain and the second one is the filter working in the spatial domain which signifies the degree of occupation of the image bits by the embedded data. This type

of attack works on certain regions of the image but is occluded by other parts of the scene represented by the secret message. Therefore, this kind of test does not remove the mask from an image but makes it clear to the human eyes.

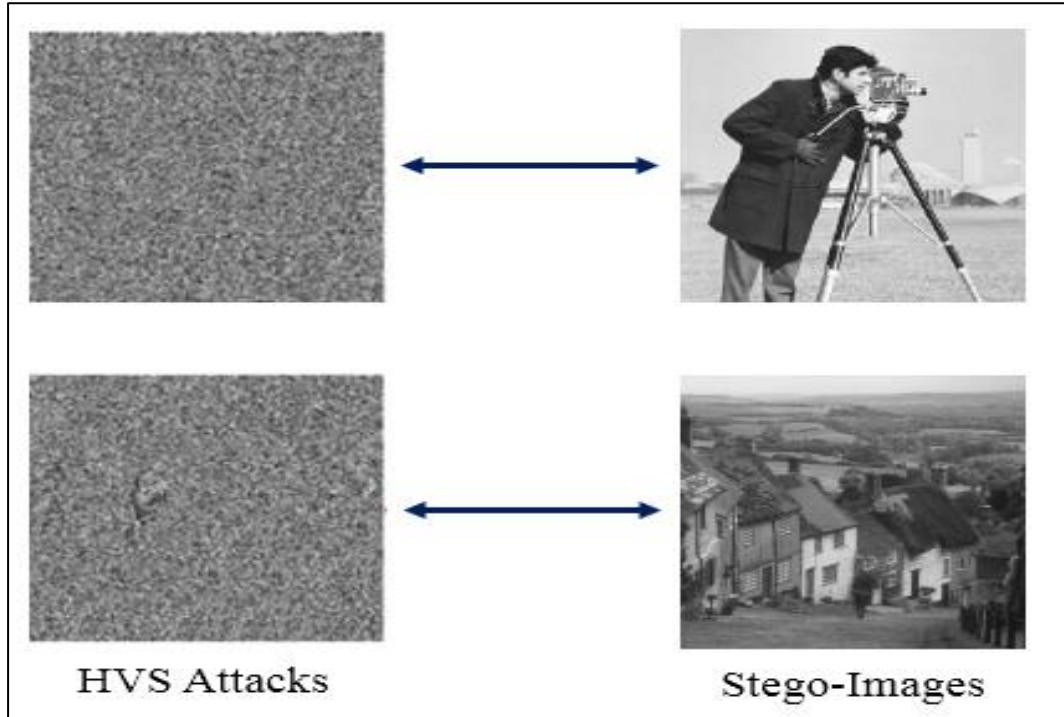


Figure 4.11: The bit plane (1) of the camera man and gold hill images with the proposed $Pixel_s / Pixel_d$ method

4.3 SUMMARY

In this chapter, the experimental results or finding is presented in detail with analysis. Graphical User Interface (GUI) of the simulation system provided in detail with the main and sub-main menu, imperceptibility of the system presented in this chapter, and how the difference among produced images referred by PSNR to prevent image distortion. Many tables and figures used to depict the findings result in terms of imperceptibility. Payload capacity and its effect in the system are discussed in detail with illustration tables and specify limits that should not exceed in the system of capacity. The objective and subjective attacks have been presented and how do they affect the hosted image.

5. CONCLUSION AND FUTURE WORK

5.1 INTRODUCTION

Steganography system helps to conceal secret information such as text inside a trusted carrier such as an image. Many methods have been proposed in the literature [13][23], but the challenge of low security and PSNR in hiding information remains (Mukherjee et al., 2020). Based on these problems, this study proposed an enhanced method to concealment the secret message to an image that is impalpable and undetected by intruders. The proposed method is able to withstand any kind of attacks such as chi-square and HVS attacks. In this chapter, we will summarize the conclusion and the future work stemming from the present research.

5.2 CONCLUSION

This study has successfully achieved all the proposed objectives related to the development of an outperforming steganography system. The main contributions of this study were to emphasize the most and common issues in the existing steganography systems including the payload capacity and security enhancement via the utilization of the new decomposition that is yet unfamiliar to the hackers or attackers. The main process in proposed method is three. The following subsections explain the mentioned three procedures. This stage carries two main processes that working together to enhance the proposed system. The first process is to compress secret message with Huffman coding algorithm to reduce the amount of data embedded to the image which mean enhance the capacity of the steganography method, by eliminating the redundant characters in the secret message. And 1; 110:107618rocess improve the robustness of the method and making analysis process very difficult to the attacker. The second process is converting logically the binary system of the image pixels into a Fibonacci decomposition and transfer the 8 bits (for each pixel) into 12 bits. As this process gives good robustness to the proposed system. Different methods have been proposed in the state of arts each has many ways to concealment the secret data. The LSB embedding is the common method used. With the proposed system, the embedding will become an adaptive using $Pixel_s/Pixel_d$ procedure. When we need to embed, the

algorithm will check pixels' value selected with corresponding single / double value of secret decomposition of secret message to check the condition for embedding.

5.3 CONTRIBUTION

The main objective of this research is to enhance the proposed image steganography system by increasing security by maintaining the PSNR value. In this study, a high payload capacity for the secret data is required to be concealment. The results achieved in this study indicate that the proposed system is efficient in terms of security and capacity. However, the current study has many valuable contributions which are like: The Enhanced Proposed Study Is Considered Highly Robust Against Any Statistical Attack as Fibonacci Decomposition Is Used to Transfer the Pixel Value of The Cover Image Logically From 8 To 12 Bits, Which Means More Chaotic and This Case Is Still Unknown By The Intruders. The other important gap in existing literature works is the embedding methods. With $P_{i_x}l_s/P_{i_x}l_d$ method. The security of the proposed system is almost impossible to reveal because the proposed embedding method is based on the adaptive way to choose the target pixels rather than sequentially concealment. It has been proven by testing the stego image that this method produced a high value of imperceptibility. Some systems may give good results with certain payload capacity but when the capacity is increased even a little the PSNR will drop down and the secret inside the image will become easy to reveal. Robustness is related to how to increase the capacity of the system while maintaining the security and PSNR of the system. Compressing the secret message using Huffman with $P_{i_x}l_s/P_{i_x}l_d$ method before embedding makes the proposed method more robust and achieved satisfactory results when tested with chi-square and HVS attacks.

5.4 FUTURE WORK

Achieving an improved and robust steganography system is ever demanding. In this study, all the proposed objectives are accomplished successfully with major contributions. Promising results are obtained. However, these results are far from the ideal ones that require further studies in this field. This study opened up many new research directions that are worth looking in the future. This new research must be explored to improve the robustness of the existing steganography system against all types of attacks. In fact, the security of the existing steganography scheme can be improved via mixing the frequency domain with an additional approach, thereby achieving superior results in terms of the

capacity and security. The limitation associated with the security of the secret messages so called PSNR has caused great difficulty to the improve steganography system against various attacks. Thus, it may be ideal to handle the secret message prior to the dynamical embedding by making the preparation steps interactive with the embedding process.



REFERENCES

- [1] Hsieh KS, Wang CM. Constructive image steganography using example-based weighted color transfer. *Journal of Information Security and Applications*. Mar 1; 65:103126.2022.
- [2] Nguyen TD, Le HQ. A secure image steganography based on modified matrix encoding using the adaptive region selection technique. *Multimedia Tools and Applications*. Mar 22:1-31.2022.
- [3] Aslam MA, Rashid M, Azam F, Abbas M, Rasheed Y, Alotaibi SS, Anwar MW. Image Steganography using Least Significant Bit (LSB)-A Systematic Literature Review. 2nd *International Conference on Computing and Information Technology (ICCIT)* Jan 25 (pp. 32-38). IEEE.2022.
- [4] Tang L, Wu D, Wang H, Chen M, Xie J. An adaptive fuzzy inference approach for color image steganography. *Soft Computing*. Aug;25(16):10987-1004.2021.
- [5] AlKhodaidi T, Gutub A. Refining image steganography distribution for higher security multimedia counting-based secret-sharing. *Multimedia Tools and Applications*. Jan;80(1):1143-73.2021.
- [6] Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A. Image steganography: A review of the recent advances. *IEEE Access*. Jan 25.2021.
- [7] Liao X, Yu Y, Li B, Li Z, Qin Z. A new payload partition strategy in color image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*. 2019 Jan 31;30(3):685-96.
- [8] Lu SP, Wang R, Zhong T, Rosin PL. Large-capacity image steganography based on invertible neural networks. *InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 10816-10825).2021.
- [9] Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A. Image steganography: A review of the recent advances. *IEEE Access*. Jan 25.2021.
- [10] Abd EL-Latif AA, Abd-El-Atty B, Venegas-Andraca SE. A novel image steganography technique based on quantum substitution boxes. *Optics & Laser Technology*. Aug 1;116:92-102.2019.
- [11] ALabaichi A, Al-Dabbas MA, Salih A. Image steganography using least significant bit and secret map techniques. *International journal of electrical & computer*

- engineering* (2088-8708). Feb 15;10(1).2020.
- [12] Hassaballah M, Hameed MA, Awad AI, Muhammad K. A novel image steganography method for industrial internet of things security. *IEEE Transactions on Industrial Informatics*. Jan 22;17(11):7743-51.2021.
 - [13] Li Q, Wang X, Ma B, Wang X, Wang C, Xia Z, Shi Y. Image steganography based on style transfer and quaternion exponent moments. *Applied Soft Computing*. Oct 1; 110:107618.2021
 - [14] Swain G. Very high-capacity image steganography technique using quotient value differencing and LSB substitution. *Arabian Journal for Science and Engineering*. Apr;44(4):2995-3004.2019.
 - [15] Valandar MY, Barani MJ, Ayubi P, Aghazadeh M. An integer wavelet transforms image steganography method based on 3D sine chaotic map. *Multimedia Tools and Applications*. Apr;78(8):9971-89.2019.
 - [16] Tang L, Wu D, Wang H, Chen M, Xie J. An adaptive fuzzy inference approach for color image steganography. *Soft Computing*. Aug;25(16):10987-1004.2021.
 - [17] Sahu AK, Swain G. A novel n-rightmost bit replacement image steganography technique. *3D Research*. Mar;10(1):1-8.2019.
 - [18] Liao X, Yu Y, Li B, Li Z, Qin Z. A new payload partition strategy in color image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*. Jan 31;30(3):685-96.2019.
 - [19] Gopil A, Narayana VL. Protected strength approach for image steganography. *Traitement du Signal*. Jul 1;34.2017.
 - [20] Li F, Yu Z, Qin C. GAN-based spatial image steganography with cross feedback mechanism. *Signal Processing*. Jan 1; 190:108341.2022.
 - [21] Hu D, Zhang Y, Yu C, Wang J, Wang Y. Image Steganography based on Style Transfer. *arXiv preprint arXiv:2203.04500*. Mar 9.2022.
 - [22] Ren Y, Liu T, Zhai L, Wang L. Hiding Data in Colors: Secure and Lossless Deep Image Steganography via Conditional Invertible Neural Networks. *arXiv preprint arXiv:2201.07444*. Jan 19.2022.
 - [23] Alatiyyat BF, Narmatha C. Survey on Image Steganography Techniques. *2nd International Conference on Computing and Information Technology (ICCIIT)* Jan 25 (pp. 57-64). IEEE.2022.

- [24] Akhtar, Nadeem.. “An Efficient Lossless Modulus Function Based Data Hiding Method.” In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Springer, 281–87.2016.
- [25] Li YH, Chang CC, Su GD, Yang KL, Aslam MS, Liu Y. Coverless image steganography using morphed face recognition based on convolutional neural network. *EURASIP Journal on Wireless Communications and Networking*. Dec;2022(1):1-21.2022.
- [26] Bhavani Y, Kamakshi P, Kavya Sri E, Sindhu Sai Y. A Survey on Image Steganography Techniques Using Least Significant Bit. *In Intelligent Data Communication Technologies and Internet of Things* (pp. 281-290). Springer, Singapore.2022.
- [27] Peter G, Sherine A, Teekaraman Y, Kuppusamy R, Radhakrishnan A. Histogram Shifting-Based Quick Response Steganography Method for Secure Communication. *Wireless Communications and Mobile Computing*. Mar 12;2022.
- [28] Joshi R, Bairwa AK, Soni V, Joshi S. Data Security Using Multiple Image Steganography and Hybrid Data Encryption Techniques. *International Conference for Advancement in Technology (ICONAT)* Jan 21 (pp. 1-7). IEEE.2022.
- [29] Ilasariya S, Patel P, Patel V, Gharat S. Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka. *International Conference on Smart Systems and Inventive Technology (ICSSIT)* Jan 20 (pp. 1320-1325). IEEE.2022.
- [30] Akhila L, Manoj VJ. Image Steganography using Pixel Value Differencing with Modulus Function and Optimization. *International Conference on Smart Systems and Inventive Technology (ICSSIT)* Jan 20 (pp. 1369-1373). IEEE.2022.
- [31] Liu C. A Proposal of Digital Image Steganography and Forensics Based on the Structure of File Storage. *In Proceedings of the 11th International Conference on Computer Engineering and Networks* (pp. 731-740). Springer, Singapore.2022.
- [32] Sahu AK, Sahu M. Digital image steganography and steganalysis: A journey of the past three decades. *Open Computer Science*. Jan 1;10(1):296-342.2020.
- [33] Sari, Christy Atika, Giovani Ardiansyah, De Rosal Ignatius Moses Setiadi, and Eko Hari Rachmawanto.. “An Improved Security and Message Capacity Using AES and Huffman Coding on Image Steganography.” *Telkomnika (Telecommunication Computing Electronics and Control)* 17(5): 2400–2409.2019.

- [34] Tang W, Li B, Tan S, Barni M, Huang J. CNN-based adversarial embedding for image steganography. *IEEE Transactions on Information Forensics and Security*. Jan 7;14(8):2074-87.2019
- [35] Valandar MY, Barani MJ, Ayubi P, Aghazadeh M. An integer wavelet transforms image steganography method based on 3D sine chaotic map. *Multimedia Tools and Applications*. Apr;78(8):9971-89.2019.
- [36] Pramanik S, Singh RP, Ghosh R. Application of bi-orthogonal wavelet transform and genetic algorithm in image steganography. *Multimedia Tools and Applications*. Jul;79(25):17463-82.2020.
- [37] Kini, N Gopalakrishna, and Vishwas G Kini. . “A Parallel Algorithm to Hide an Image in an Image for Secured Steganography.” In *Integrated Intelligent Computing, Communication and Security*, Springer, 585–94.2019.
- [38] Kadhim, Inas Jawad, Prashan Premaratne, and Peter James Vial.. “High Capacity Adaptive Image Steganography with Cover Region Selection Using Dual-Tree Complex Wavelet Transform.” *Cognitive Systems Research* 60: 20–32. <https://doi.org/10.1016/j.cogsys.11.002>.2019.
- [39] Hureib ES, Gutub AA. Enhancing medical data security via combining elliptic curve cryptography and image steganography. *Int. J. Comput. Sci. Netw. Secur. (IJCSNS)*. Aug;20(8):1-8.2020.
- [40] Das, Madhulina, and Samir Kumar Bandyopadhyay. “Survey and Analysis of Current Methods of Steganography.” *International Journal of modern Trends in Engineering and Research* 2(7): 527–37.2015.
- [41] Akhtar, Nadeem.. “An Efficient Lossless Modulus Function Based Data Hiding Method.” In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Springer, 281–87.2016.
- [42] Dhall, Sangeeta, Rinku Sharma, and Shailender Gupta.. “A Multi-Level Steganography Mechanism Using Quantum Chaos Encryption.” *Multimedia Tools and Applications* 79(3): 1987–2012.
- [43] Li, Mengdi et al. 2019. “Generating Steganographic Image Description by Dynamic Synonym Substitution.” *Signal Processing* 164: 193–201. <https://doi.org/10.1016/j.sigpro.2019.06.014>.
- [44] Chen B, Wang J, Chen Y, Jin Z, Shim HJ, Shi YQ. High-capacity robust image

- steganography via adversarial network. *KSII Transactions on Internet and Information Systems (TIIS)*.;14(1):366-81.2020.
- [45] Li B, Wang M, Huang J, Li X. A new cost function for spatial image steganography. *IEEE International Conference on Image Processing (ICIP)* Oct 27 (pp. 4206-4210). IEEE.2014.
 - [46] Rawat, Ritvik, Brijesh Singh, Arijit Sur, and Pinaki Mitra.“Steganalysis for Clustering Modification Directions Steganography.” *Multimedia Tools and Applications* 79(3–4): 1971–86.2020.
 - [47] Qian, Zhenxing, Kim-Kwang Raymond Choo, Rémi Cogranne, and Xinpeng Zhang.. “Multimedia Security: Novel Steganography and Privacy Preserving.” *Security and Communication Networks* 2018.
 - [48] Kadhim, Inas Jawad, Prashan Premaratne, Peter James Vial, and Brendan Halloran. 2019. “Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research.” *Neurocomputing* 335: 299–326. <https://doi.org/10.1016/j.neucom.2018.06.075>.
 - [49] Hussain, Mehdi et al.. “Image Steganography in Spatial Domain: A Survey.” *Signal Processing: Image Communication* 65(December 2017): 46–66.2018.
 - [50] Singh, Neha, Mamta Jain, and Sunil Sharma.. “A Survey of Digital Watermarking Techniques.” *International Journal of Modern Communication Technologies and Research* 1(6): 265852.2013.
 - [51] Al-Husainy, Mohammed Abbas Fadhil, and Diaa Mohammed Uliyan.. “A Secret-Key Image Steganography Technique Using Random Chain Codes.” *International Journal of Technology* 10(4): 731–40.2019.
 - [52] Swain G, Lenka SK. Classification of image steganography techniques in spatial domain: a study. *Journal of Computer Science & Engineering Technology (IJCSET)*. Jan;5(03):219-32.
 - [53] Al-Husainy, Mohammed Abbas Fadhil, and Diaa Mohammed Uliyan.. “A Secret-Key Image Steganography Technique Using Random Chain Codes.” *International Journal of Technology* 10(4): 731–40.2019.
 - [54] Chakraborty, Soumendu, Anand Singh Jalal, and Charul Bhatnagar.. “LSB Based Non Blind Predictive Edge Adaptive Image Steganography.” *Multimedia Tools and Applications* 76(6): 7973–87.2017.

- [55] Al-tamimi, Abdul-gabbar Tarish, and Abdulmalek Abduljabbar Alqobaty.. “Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm.” *International Journal of Computer Science and Information Security; Pittsburgh* 13(1): 5500.2015.
- [56] Al-Husainy, Mohammed Abbas Fadhil, and Diaa Mohammed Uliyan.. “A Secret-Key Image Steganography Technique Using Random Chain Codes.” *International Journal of Technology* 10(4): 731–40.2019.
- [57] Agarwal, Parth, Dhruve Moudgil, and S Priya.. “Encrypted Transfer of Confidential Information Using Steganography and Identity Verification Using Face Data.” In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, 155–66.2020.
- [58] Sailaja, C, and Srinivas Bachu.. “A Comparative Study on LSB Replacement Steganography.” In *Innovations in Electronics and Communication Engineering*, Springer, 601–12.2020
- [59] Mahajan, Manish, and Navdeep Kaur.. “Adaptive Steganography: A Survey of Recent Statistical Aware Steganography Techniques.” *International Journal of Computer Network and Information Security* 4(10): 76.2012.
- [60] Zodpe, H., & Sapkal, A. An efficient AES implementation using FPGA with enhanced security features. *Journal of King Saud University-Engineering Sciences*, 32(2), 115–122.2020.
- [61] Al-Nofaie, S., Gutub, A., & Al-Ghamdi, M. Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces. *Journal of King Saud University-Computer and Information Sciences*.2019.
- [62] Mukherjee, Nabanita, Goutam Paul, Sanjoy Kumar Saha, and Debanjan Burman.. “A PVD Based High Capacity Steganography Algorithm with Embedding in Non-Sequential Position.” *Multimedia Tools and Applications*: 1–31.2020.
- [63] Sengupta, A., & Rathor, M. IP Core Steganography for Protecting DSP Kernels Used in CE Systems. *IEEE Transactions on Consumer Electronics*, 65(4), 506–515. <https://doi.org/10.1109/TCE.2019.2944882>.2019.
- [64] Patil, Rupali, and Dipak Pawar. “Secure Audio Steganography by LSB for Hiding Information.” *International Journal of Innovations in Engineering Research and Technology* 3(4): 1–6.2016.

- [65] ALabaichi, Ashwak, Maisa'a Abid Ali Al-Dabbas, and Adnan Salih.. "Image Steganography Using Least Significant Bit and Secret Map Techniques." *International Journal of Electrical & Computer Engineering (2088-8708)* 10.2020.
- [66] Bedi, Punam, and Arti Dua. "Network Steganography Using the Overflow Field of Timestamp Option in an IPv4 Packet." *Procedia Computer Science* 171: 1810–18.2020.
- [67] Al-Husainy, Mohammed Abbas Fadhil, and Diaa Mohammed Uliyan.. "A Secret-Key Image Steganography Technique Using Random Chain Codes." *International Journal of Technology* 10(4): 731–40.2019.
- [68] Prasetyadi, Gotfried C, Achmad Benny Mutiara, and Rina Refianti. 2017. "File Encryption and Hiding Application Based on Advanced Encryption Standard (AES) and Append Insertion Steganography Method." *Second International Conference on Informatics and Computing (ICIC)*, IEEE, 1–5.2017.
- [69] Cancelli, Giacomo, Gwenaël Doërr, Mauro Barni, and Ingemar J Cox. . "A Comparative Study Of±steganalyzers." In *2008 IEEE 10th Workshop on Multimedia Signal Processing*, IEEE, 791–96.2008.
- [70] Chakraborty, Soumendu, Anand Singh Jalal, and Charul Bhatnagar. "LSB Based Non Blind Predictive Edge Adaptive Image Steganography." *Multimedia Tools and Applications* 76(6): 7973–87.2017.
- [71] Al-Harbi, Omnia Abdullah, Walaa Essa Alahmadi, and Asia Othman Aljahdali.. "Security Analysis of DNA Based Steganography Techniques." *SN Applied Sciences* 2(2): 1–10.2020.
- [72] Bucerzan D, Rațiu C, Manolescu MJ. SmartSteg: a new android-based steganography application. *International Journal of Computers, Communications and Control*. Oct 1;8(5):681.2013.
- [73] Mohsin AH, Zaidan AA, Zaidan BB, Ariffin SA, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI, Hashim M. Real-time medical systems based on human biometric steganography: A systematic review. *Journal of medical systems*.Dec;42(12):1-20.2018.
- [74] Bao Z, Guo Y, Li X, Zhang Y, Xu M, Luo X. A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. *Journal of Ambient Intelligence and Humanized Computing*.

May;11(5):1889-901.2020.

- [75] Farrag S, Alexan W. Secure 2d image steganography using recaman's sequence. *International Conference on Advanced Communication Technologies and Networking (CommNet)* Apr 12 (pp. 1-6). IEEE.2019.
- [76] Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*. Mar 28;335:299-326.2019.
- [77] Ghebleh M, Kanso A. A robust chaotic algorithm for digital image steganography. *Communications in Nonlinear Science and Numerical Simulation*. Jun 1;19(6):1898-907.2014.
- [78] Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M. CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*. 2017 Mar;76(6):8597-626.
- [79] Nyeem H. Reversible data hiding with image bit-plane slicing. *20th International Conference of Computer and Information Technology (ICCIT)* Dec 22 (pp. 1-6). IEEE.
- [80] Shanthakumari R, Malliga S. Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. *Multimedia Tools and Applications*. Feb;79(5):3975-91.2020.
- [81] Rasheed ZA. Steganography Technique for Binary Text Image. *International Journal of Science and Research (IJSR) ISSN (Online)*. Jan:2319-7064.2015.
- [82] Bower A, Insoft R, Li S, Miller SJ, Tosteson P. The distribution of gaps between summands in generalized Zeckendorf decompositions. *Journal of Combinatorial Theory, Series A*. Oct 1;135:130-60.2015.
- [83] Li B, He J, Huang J, Shi YQ. A survey on image steganography and steganalysis. *J. Inf. Hiding Multim. Signal Process*. Apr 1;2(2):142-72.2011.