T.C.

ALTINBAŞ UNIVERSITY

Graduate School of Science and Engineering

Information Technologies

AN EFFECTIVE MEDICAL IMAGE STEGANOGRAPHY BASED ON PIXELS DISPARITY VALUE TO IMPROVE THE SECURITY AND IMPERCEPTIBILITY

Mohammed Kareem Abed ABED

Master's Thesis

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2020

AN EFFECTIVE MEDICAL IMAGE STEGANOGRAPHY BASED ON PIXELS DISPARITY VALUE TO IMPROVE THE SECURITY AND IMPERCEPTIBILITY

by

Mohammed Kareem Abed ABED

Information Technologies

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2020

The thesis titled “AN EFFECTIVE MEDICAL IMAGE STEGANOGRAPHY BASED ON PIXELS DISPARITY VALUE TO IMPROVE THE SECURITY AND IMPERCEPTIBILITY” prepared and presented by “Mohammed Kareem Abed ABED” was accepted as a Master of Science Thesis in Information Technologies.

Asst.Prof.Dr. Sefer KURNAZ

Supervisor

Thesis Defense Jury Members:

Asst.Prof.Dr. Sefer KURNAZ	School of Engineering and Natural Sciences, Altinbas University	_____
Assoc.Prof.Dr. Yasa EKŞİOĞLU ÖZOK	School of Engineering and Natural Sciences, Altinbas University	_____
Prof.Dr. Mesut RAZBONYALI	faculty of engineering and architecture Maltepe University	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Mohammed Kareem Abed ABED

Signature

DEDICATION

First, I would like to thank Allah Almighty for the power of the mind, health, strength, guidance, knowledge, and skills to complete this study.

I would like to dedicate this work to my first teacher, my mother, my first supporter and role model, my father and my companion throughout the journey. Without you, this dream would never come true and to my brother and my sister who stood with me in order to achieve my dream.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all the instructors that have taught me more than just science, especially my supervisors Asst. Prof. Dr. Sefer KURNAZ, for all the time, support and guidance provided to me along the journey to accomplish this work. Thank you all for all the knowledge and advice that made me overcome all the difficulties that I have faced.

ABSTRACT

AN EFFECTIVE MEDICAL IMAGE STEGANOGRAPHY BASED ON PIXELS DISPARITY VALUE TO IMPROVE THE SECURITY AND IMPERCEPTIBILITY

ABED, Mohammed Kareem Abed

M.Sc. Information Technologies, Altınbaş University,

Supervisor: Asst.Prof. Dr. Sefer KURNAZ

Date: November, 2020

Pages: 94

The steganography is an emerging and greatly demanding technique for the secured information communication over the internet web using a trusted media such as an image so that it becomes unnoticeable by intruders or unauthorized users. The steganography can be categorized into several types depending on the cover medium including the image, audio, text, video, DNA or even protocol. Commonly, the digital images are used as the cover for the steganography owing to their redundancy in the representation, making them hidden to the intruders/hackers/adversaries/unauthorized users. Still, any steganography system launched over the WWW can be cracked upon recognizing the stego cover. Thus, the undetectability that involves the data imperceptibility or concealment and security is the significant trait of any steganography system. Presently, the design and development of an effective image steganography system are facing several challenges including the low capacity, poor robustness and imperceptibility. To surmount such limitations, it is important to improve the capacity and security of the steganography system while maintaining a high signal-to-noise ratio (PSNR). Based on these factors, this study aimed to design and develop a Pixels Disparity Value (CLV) method to effectively embed the secret data into a cover image for achieving a robust steganography scheme. The design and implementation of the proposed scheme involved three phases. First, an enhanced Huffman compression algorithm to improve the text security and payload capacity of the scheme. Second,

the image decomposition normalization before the embedding process. Third, an improved embedding method was utilized by integrating a random block/pixel selection with the CLV and implicit secret key generation for enhancing the imperceptibility of the scheme. The performance of the proposed scheme was assessed experimentally to determine the imperceptibility, security, robustness, and capacity. The standard USC-SIPI and medical images were used as the benchmarking dataset for the performance evaluation and comparison of the proposed scheme with the existing state-of-the-art reports in the recent literature. The resistance of the proposed scheme was tested against the statistical, HVS steganalysis detection attacks. The obtained PSNR and SSIM values revealed the accomplishment of the higher imperceptibility and security by the proposed CLV method while maintaining a higher capacity compared to the reported findings.

Keywords: Medical Images, Image Steganography, Huffman Coding, Security, Imperceptibility

TABLE OF CONTENTS

Pages

LIST OF FIGURES

Pages

LIST OF TABLES

Pages

LIST OF ABBREVIATIONS

SSIM : Structural Similarity Index For Measuring

PDV : Pixels Disparity Value

PSNR : Peak Signal To Noise Ratio

EP : Embedding Process

CPS : Cyber-Physical Systems

1. INTRODUCTION

1.1 INTRODUCTION

Steganography can define as the art of concealing secret data or information within non- secured media such as image. Lately, security in term of images took more attention due to increasing the applications in such domain. Thus, data hiding in image or steganography got a lot of studies and contributions in this field.

All documentations such as video, audio and image has been digitalizing due to the rapid growth of the electronic era. So security and reliability of such documents increased for each hosting media to maintain privacy [1]. Two techniques used for this purpose which are steganography and encryption, first one is perceptible as noise and second one considered as human eye [2]. Easy and robust ways to editing data provided by current digital multi-media. Over computer network data should delivered safely is needed without any interference. Steganography is the art of concealing data over pixels of image or other media such video or audio. A modern technology has created threats to ensure and secure information transmitted within network and digital communication. Two techniques used for this purpose to gain security which are encryption and steganography. For encryption scrambling for data is used by different method and information, while steganography responsible for hiding secret data without notice by any presence. Any information wills carried by the image called stego image that mean image carry secret data [3]. Stego image must be in form of not detectable from any intruder. The main factors in steganographic are high capacity, better imperceptibility (PSNR), robustness for distorted or noise in the system while communication [4]. There are two main requirements for steganography system which are embedding method and extracting method. Embedding is the main process in sender part which is reflect the different technique for steganography and the extracting to reveal the secret message from stego image in receiver side. Steganography technique deferent from one to another by embedding and how to hide secret message inside cover image to get stego image that carry the secret message at the same time all strategy of embedding store in stego key. In the receiver side doing the same process of embedding but in reverse that called extracting by using stego key.

Several issues and problems in security and hiding secret data in the image still undissolvedin additional to understanding how to embed the secret data in image still undiscovered.

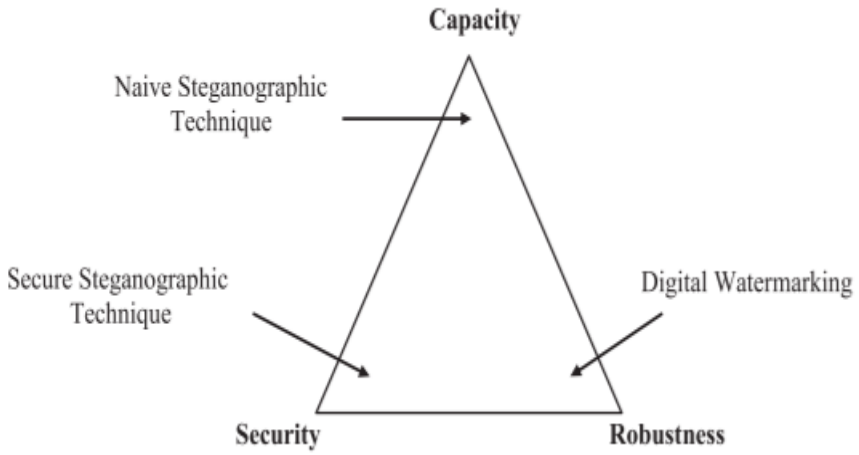


Figure 1.1: Trade-off among the properties of the Information hiding.

Different solutions are predictable to discover great systems and possibilities occurs in medical [5] or military [6]. Now days, the key issues and difficulties associated with three main things such as lack of (1) increasing the payload capacity which reflect the amount of data embedded to the image that is limited in existing methods, (2) security of secret message hiding in the image, and (3) maintaining the robustness and imperceptibility of steganography system a way that keep the security high. Figure 1.1 presents the steganography method performance criteria.

Information hiding including differentteyps, the secret message can be embed in several media such as image, audio, text, video, or even protocol. Each has its advantage and disadvantage [7]. Information hiding is defined as hiding text in the image that can call steganography. Many types of media used to host the data, such as text, image, video… etc, as shown in Figure 1.2 and with proposed method, we consider the image as a media to host text secret message.

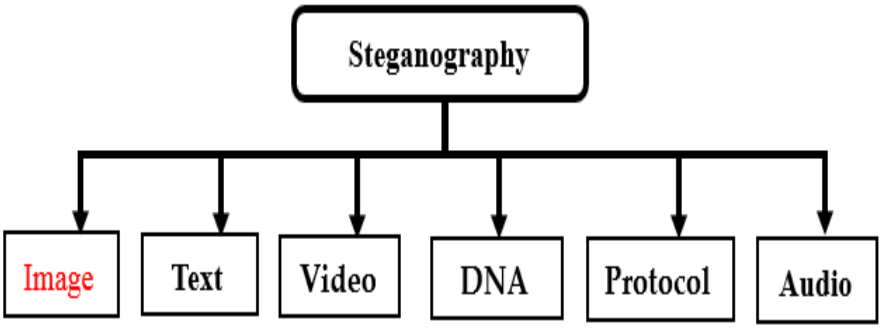


Figure 1.2: The steganography mediums.

1.2 EXISTING PROBLEM

The main problems in information hiding or steganography are the size of information or data embedded inside the media, the security, and imperceptibility (embedding method). The embedding methods including security and capacity are not achieved high scores yet, and research of such fields still on-going.

1.2.1 Security

Requirement of data security becomes necessary because of the privacy issue The data spread over the web and internet now is sensitive needs to authorize in many fields such as financial, medical and military. However, some mechanism of protection is needed and necessary from any hackers or intruders.

Modern steganography need secret key to store the method of hidden message. Because of the secret key in steganography security becomes more accurate and confident. Internet widely used in communication and transform media, one of the most important media through the internet is image due to flexibility and easy to process. So image considers the most acceptances choose among the media to host secret information inside it but security remains outstanding challenging.

1.2.2 Embedding method

Secret message will convert into a serial of bits and these bits should embed inside an image that is called cover image which is cover all the information inside. Image pixels (Picture Cells) will host secret bit accordingly, choosing of which pixel from whole pixels called embedding technique in addition to selecting the best bit to replace from this pixel (one-pixel consist of 8-bits) More interest by researchers in the existing methods and during the past decade considered steganography and steganalysis. In order to the fact steganography just considers less important bit impact or little important, an attacker can check and trace both less and high importance in the image. From this point of view, the importance of the embedding process comes in. Many researchers in literature introduce different methods for embedding some of them were difficult to estimate or discover by the attacker and other was easy to reveal by an intruder [8]. The complexity

of the embedding method not effect here but smart technique play a vital role here and how to hide a secret bit in a way cautious and not seen by the hacker's algorithm not just hide from human eye.

Existing methods most of them used the Least Significant Bit (LSB) for embedding and hiding the secret message. Critical space for holding the message always manipulates to make it appropriate for hosting a secret bit. The LSB considered as spatial domain class Figure 1.3 that has advantages and disadvantages however the majority take advantage of that due to easy understanding and use.

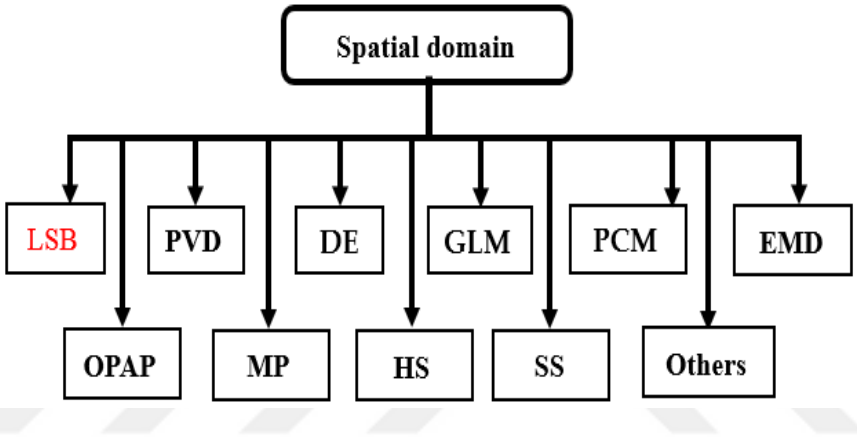


Figure 1.3: The spatial domain techniques in image steganography.

1.2.3 Capacity

The maximum payload that can image hold within embedding in the steganography system called capacity. Steganography suffers from weaknesses that affect the system, one of these weaknesses is capacity. The proposed method used the LSB technique for embedding and add a secret message to the pixel, this LSB is limited due to inserting is just use one or two bits to host the data. To solve this method we used the compression technique represented by Huffman. Stego image is critical to increasing secret messages because of cannot stand against the attack and become critical. Therefore, the Human Visual System (HVS) attack is used to draws a map of LSB pixels and if there is much payload capacity pattern will recognize it. So, any exchange in LSB will be sensitive.

1.3 PROBLEM STATEMENT

There are several issues in the existing image steganography systems that need to be overcome. Firstly, payload security must be improved to prevent attackers from reading the contents of the hidden message even if they managed to analyse the stego image. These methods are well-known to intruders, which make it to reveal the secret text once detected in the stego image. Secondly, existing solutions suffer from a high rate of MSE which decreases the imperceptibility (PSNR) of the stego image and adversely affects the robustness of the steganography system [9] . Thus, it is important that the steganography solutions address this issue and decrease MSE to improve the imperceptibility of the stego image. In addition, existing steganography solutions suffer low embedding capacity. Although some of these solutions employed several compression techniques to compress the secret message before embedding, their concern was to reduce the size of the secret text. Such a reduction is suboptimal as it overlooks the capacity limitation of the stego image. For an effective steganography system, it is important to decrease the size of secret text while increasing the capacity of the stego image. Thus, a new scheme is needed for expending the coding value to enhance the capacity.

1.4 AIMS

The aim of this thesis is to propose an improved image steganography scheme by increasing the security of the payload and capacity of the stego image while maintaining high imperceptibility.

1.5 OBJECTIVES

The primary goal of this work is to conceal the secret message in an image using a new embedding method. By using the aforementioned research gaps the following objectives are set:

i. To develop a new steganography system that hides a secret text in the image with high degree of security.

ii. To propose a new embedding method for hiding information in the image based on Pixels Disparity Value (CLV) and to increase the capacity while maintaining the imperceptibility.

iii. To increase the security of embedded message in the hosting image using Henon map function to increase the randomization of method.

1.6 SCOPE OF THE THESIS

i. Proposed system can embed text files in a carrier image based on steganography scheme.

ii. The rotation, zooming, scaling is not considered in this study.

iii. This system is used Medical Image and Signal Processing (MEDISP) and SIPI which are standard dataset.

iv. Results are evaluated using PSNR, SSIM.

1.7 SIGNIFICANCE OF THE STUDY

Presently, many fields such as military, medical, and industry used applications based on security. Therefore, the proposed system will try to help to increase the robustness of such applications. In the proposed method, we hope to get encouraging results in the steganography system in both important factors (capacity and security).

1.8 THESIS ORGANIZATION

In this proposal five chapters organized as the introductory for the first Chapter and follow with Chapter 2, that shows the hiding data techniques generally, then principles with classification of steganography systems. Some weaknesses with advantage of existing methods introduced. Full methodology of proposed method with detail framework explained in Chapter 3. Experimental results with evaluation explained in Chapter 4. Finally, the conclusion and future work has been introduced in chapter 5.

2. LITERATURE REVIEW

2.1 INTRODUCTION

This chapter will provide an overview of the existing method in literature which identifies questions for this proposal with a set of objectives. Steganography known as the art or science of hiding data within the communication channels. In steganography secret content is embedded in certain media that unremarkable hosting images, in a way that no one can recognize there is a secret inside it. Before discovering steganography, invisible ink is used during transmission or some time tattoo for conveying secret data. Due to modern technology and network development, transferring secret data over the network becomes very easy when using hosting media. More effort spent in terms of media communication to hide messages inside the media in a way of not detectable and not seen by an intruder [10]. Steganography consists of two parts "Stegos" that mean "cover" in Greek word and the second part is "grafia" which mean "writing" the whole word defined as "covered writing", for this reason, can say steganography is derived from Greek [11].

2.2 INFORMATION HIDING HISTORY

Information hiding idea is older than the idea of communication and network. Which is consisting of two general terms: first steganography that considered in this proposal and the second concept is watermarking. Steganography itself was very messy, firstly before using transportation like mail, phones, and horses the message was delivered on foot. Thus hiding the message must have two choices first memorized by messenger or else hidden by messenger.

During World War II invisible ink widely used but the extraction was a different method and not easy. Ultraviolet light used to read the invisible ink latterly by using ant counterfeit devices. Monk Johannes Trithemius used cryptography of modern founder, this considered the as the first attempt to conceal secret data in the text [12]. Trithemius scheme used to hide data through invocations name of angles, for stranger secret message present as a pattern of character during the text. Consider this example:

(Padiel-aporsy-mesarpon-omeuas-peludyn-malpreaxo)

Can extract the word (Prymus-apex.)

German during World War used a special technique null cipher which considered as an unencrypted message for hiding secret information. Using this technique appeared very innocent outside. Steganography developed rapidly due to the fast progress in internet and communication development. One of the objectives of such a proposal is to keep the pace of development in this area and hide secret messages within a robust system.

2.3 STEGANOGRAPHY

Steganography can define as the smart way to hide secret information within trusted media to host it in a method that does not make any doubt by an intruder or detect it while hidden in the image. Steganography and cryptography in the same domain are keeping the secret message protected inside the media. In the same context using both or one of them or sometimes one complete another also the performance will be good. For better security sometimes we use both of them to achieve better results.

Nowadays using of steganography can host data in many different formats these formats including .doc (text), .bmp (image), .mp3 (audio), or .wav (video). For this reason, steganography is very important when developing and using the internet when considering security and privacy. Due to the rules applied by the government and some limitations that deal with cryptosystems make some weaknesses in internet communication when using such an algorithm. In the steganography system, there are two parts sharing a certain message and when the sender sending the message only the receiver can catch it via using the stego key to reveal.

General classification for data security can be shown in Figure 2.1 in detail. This classification actually suggested by this classification considered the best one due to cover all domain and class in steganography system.

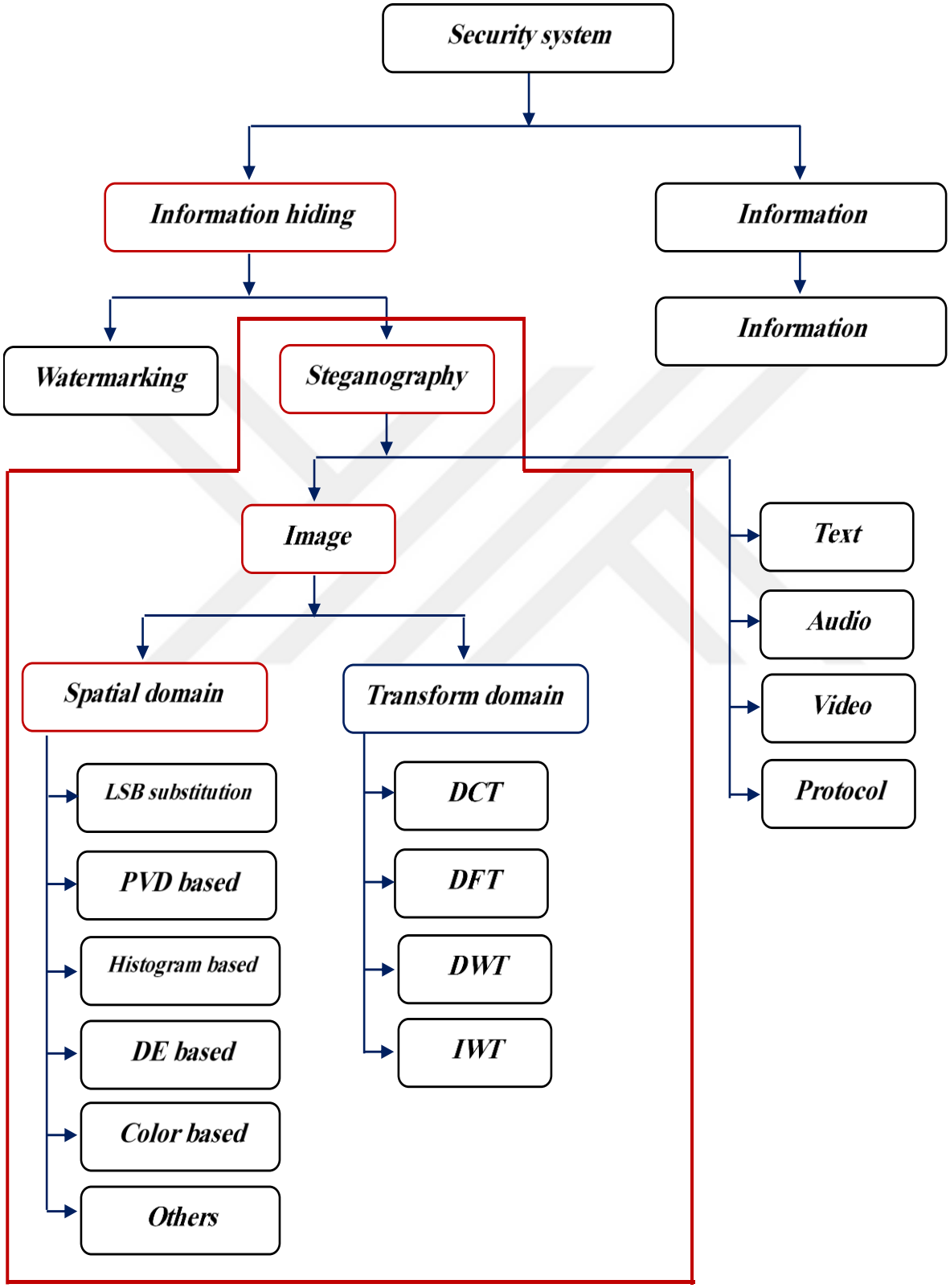


Figure 2.1: Classification of Security System.

2.4 METHODS OF EMBEDDING

- **Spatial or map domain**

Pixels intensity used here to insert or embed the secret message. This type or class has many advantages for embedding, like increase the capacity (no limitation), reduce the complexity, therefore imperceptibility of hiding message. Disadvantage of this class is lacking in techniques of statistical analysis.

- **Frequency domain**

In this regard given image will change or transformed into frequency class (domain) then embedding the secret message will be in the coefficient's factors. The benefits of using frequency domain is robustness against statistical attacks but in other hand suffer from very low capacity.

In literature spatial domain is widely used because of it is simple and give more efficiency [2]. Later, we will explain in details examples for both frequency and special domain.

2.4.1 LSB Method for Substitution

In steganography system most of the methods used substitution of LSB techniques for secret message embedding. [4] proposed a new system using substitution of LSB for message embedding of "Optimal Pixels Adjustment Process" OPAP. This approach utilized to enhance the image quality of stego image. Four LSB bits changed in this method used to hiding the information. The PSNR achieved was 51 dB. In 2018 [13] suggested method based on adaptive LSB substitution steganography technique, in this method image aim to divided into two segments non-sensitive and sensitive place based on texture analysis. With non-sensitive area majority of bits used to hold secret message and other bits in sensitive area. Main advantages of this method are achieving high payload capacity and imperceptibility. [14] introduced new steganography LSB method for embedding secret message by normal LSB bit position in cover image. Inverting pixels before embedding is the main contribution in this method, high results reported in term of capacity and PSNR. Foe existing method reported that methods based on LSB are easy just by changing the LSB bits of the pixels but the problem with lacking of capacity. One of the most interesting methods

which is based on LSB, and when matching bits then replacing just in case of different. Embedding here behave differently by embed 0,1 or -1 to the LSB pixels of cover image.

2.4.2 Differencing of Pixel Value (PVD)

By using this method high quality image is introduced as stego image, the payload capacity increased by this method to hide the data. Embedding in this method took place in edge of smooth areas where the pixels with neighbours got high different intensity. Any change in smooth area of the image will be noticeable by human eye so in this method smooth area neglected, while most of embedding will be in edge area where the intensity of pixel got big different and called less sensitive area. Target pixel that needs to embed should check its surrounding pixels to ensure the suitable position of pixel in the image.

Neighbour surrounding pixel can be found by up p(x,y-1), down p(x,y+1), right p(x+1,y) and left p(x-1,y) pixels. For the given target pixel p(x,y). The main advantage of this method is high capacity with better image quality due to changing of pixels not arbitrary but arranged. In addition to increasing the security because of embedding is not sequential and depends on pixels intensity calculation, and

Adaptive steganography system suggested by [9] using special embedding method to achieve PSNR around 34 dB, but it was not encouraging score and imperceptibility as well. Steganography system based on PVD method of embedding secret message proposed by [16] and achieved high PSNR value with reasonable imperceptibility. Introduced steganography depends on pixels indicator using improving of RGB image technique as cover image. to handle the channel two LSBs used to refers to the next two pixels. This method opens the ideas for developer to mix between it and any combination of RGB to increase the security of the system at the expense of capacity.

Method based on edge detection that is similar to PVD proposed by [17] , difference of 8-neighbours method used for embedding secret message. Fuzzy of canny filter to detect edge considered to specify the place of embedding. This method improved the quality of the image (imperceptibility).

2.4.3 Based Method of Histogram

This method used the histogram of the image in order to hide secret messages. In this method reasonable PSNR achieved around 35 dB for embedding secret message of 190000 bits. After embedding stego image will send into other side then extracting will be easy by reconstruct the image without any little mistake. Good PSNR achieved by [19] which considered two dimensional histograms to embed the data and modifying it. The method has a limitation in the payload capacity.

2.4.4 Difference Expansion (DE) Method

To solve and enhance the problem reversible difference of expansion method this method is used. One-layer embedding represented by location used to solve the embedding method in cover image.

A new DE embedding method suggested by [20] to solve the problem erased by simplified location and interpolation. Good stego image produced when bilinear interpolation used for embedding inside the image. The imperceptibility achieved considers good but the capacity is very good.

New prediction method suggested by [21] used to reversible secret message embedding, partial difference equation PDE used to predict the error expansion of cover image. In original image four pixels in different direction with their gradient then for next step weight calculated from the magnitude every iteration gives good prediction. This method better than other for the pixel's selection used to embed secret message.

.

2.4.5 DFT Steganography Domain

The Discrete Fourier Transform (DFT)-based steganography is used when one deals with the intensity estimates of the pixels in the cover image (implying the frequency components). Let, $F(x, y)$ represents the original image with size M × N, the DFT of this image can be written as

$$F(u,v)=\frac{1}{\sqrt{MN}}\sum_{X=0}^{M-1}\sum_{Y=0}^{N-1} f(x,y)\, e^{-j2\pi(\frac{ux}{M}+\frac{vx}{N})} \quad (2.4)$$

Where u is ranged between 0 and M-1 and v is ranged between 0 and N-1.When transforming the image after embedding the original image must be reconstructed, and this process is done by

Inverse Discrete Fourier Transform (IDFT) which retrieves the pixels value from transformed image. Simple steps represent the DFT algorithm: first, take the cover image (C) and read Secret data (S); second, apply DFT to the cover image (C); third, split the Real part from given coefficients DFT; fourth, secret embedding bits to the Real space of the DFT ; fifth, Inverse DFT to get stego image (C') as illustrated in Figure 2.2.

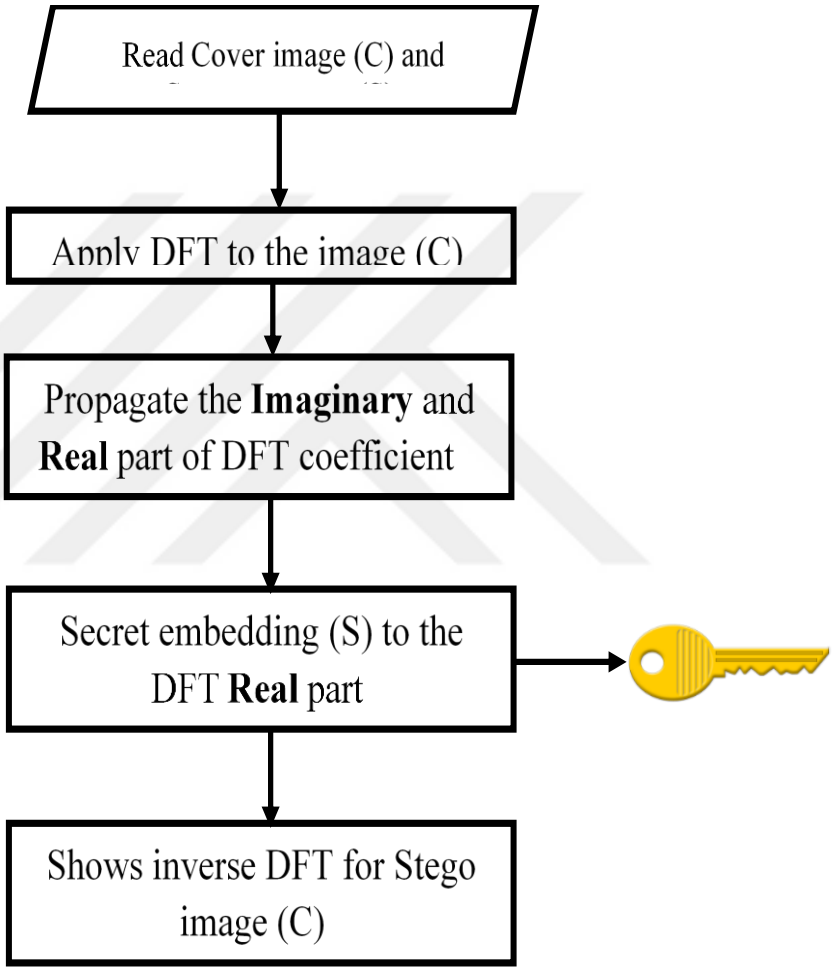


Figure 2.2: Embedding method based on DFT.

For extraction just invert the procedure of embedding from the bottom up. New embedding method using DFT was proposed by [24] and with this method 2 × 2 block division was used for sliding windows manner. Then DFT was applied for each block of the cover image considering coefficient, and the embedding procedure is done within real part of DFT. Reported results shows improvement of security and robustness.[25]introduced different method of DFT based on Weight Fractional Fourier Transform (WFRFT) instead of using normal DFT. Block size 2 × 2 was used

for Fourier transform. Two LSB were used for embedding the secret message, with the embedding occurring in the real part. For this method payload capacity improved.

2.4.6 DCT Steganography Domain

Two Dimensional 2D- Discrete Cosine Transform DCT used in steganography system and given Discrete Cosine Transform can be defined as:

$$B_{p,q} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \cdot \sum_{n=0}^{N-1} A_{m,n} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (2.7)$$

when $A_{m,n}$ is represented the image of size M x N and $B_{p,q}$ represent coefficient transform.
To inverse 2D-DCT which is needed in extracting process given by:

$$A_{m,n} = \sum_{m=0}^{M-1} \cdot \sum_{n=0}^{N-1} \cdot \alpha_p \alpha_q B_{p,q} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (2.8)$$

2D-DCT procedures or steps will be followed as : step 1, partitioning of cover image into sub-image (8 × 8) blocks assigned as (B_i) where *i*considered as the i^{th} of blocks. Step 2, apply 2D_DCT in each block or sub-image to find the coefficients of DCT (in this case will get one DC for each block and 63 of AC). Step 3, use the (u1,v1) with (u2,v2) to generate stego key. Step 4, read (m_i) as a secret bits of i^{th} bits. Step 5, to get original sub-image or block invert DCT will apply. Step 6, repeat the above steps for all blocks to find stego image.

In receiver side (extracting process) follow the same steps in embedding secret message but in reverse order. Many researchers applied and modified the DCT algorithm to find the goals of steganography system.

New method suggested by [26]. That depends on reversible data embedded using partitioning of cover image into two sections low and high frequency of components. The embedding will be in high frequency section because of low frequency is more sensitive for any change. Integer mapping used to implement the 2D-DCT. During shifting the histogram we looking for appropriate location this consider better position for embedding. Procedure of shifting occurs in both side right and left and continues until find empty space that is used for embedding. This method has been achieved capacity of 170992 bits to results PSNR around 36.80 dB. Superior improvement achieved by DCT method when comparing with other methods.

In 2018 [26] introduced a method that consist of combination between DCT steganography and affine transformation and reported good results due to integer of DCT steganography is less loss invertible. Spreading of Laplacian-shape used in transforming integer DCT. For any statistical attacks this method considers more robust than others. Integer Wavelet Transform IWT with DCT steganography is a method suggested by [27]. Two steps used for embedding, DCT for secret message preparation and IWT for image preparation. Then Munker's assignment algorithm carried out the thecomplet embedding in this method.

2.5 STEGANOGRAPHY STRUCTURE

In order to build any image steganography method, the different requirement must be considered:

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

Secret message (M) will store in cover image (C) in embedding process this consider function (Fe) one and all the information stored in stego key (K), in other hand function to extract secret message from hosted image (S) in receiver side as shown in Figure 2.3.

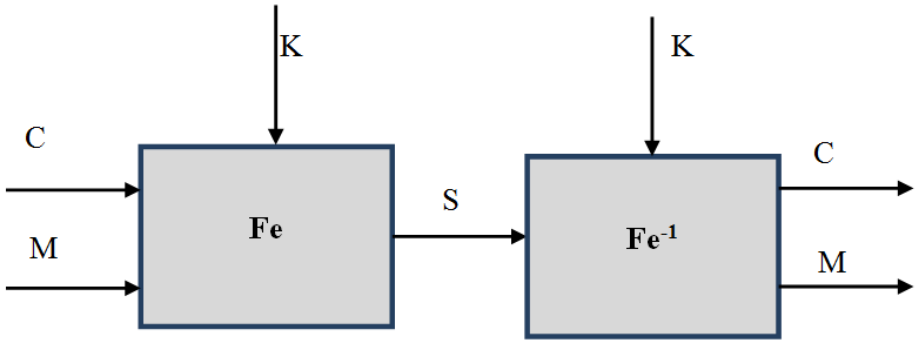


Figure 2.3: Steganography structure.

2.6 APPLICATIONS OF STEGANOGRAPHY

In image steganography domain many kinds of application each based on their contributions, like protection of copyrighting, feature tagging and security of communication [28],[29]. Embedding in

both copyright and watermarking happen inside special area of image like intellectual property. For this reason using of the image become easy without permission via proving from the author.

Modern stamping will be intelligent that involved inside an image and other types of security as well, such as tagging, captions and elements of descriptive. During copy or transfer the image (stego image) the properties of the image still attached through transforming. Stego key implicit or explicit also keep the information regarding embedding inside it during copying [30] due to all the secret data not including the communication by steganography. Anyway double checking is necessary before embedding to avoid hacking the system.

2.7 STEGANALYSIS

Steganalysis is considered as the same age with steganography itself. Same steganography consists of many techniques during developing it and the developer can assess the progress within its techniques. It is necessary when revealing the information from an image so can browse the stat of the art in this context as follows:

1. **Visual attack**

It is the main concept in steganalysis and considers the basic form in the world of digital image. Here, image will be reduced into single bit plane that is the first bit in LSB and more effective. To discover any change in an image can notice and investigate within human eyes to recognize any different pattern in the image [2]. Observing the colour change is another approach, while some algorithms get weak to handle the colour during embedding process. Also, identical results provided by many researchers that using steganographic tools when using original files. In order of considering this procedure is the basic technique and simple but still facing two problems issue with detection [31]. First issue is the variable sensitivity with vision of the human within observer. eg: classification for different condition [32]. Second issue is not suitable for large image volume or hug data [33].

2. Structural attack

In computer information world there is special structure as internal such as body, header; pointer and so on. This is known file format. Each document has specific data raw, format, or specific structure. This informationmakes their data structure. Different structure can be represented by same information it is possible also, in a way without changing of its format. Like when two person sings same song but in different way. In this way the structure of the song still the same but handling or processing it in different manner [34] So steganographic algorithms always deal with characteristics of data structure. And this method commonly used in steganogram classification.

3. Statistical attack

This kind of attack can test the image and reveal if there is some modification occurs by steganography. Due to this kind based on statistical prosperities of an image if become up normal. Statistical attack normally tests the entropy of the redundant data in the image and it's independent from the format of the data. In this context the image of hidden data inside it has higher entropy than the other images [35]. Some existing researches observed that hiding data encrypted to the image with GIF format will affect the colour frequencies and reflected by histogram of the image [36]. Because of encrypted data its 1 and 0 most of the time are equally. LSB is critical to change when some data embedded specially in colours image rather than greyscale image. So the difference in embedding with colour frequency in the second and third byte lead to reduce the data embedded not like first byte of colour image.

In JPEG images same talking is true. It will be use DCT of cosine transform coefficient to analyse the frequency. Embedding this time is with the pixels of high frequency value to avoid this kind of attack.

2.8 HUFFMAN CODDING

Huffman coding is a particular kind of prefix code always used in lossless data compression. David A. Huffman developed an algorithm when he was a PhD student at MIT, and published a paper in 1952 known as "A Method of the Construction of Minimum-Redundancy Codes" [37].

Output of Huffman algorithm is a variable and a table consisting of symbols and characters. The frequency of character weights are calculated with probability of source symbol. The general algorithm can be described as:

Input: Alphabet $A = \{a_1, a_2, \dots, a_n\}$ which represents alphabet symbols with size *n*.

Set $W = \{w_1, w_2, \dots, w_n\}$ which represents positive symbol weight such as $w_i = weight\ (a_i),\ 1 \leq i \leq n$.

Output: Code $C(A, W) = (c_1, c_2, \dots, c_n)$ which are the binary codewords such as c_i is the code words of $a_{i,}$ $1 \leq i \leq n$.

The main **goal** is

Let $L(C) = \sum_{i=1}^{n} w_i \times length\ (c_i)$ is the length of code *C* with the condition that *L(C)* <*L(T)* for any code *T(A,W)*.

In literature, many studies used Huffman coding in steganography with LSB image in order to provide high payload capacity and to divide the secret code into three main groups for encoding [38]. Compressing the secret message before embedding increases the capacity and security and different methods used this condition when designing steganography. Lossy image embedding with lossless Huffman coding was used in [11] to increase the robustness of the system against histogram and statistical attacks. This method with novel Coefficients was used to increase robustness as shown in the schema in Figure 2.4.

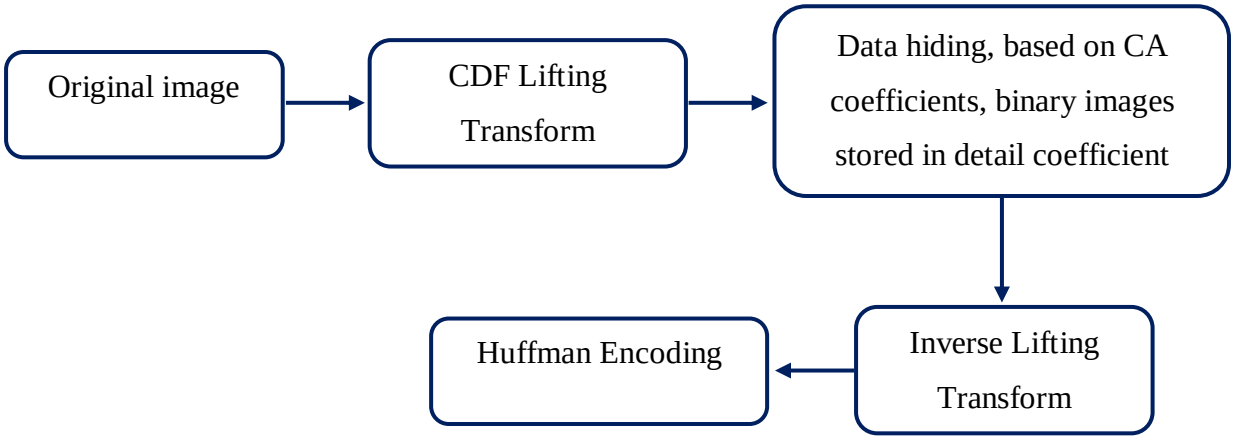


Figure 2.4: Steganography and Huffman compression.

Huffman coding was used to increase capacity and PSNR in [39] . This method applied Canny filter to find the edge and smooth area in image, then selects the pixel through this area for embedding. The method of 2^k correction was used to get better imperceptibility with stego image.

When using mobile health care by compressing the loss data over the TCP/IP protocols, after removing the noise data was compressed and extracted to be decoded in order to obtain the final dataachieved better results in terms of compression [40]. Huffman is used in many fields and combining steganography with cryptography is common [41]. Probability or frequency of the symbol code is considered when designing a steganography system to increase the compression of the secret data embedded in addition to compression image format JPEG for more efficiency [42]. In general the term Huffman is a synonym for the word payload capacity in steganography system, and many methods have been suggested in literature [43]. Huffman is usedto compress the secret message but impossible to use for compression of the image itself as it may affect the hidden data inside it, limiting the process to only secret data streams as shown in Figure 2.5.

We can conclude that Huffman coding algorithm is helpful in steganography system to increase payload capacity and when applied to the secret message before embedding [44]. At the same time the system is made more robustness against histogram and statistic attack. Embedding method or selection pixels will be discussed later.

2.9 DATASET

The USC-SIPI dataset that contained the digitized images was used by the proposed work in order to train the system. The purpose of selecting this dataset is to support the studies in image processing, analysis of image, and vision analysis [45]. The first version of the USC-SIPI dataset was released in 1977 since that time many images have been added into this dataset to make it versatile [46]. This dataset is already classified into volumes depending on the basic character of its image. The Lena, Tiffany, Baboon, and Peppers were the images used in the proposed research for color images as seen in Figure 2.5. In addition, these images were used to benchmark the experimental result with existing one for the evaluation.

Figure 2.5: The standard SIPI dataset used in the proposed framework.

The proposed method performance was tested using different medical images taken from a famous widely used dataset for CT images from [47] and MRI images from computer vision tested images [48]. Medical images contain huge information inside and the specialist doctors can explain it, some time for the special purposes the doctor must hide some information even from other specialist people. In this case, our system plays an important role to do that, and conceal all the required information inside the image and can extract easily if have the stego key. Image normally comes from a scanner device some time become as the 2D or 3D image. Figure 2.6 shows the scanner device, the proposed system deals with any type of image and any formats. Figure 2.7 is shown all medical images used for testing the system.

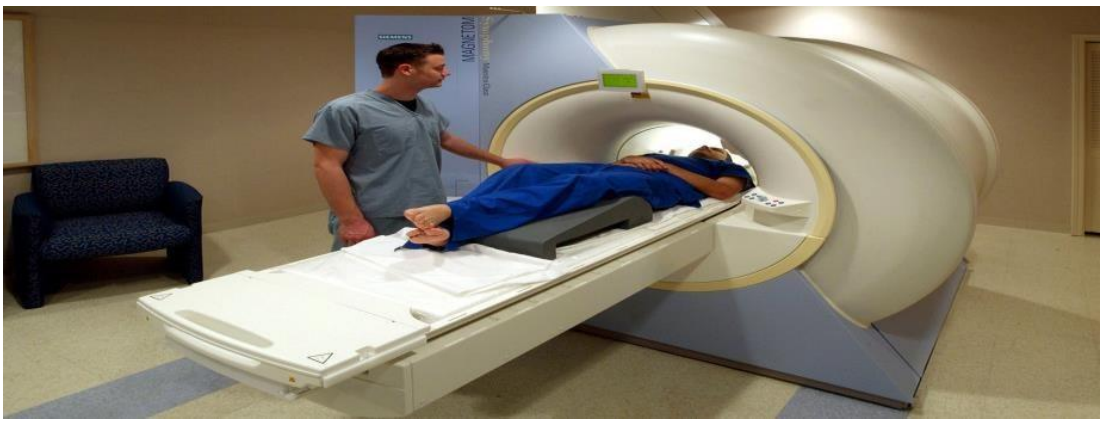


Figure 2.6: MRI scanner.

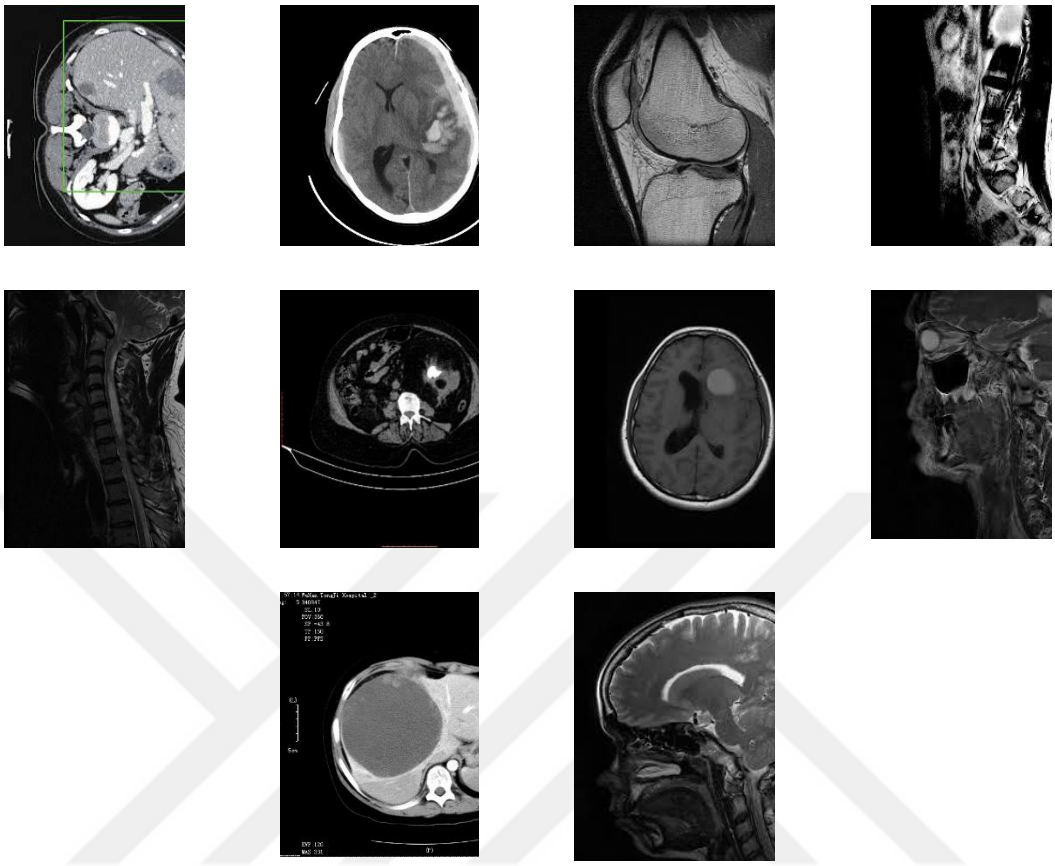


Figure 2.7: Medical images used in the system performance evaluation.

2.10 RELATED METHODS OF IMAGE STEGANOGRAPHY

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 image steganography frameworks are presented. As mentioned earlier, the digital image steganography systems have been divided into a spatial, frequency and adaptive domains. Several recent studies related to the steganography in terms of the capacity and the corresponding PSNR are listed in Table 2.1 (between the years 2015 to 2020). These include the works by [14], [19], [28], [29], [30], [22], [32], [22], [4], [8], [33], [34], [36], [38], [41], [42], [44], [25], [45], [46], [47], [24], [48] and [49].

Table 2.1: Overview of the state-of-the-art works reported in the recent literature (between the years 2015-2020)

Domain	References	Method	Remarks	Performance
Spatial Domain	[25]	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
	[26]	MF-PVD:	-Weak against statistical steganalysis. -Low embedding capacity	36 dB 1.03 BPP
	[27]	LSB - MLEA: Multi-level encryption applied on stego-key as well as secret data.	-Limited embedding capacity (EC). -Limited robustness.	> 45dB 1BPP
	[28]	PVD-TPVD:	-Lack of security -Weak against statistical attacks	38.33 dB 2.14 BPP

Table 2.1: Overview of the state-of-the-art works reported in the recent literature (between the years 2015-2020)(Continued)

Domain	References	Method	Remarks	Performance
Spatial Domain	[30]	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) attacks	40 dB 5.0 BPP (High EP)
	[22]	PVD: Adjusting the Tri-way PVD by finding the best value of each pixel pairs where their difference afford 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
	[32]	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
	[22]	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 2.1: Overview of the state-of-the-art works reported in the recent literature (between the years 2015-2020)(Continued)

Domain	References	Method	Remarks	Performance
Spatial Domain	(Swain, 2018)	PVD: PVD method with 1×2 pixel blocks in overlapped fashion	-Less visual quality -Lack of Security	42.96 dB 2.96 BPP
	[8]	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
	[33]	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
	[34]	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 1.0 BPP

Table 2.1: Overview of the state-of-the-art works reported in the recent literature (between the years 2015-2020)(Continued)

Domain	References	Method	Remarks	Performance
Frequency Domain	[36]	Wavelet coefficients and RC4 encryption	-Low embedding capacity	65.9 dB 0.5 BPP
	[38]	DCT: Two parallel methods (2D-DCT with RSA) and (2D-DCT with chaotic) are suggested. Before embedded into DCT coefficient, of the given original image, Duffing map the secret image is applied for encrypting into a set of uniform pixels	-Low embedding capacity -Low visual quality -Unsatisfied robustness against geometric and compression attacks	0.5 BPP 25 dB
	[41]	DCT: The proposed study used two methods for embedding DCT domain subbands and chaotic map. The modifications of the elements in the high-frequency sub-image will not result in considerable changes in the perceptibility. The DCT method applied on the given cover image and scans the high-frequency coefficients in a zigzag technique, then embedding positions are decided using a chaotic function	-Low visual quality -Unsatisfied robustness against geometric and compression attacks -Low embedding capacity	0.5 BPP 30dB
	[42]	DWT: A DWT domain-based image steganographic system is processed. Using three details coefficient (horizontal, vertical, and diagonal) for embedding the secret bits. Using a secret key computation to reduce the distortion in the stego image. Also, a blocking concept is used to save the imperceptibility of the cover image. The embedding process using a matching block between the original and stego image	- Unsatisfied image visual quality	2 BPP 45 dB

Table 2.1: Overview of the state-of-the-art works reported in the recent literature (between the years 2015-2020)(Continued)

Domain	References	Method	Remarks	Performance
Adaptive Domain	[44]	LSB-ANN: The presented scheme used LSB based ANN and chaotic edge. Firstly, using ANN for finding the edge of the original image then-secret data embedded randomly based key chaotic system.	-Limited EP in the edge region. _ The researchers didn't test the presented scheme against different attacks.	54.5 dB 2.0 BPP

	[25]	Edges based fuzzy method: The presented scheme used a dynamic fuzzifier for the segment of the cover image and secret bits.	-The researchers didn't address the embedding capacity.	46.8 dB N/A
	[45]	LWT with ANN: -The cover image is decomposed into three-level LWT, then it is randomized in 2 ×2 non-overlapping blocks. Binary data are encrypted ,and then embedded on the LWT coefficient component.	-Lack of robustness against compression and rotation - Very low payload capacity	43.8 dB 512 bits
	[46]	Genetic Algorithm (GA): Modified GA approach with frequency domain techniques for QR embedding.	-Low security -The researchers did evaluate their proposed system with NCC or SSIM. Also, HVS, Chi-square attacks were missing	50.29 dB 1.0 BPP

T **Table 2.1:** Overview of the state-of-the-art works reported in the recent literature (between the years 2015-2020)(Continued)

Domain	References	Method	Remarks	Performance
Adaptive Domain	[47]	GA: GA based fragmentation of 8-bit binary stream of each color component (R,G and B) to 4-bit and applying (GA) to increase the robustness of the presented scheme.		38.27 dB 2.0 BPP
	[24]	Adaptive QW: The presented system used inverse wavelet transform along and Genetic algorithm (GA).	-Lack of security -Lack robustness against filtering and scaling. - Chi-Square, HVS attacks were missing.	46 dB 1.0 BPP
	[48]	Edge-based image: The proposed approach used an adaptive embedding process over the Dual-Tree (DT-CWT) subband coefficients with machine learning-based optimization techniques.	- The researchers did evaluate their proposed system with NCC or SSIM. Also, HVS attack was missing.	53.71 dB 1.9 BPP
	[49]	Content adaptive steganography: The method is divided into 3 sequential processes: image segmentation (IS), pixel complexity identification (PCI).	- The researchers did not mention how strong the proposed method was against the statistical attacks?	50.98 dB BPP

2.11 DISCUSSION

Of late, the steganography has emerged as a significant system in the research and development of the data security in WWW in its own right. Over the years, numerous methods have been suggested to address the issues of the steganography where diverse embedding procedures were invoked. The exponential growth of the information technology in the past decades and the related attacks by the intruders enforced the computer scientists and engineers to develop smarter and smarter algorithm for concealing the sensitive and private information freely flown over the internet. In this regard, the state-of-the-art works in the literatures are overviewed comprehensively. Some explanations on the most versatile embedding techniques related to the LSB and DWT descriptor are emphasized. In the current study, several studies have been reviewed that rely on various methods of embedding (especially between the years 2014-2020). These methods have been used for preparing the secret message setup. These techniques include the edge detection, LSB substitution, and DWT. The existing literatures are critically reviewed on the strength of the proposed idea was also conducted. This chapter is expected to provide enough evidences towards the correct selection of the research gaps, research questions, and the proposed objectives of the study.

3. IMAGE STEGANOGRAPHY SCHEME

3.1 INTRODUCTION

This chapter explains the details of the research methodologies that are implemented to accomplish the cited objectives of this study in the context of the proposed steganography scheme. The preparation of the cover image for embedding and managing the blocks as well as pixels are presented. In addition, two significant approaches are explored namely the random function that is responsible for the distribution of the main image into blocks and then the allocations of these blocks into sub-blocks. The randomness that played a vital role to enhance the security of the proposed scheme is also underscored. The compatibility of the selecting blocks with the system and the impact of the embedding on the system security are emphasized.

The security of the proposed steganography scheme was attained and maintained using three important procedures. First, the splitting decomposition process that enabled to increase the robustness and security of the scheme. Second, enhanced Huffman coding that will be used to increase the system capacity, thus contributing to the enhanced security. To get a deep understanding of the proposed steganography scheme, several images were illustrated. The complexity of developing a robust image steganography scheme for information hiding in the field of communication and security system is undoubtedly challenging. Many methods have been proposed in the software and communication fields. Due to the rapid progress of the WWW and communication media such as the video, audio and image the requirement of more secure and robust data hiding system became mandatory. In is needless to mention that in recent times the information hiding system generated renewed interests especially in terms of image processing and communication via the internet.

The new embedding method was proposed to improve the high level of security and imperceptibility of the system while maintaining the robustness. Distribution of the secret message embedded to the cover image reflected the PSNR value. The PSNR detected the frequency of the bits within the cover image especially with the proposed Pixels Disparity Value (CLV) and distribution. When the bits became heterogeneous (more chaotic) then the PSNR received high value, indicating the selection of the CLV. High PSNR value reflected a good image quality [33] and thus all the previous methods tred to increase the PSNR value of the

proposed data concealing system. In the present research, two important factors were considered. First, the embedment of the secret message was performed using the new method. Second, the capacity of the payload amount embedded in one cover image was enhanced. Actually, these two factors were very important because the robustness of all steganography systems is characterized by these two factors. Thus, the researchers in the past tried to get the best performance in embedding method and capacity. The security and capacity are opposite to each other wherein the security decreases with increasing amount of data embedment and vice versa. It is customary to discuss briefly the structure of the entire scheme used in this study.

3.2 THE PROPOSED SCHEME

The proposed method has three main stages (data preprocessing, embedding, and extracting processes), while the literature review and evaluation stages are used to review the previous studies problem and evaluate the proposed method respectively. The proposed method was evaluated using the statistical and non-stractural criteria which explained in Chapter 4. Figure 3.1 explains in detail the entire scheme steps through which the final structure of the proposed scheme was obtained which resisted all the common attacks used in the image steganography systems, as well as achieving the required results that were compared with previous works that proved to be better than the state of art.

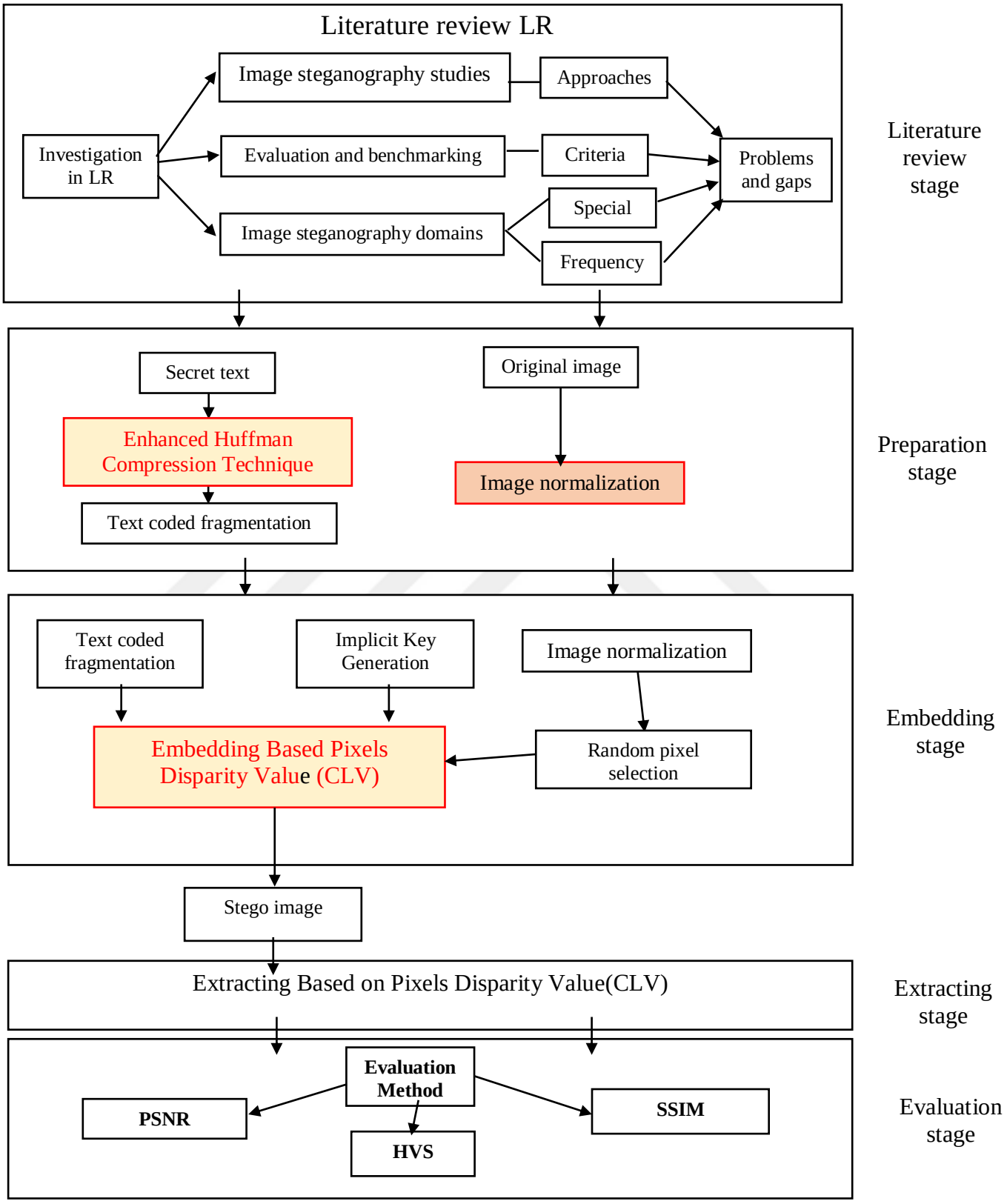


Figure 3.1: The Structure of proposed steganography scheme.

3.3 INVESTIGATION OF RECENT LITERATURES

In this stage, the literature review focuses on three parts. The first part investigates recent literature on image steganography methods whereby the most popular and important approaches are subsequently selected as references for this research. The second part investigates the different evaluation and benchmarking methods used in image steganography and how the evaluations (i.e., PSNR, Histogram analysis, HVS, Chi-square, and SSIM) are implemented. Benchmarking with authoritative studies is necessary to evaluate the performance of the proposed scheme. The third part of the literature investigations focuses on discovering and describing limitations pertinent to image steganography domains. This helps the authors to propose a suitable solution to resolve these limitations.

3.3.1 Image Steganography Studies

In image steganography literature, different methods and techniques have been proposed to embed secret messages in image steganography systems [44]. The review of literatures for this study is discussed in chapter two, which covers definition of image steganography, classifications, structures, techniques, applications, and comparison between cryptography and steganography systems. Scrutinising this information allow the authors to discover authoritative approaches and methods of this field. Subsequently, these approaches and methods are further scrutinised to discover gaps and problems related to image steganography.

3.3.2 Evaluation and Benchmarking

In the investigation of the literatures, development of data hiding is observed as targeting to either solve payload, quality, or security separately, and there is a lack of studies investigating the trade-off between them. From this observation, the authors concluded that a majority of researchers has only primarily focused on enhancing a single criterion, which makes the comparison of multi-criteria data hiding works with previous approaches challenging or almost impossible [32]. Therefore, studying evaluation criteria is necessary to recognize the parameters that are used to evaluate a proposed work. This is because appropriate evaluations allow researchers to report on multiple issues that are pertinent to improving image steganography while highlighting the performance of the proposed scheme at the same time.

3.3.3 Image Steganography Domains

In literature, the steganography systems can be divided into two parts, depending on the embedding locations and image nature. Each type has its own advantages and limitations. The first type is known as a spatial or map domain. For this type, intensity pixel is utilized to insert or hidedata. On one hand, advantages of this type of secret message hiding include increasing hiding capacity, reducing hiding complexity, and improving message hiding imperceptibility [54]. On the other hand, the limitation of this type of message hiding is that it lacks in terms of security. For instance, when subjected to statistical analysis attacks, this type of steganography system will not perform favourably. Spatial domain is widely used and proposed by researchers using different methods due to simplicity in implementation while being highly efficient [34]. The second type of embedding of steganography systems is known as frequency or transform domain. In frequency domain, an image is initially altered or transformed into a frequency domain, followed by the hiding of the secret message in the factors of the coefficient. The benefit of using a frequency domain is that it yields a greater security than spatial domain when subjected to different statistical attacks. However, this causes the steganography system to suffer from a very low message hiding capacity and low imperceptibility.

3.4 SECRET TEXT PRE-PROCESSING

The pre-processing stage of the secret message was performed before the embedment which is vital for any digital steganography system. In the proposed scheme, the pre-processing of the secret message enables to add an extra level of the security on top of increasing the payload capacity of the hidden bits. In the previous studies, the researchers have used different payload capacities to be hidden in a digital image [46]. Consequently, the hidden payload capacities were differed in terms of the pre-processing from one researcher to another. To overcome such limitation and to accomplish a good embedding capacity the Huffman algorithm was enhanced and applied to the secret message before the embedding wherein the use of such an algorithm allowed compressing the secret text more securely and efficiently. Finally, each stream was converted into a secret code via the Huffman dictionary. Accordingly, the results achieved after the compression process were the vector of the secret codes.

The aforementioned procedures are explained in Figure 3.2. It was necessary to keep the sequence of these processes to achieve the better results using the proposed steganography scheme. It is important to mention that any image steganography system have three salient features such as the storage of maximum payload in the image, good imperceptibility (visual quality of the image after embedding), and robustness (Shanthakumari and Malliga 2020). Thus, enhanced Huffman compression coding assured the attainment of these aspects by the proposed steganography scheme.

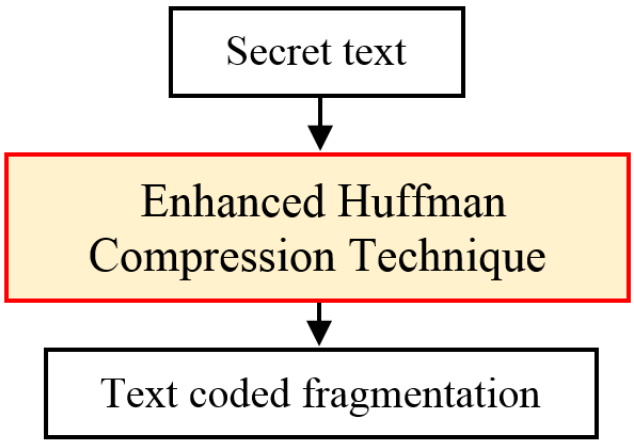


Figure 3.2: The secret text preparation in the proposed scheme.

3.4.1 Enhanced Huffman Compression Technique

The main aim of the Huffman coding algorithm is to reduce the size of the text before embedding to the image. Figure 3.3 illustrates the strategy for the text frequency (redundancy) reduction via the Huffman coding. In this process, the Huffman algorithm depends on the lowering of the frequent letters and offers them the priority code or short path in the Huffman tree.

Figure 3.3: The text frequency (redundancy) reduction within the Huffman coding.

The capacity is an important feature of any steganography to make the system more robust in which it is possible to hold a high amount of data inside a hosting image while maintaining the quality of image represented by PSNR. The concept of data management and transfer protocol

compression from the sender to the receiver was very advantageous beside other techniques used in this study. Figure 3.4 shows a simple flowchart of the Huffman coding implemented in the current steganography scheme.

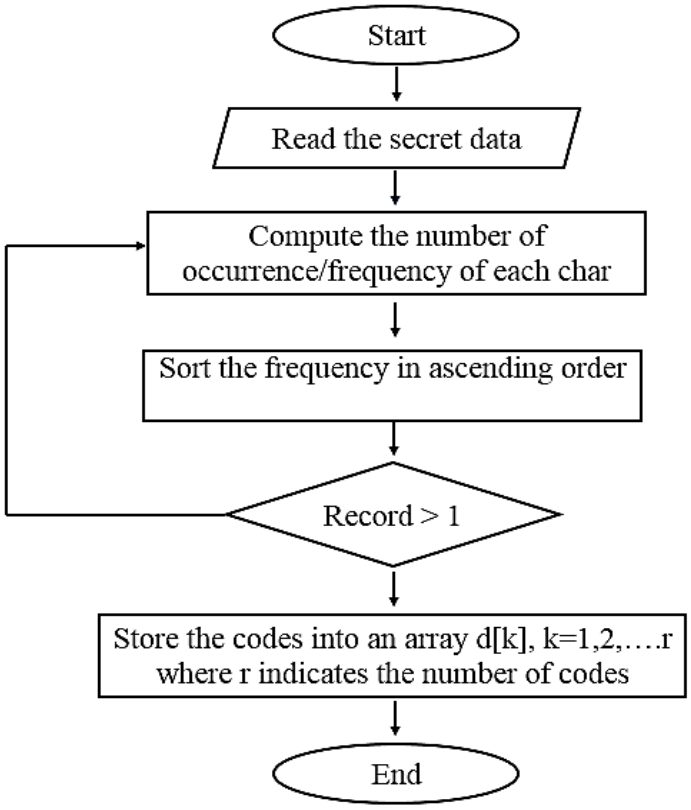


Figure 3.4: The flowchart of the Huffman coding showing its working principle.

For further illustrations of the Huffman coding and its working, a numerical example has been provided within the proposed scheme. This example used five different symbols that yielded:

Table 3.1: Simple example of using Huffman coding**.**

Symbol	S	T	E	G	O
Frequency	22	10	8	6	6

The process started with "G" and "O" for the low frequency to build the tree structure of the first branch followed by the "E" and "T" at the same level. These parent nodes had the frequency of 12 and 18, respectively. Each parent node accumulated the frequency of their children in the tree. For instance, the high frequency letter "S" was created in the high level to construct the final tree

which finally connected both children in one parent with the frequency 22. Figure 3.5 illustrates the typical Huffman coding tree structure.

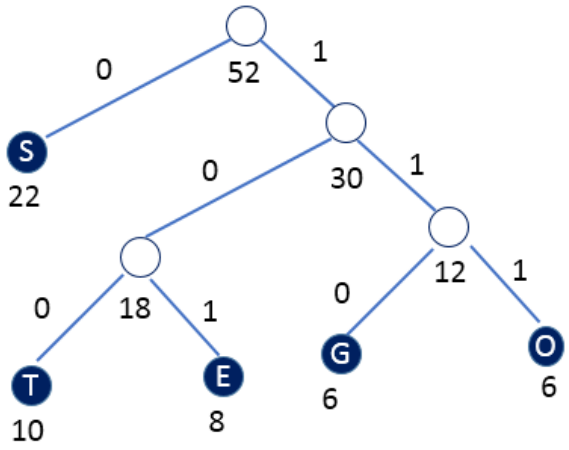


Figure 3.5: Huffman coding tree.

The frequency was reduced and the compression for this example removed the 41 % from the original text in case the same frequency of letters occurred as depicted below (Table 3.1).

Table 3.2: The letters frequency in Huffman coding.

Symbol	**S**	**T**	**E**	**G**	**O**
Frequency	22	10	8	6	6
Track code	0	100	101	110	111
Length	1	3	3	3	3

The high frequency in this case got less path of visiting to reduce it by going deep to the tree every time, thereby gaining many clocks in the digital word as 0 and 1. The procedures of the text compression in the Huffman coding for the proposed steganography scheme can be presented via Algorithm 3.1.

Algorithm 3.1 The Huffman Coding Algorithm

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= extractMin(Q)

j = extractMin(Q)

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

insert Node (T, $n + k$) with children i, j

insert Rear (Q,($n + k$, $f[n + k]$))

Return*T*

The secret message in the steganography system is always in the form of text. Thus, following the earlier literature reports the Huffman coding was chosen to enhance the payload capacity and significant compression ratio [50]. Three conditions was considered to attain better steganography system such as the maximum payload capacity, imperceptibility (visual quality of the image that includes the secret message), and robustness [51]. The Huffman coding was used to achieve the first condition. In the computer science, the Huffman coding is considered as the lossless data compression. This algorithm was basically based on the frequency of the letters (weight) and text file length or text stream. Thus, the length of the text stream was arranged to make the algorithm sufficient and to get more useful from applying the Huffman algorithm in

this system. The proper length or fragment of the text stream made the scheme more reliable and more robust. This fragment procedure is explained below.

3.4.2 Text coded Fragmentation

In the secret message preparation process, the bit stream must be fragmented. After the Huffman coding process, the produced text was converted into the digital form of 0 and 1. The processing of bits stream depended on the length of the data from the embedding stage. These bits were manipulated before embedding to ensure the scheme reliability. In other words, the sample taken from these bits stream was compatible with the process in the embedding stage. Cutting of a given text that represented the bit stream (sample) produced more effects. The data embedding to an image, especially when a down payment of bits was processed as one packet and separated from the original bit stream as illustrated in Figure 3.6.

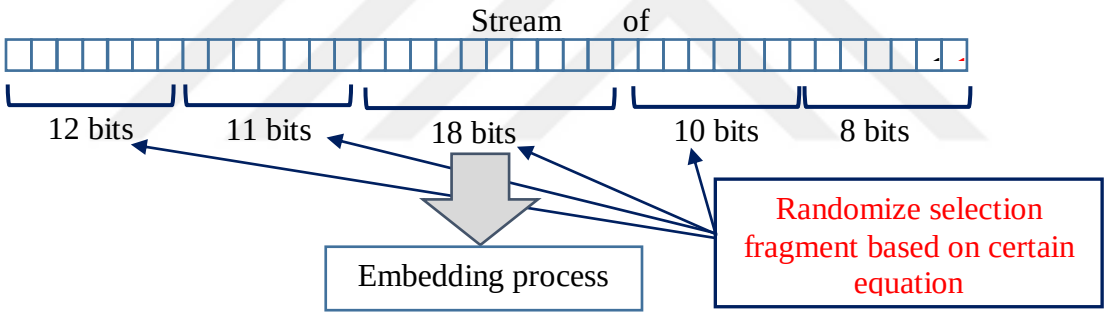


Figure 3.6: The bit stream fragmentation using the proposed method.

There are many advantages and disadvantages of choosing the long or short fragments. Short ones make the embedding and distribution over pixels easy but lead to low image imperceptibility. Conversely, the long fragments are difficult to embed but at the same time easy to get high PSNR (good imperceptibility). Thus, a compromise was necessary to get the optimum condition. To surmount this shortcoming, the best length was chosen experimentally based on the random equation for 6 iterations that was manipulated separately as a fixed sample. The interval part for separate parts became imaginary as the logic, not physical part. All the data collected was stored in the key that generated during the process as shown in Figure 3.7.

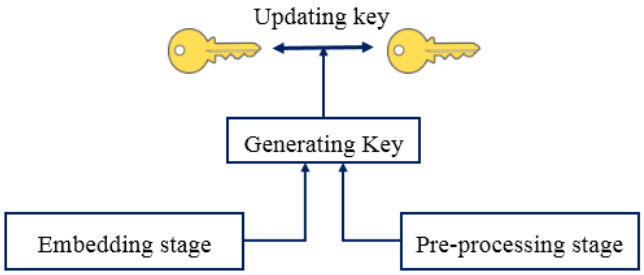


Figure 3.7: Generating the key in two stages.

The secret messages usually took the shapes such as the serial of 8 bits each and reflected the decimal number. Every action taken by these processes achieved two objectives which were capacity and security as needed by the steganography system. The main objectives in this stage (secret text pre-processing) were capacity and security improvement. Thus, the Huffman codingalgorithm was used to attain the optimum capacity precisely.

The binary tree code was issued and each path was found according to the frequency of the letters included in this word. The Huffman technique is the best text compression technique compared to many others [52]. The use of Huffman with the text was like the probabilities of symbols that were arranged in although each character was coded with a different decreasing order. In addition, the lower probabilities were merged a number of bits, where the receiver automatically got it and this step is continued until only two probabilities determined the character whatever their order. Regarding the high compressing ability and more security for the text it was useful to compress the secret message so that this procedure could increase the capacity of message data and made it more robust. This technique allowed reducing the size of large secret messages for embedding the large amount of data in one cover image. This was very important in terms of the data management and transfer protocol [53].

To clarify this process further a numerical example is provided below. Let the text be: THIS IS A CAR, Figure 3.8.

Step1: Construction of the Figure 3.8 (1) that contained individual letters and their frequencies.

Step2: Sorting of the letters in ascending order with regard to their frequency field (Figure 3.8 (2)).

Step 3: Addition of the first two and then re-arrangement of the table again as in Figure 3.8(3).

Step 4: Repeating the step 3 until a single record was achieved.

Step 5: Construction of the Huffman Tree and then coding every two branches (0,1) for all the branches of the tree. The construction of the tables in Figure 3.8 was performed in terms of the trees. The circled numbers were the number of occurrences of each character in Figure 3.9.

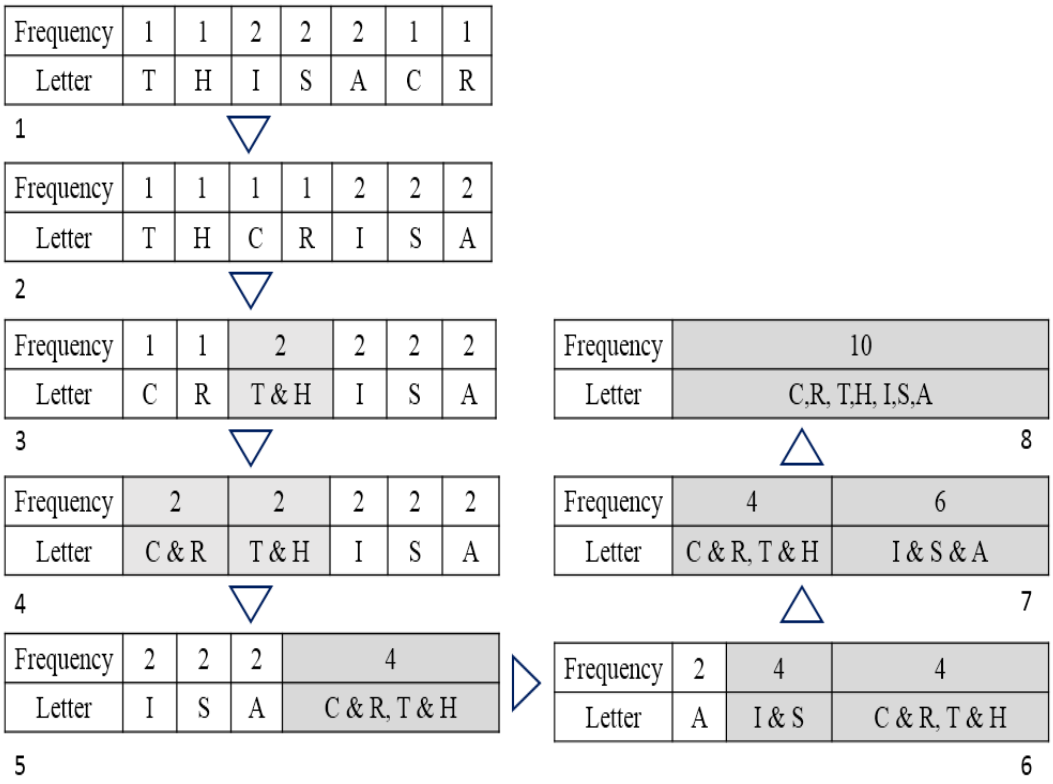


Figure 3.8: The Huffman tables algorithm.

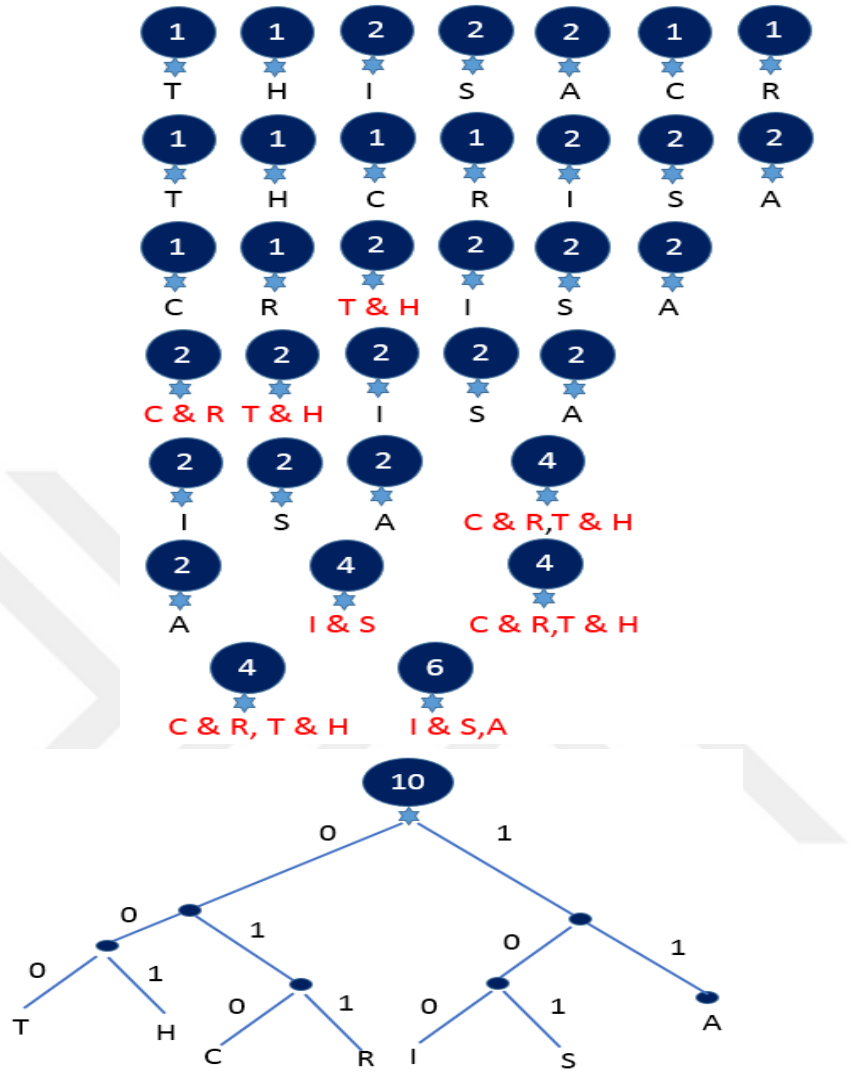


Figure 3.9: The Huffman tree according to the tables of algorithm steps.

In case the secret message was in the form of text, then the Huffman was useful to compress this text message before proceeding with the embedding process. The data pre-processing stage considered only the cover image and secret message process where the data was ready to be handled by other stages. This stage was considered as the pre-processing stage. It is worth to note that a robust steganography technique must fulfil three criteria including the maximum payload stored in the image, imperceptibility (visual quality of the image after embedding), and robustness as mentioned before [54]. In short, the application of the Huffman coding in the proposed steganography scheme guaranteed the fulfilment of the first condition of the secret message capacity.

Table 4.3 shows the experimental results that were conducted on the secret data with different embedding payload (EP), where the mentioned secret data were compressed using the lossless Huffman compression algorithm directly without an earlier encryption process, the table 3.2 showed that the Huffman algorithm reduced the payload percentage well. However, the secret data was compressed in a larger amount when the secret data was first encrypted using the proposed new SSSM encryption method and then compressed with the same compression algorithm (Huffman coding), the reason is that the proposed SSSM method increases the chaotic of the letters in the secret message and this, in turn, enhances the compression algorithm to compress the data in larger quantities, and this is what did the present study obtained practically and as shown in the table below.

Table 3.3: An experimental study on compressing secret data with different EP using compression and encryption algorithms

EP	16384 Byte	32768 Byte	49152 Byte	60000 Byte
Huffman only	12943.36	24903.68	36864	43800
Enhanced Huffman	12124.16	23920.64	35389.44	42600

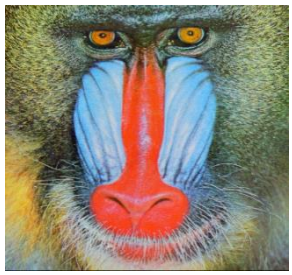
3.5 ORIGINAL IMAGE PRE-PROCESSING

Another pre-processing stage is applied to the proposed scheme before the embedding process to achieve an efficient embedding process called original image preparation. The following sections explain the detailed process of image normalization technique and image transformation decomposition method.

3.5.1 Image Structure

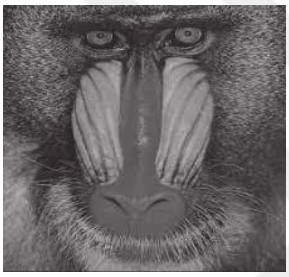
Before explaining the original image repreparation, the structure of image must discuss. The basic item that constitutes the image is the pixels (Picture Cell), wherein every process in the image has to deal with the pixels. In addition, the pixel has two important issues related to the position (coordinate) and value. In this study, both of them were considered to hide the information inside the image. The least significant bit (LSB) was used to hold the secret data and every pixel was represented by 8-bits to achieve the maximum range of the pixel value 255

(2^8). Therefore, for the colour image, 3-pixels were needed each with 8-bits (24 bits) as shown in Figure 3.10.



24 Bits for each pixel

Pixel of (10010101) Pixel of (10010101)Pixel of (10010101)



8 Bits for each pixel

Pixel of (10010101)

Figure 3.10: Typical distributions of the bits in the colour and gray images.

The modulation of the LSB located in the least of the bits in the pixel is very difficult for the human eyes to recognize. Thus, the embedding of this part of the pixel was useful [10]. The main advantage of embedding in the LSB was to provide the image transparency as illustrated in Figure 3.11.

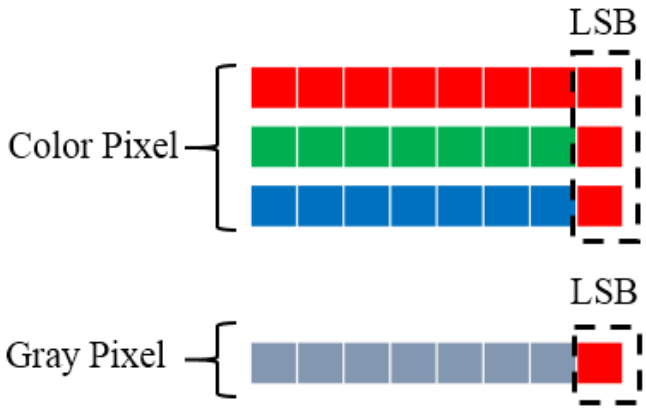


Figure 3.11: The LSB of the pixels in colour and grey images.

Any change or modification of the Most Significant Bit (MSB) makes the difference more noticeable to the human eyes for the gray or color images. Thus, in the steganography method the main aim was to change the image into the LSB format to take advantage of the unseen. Every image must be converted into a binary number to get the LSB for embedding so that changing the LSB provides more facility due to less impact value in this place. Figure 3.12 displays the normal embedding process in the steganography method using the LSB.

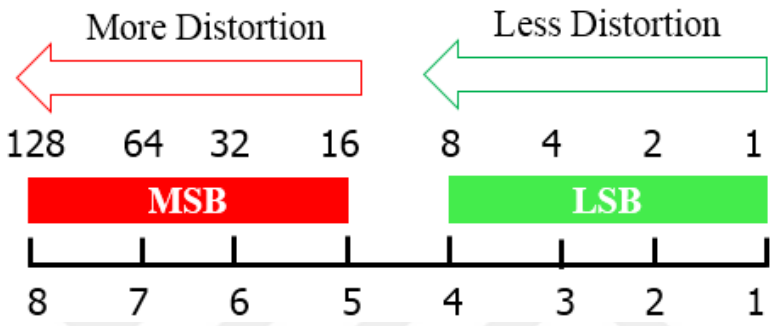


Figure 3.12: The LSB and MSB impact value for each image pixel.

It was clear that any change in the LSB led to an increase or decrease in the pixel value by one while any alteration in the MSB produced a big difference 128. In this case, the MSB place was avoided because it was noticeable by the human eyes. It was vital to check the LSB of the pixel because all the checked information was also stored in the pixel bits. Tracking of the pixel was impossible without the key generated through the embedding process. Thus, the mapping procedure was necessary. The insertion of the secret message directly increased the PSNR of the system and the distortion of the first bit-plane of an image was also increased. The made the detection easy by an HVS attack that is sensitive to any systemic changes. When the matching pixels were checked, the messy bit distribution was kept as much as possible so that the HVS attack could be avoided. The regular embedding process involved the replacement of the bit value of the secret message with the bit in the LSB of the cover image.

For a colour image, the same procedure was followed for the three parts in the pixel. Colour pixels consist of three parts with 8-bits for each Red, Green and Blue. This study considered each part as an 8-bits gray scale pixel and followed the same procedure of converting into the Fibonacci decomposition and embedding into the LSB. The same approach was used in the embedding process, where all bits in the secret message were replaced with bits of all bit-plane

(1), meaning that the bits of the secret message were distributed in image(bit-plane (1)). It is important to look at the image preparation procedure before the embedment.

3.5.2 Image Normalization Technique

This pre-processing phase covered the selection and analysis of the given image before the implementation of any action on it. The image was normalized into a certain range before starting the other processing stages [55] . The cover image was consisted of the 512×512 pixels, where any image used in the proposed steganography scheme followed this range via the expression:

$$I_N = (I - \text{Min})\frac{\text{new Max} - \text{new Min}}{\text{Max} - \text{Min}} + \text{new Min} \quad (3.1)$$

Where $I$is original image, $I_N$normalized image, Max is the maximum range of the selected image, Min is the minimum range of the selected image.

In the beginning, an image was selected from the chosen SIPI dataset [13]. The proposed scheme dealt directly with the chosen image is the 8-bit greyscale. However, for the 24-bits RGB images, the image was first analysed and then its RGB channels were implemented to deal with each channel separately. After completing the separation stage, each image channel in a single 8-bits matrix had an equal dimension with the original image. This implementation produced three channels image and each of these channels was an 8-bit image as illustrated in Figure 3.13

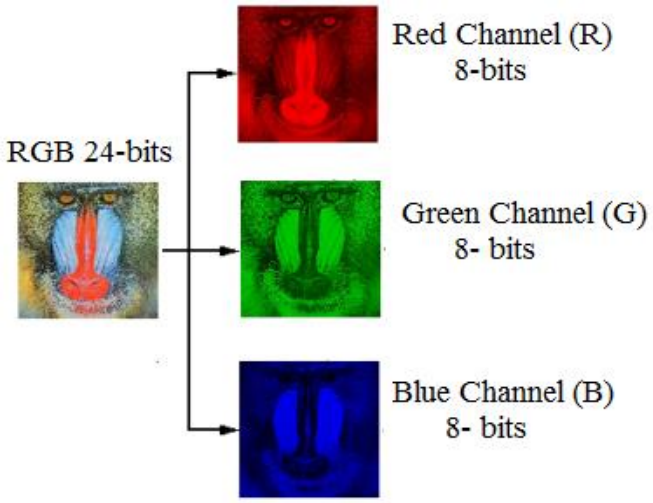


Figure 3.13: Image analysis into RGB channels.

3.6 PIXELS DISPARITY VALUE METHOD (CLV)

This study proposed a new steganography method to hide the secret message inside the cover image using a new partitioning random pixel selection with two parameters. The basic essence of the proposed steganography scheme is to hide the secret message in the certain image and transfer it from the sender to the authorized receiver side without any suspicion raised by the attackers or intruders. The most important thing in the steganography scheme is to keep the quality of the hosted image as identical as the original without causing any doubt to the unauthorized users even in the presence of some text inside it. The lack of awareness of the intruder regarding the existence of some text inside the image was the main aim of the robust image steganography system development.

The resultant image satisfied the imperceptibility by maintaining very high PSNR. The concept behind the secret data embedding process inside the image was based on the generation of the key to select the position of the blocks or pixels of the block. All the procedures inside the embedment were represented by this key. Thus, the best key was generated (called the stego key) for the robust steganography method to achieve the high security. This stego key was used in both sender and receiver side, which carried the embedding procedures and the receiver side was aware of it to reveal back (decrypt or retrieve) the secret text as demonstrated in Figure 3.14

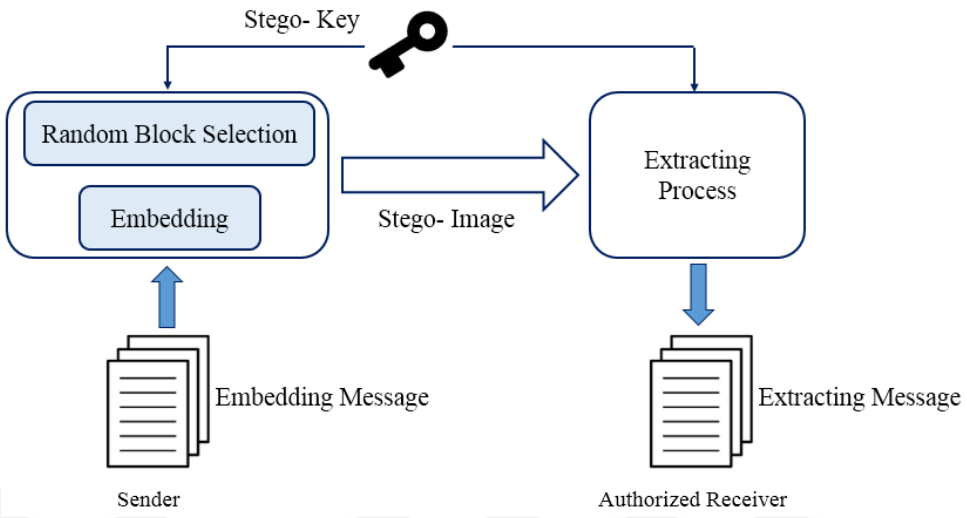


Figure 3.14: The principles of the stego key and hosted image.

The purpose of applying the proposed method is to achieve improved security of the steganography scheme. Each pixel in a colour or grayscale image consisted of decimal numbers that represented the contrast of this pixel or illumination. The grey image is comprised of one decimal value from 0 to 255 (represented in the binary 2^8 occupy 8 bits) where the zero value reflects black pixel while 255 value reflect white pixel and the grayscale starts from the white and ends in black. Most of the differences between the contrasts are at the edges and boundaries of the object, especially when moved from the low to high contrast or vice versa. Figure 3.15 shows the contrast area with the corresponding decimal representation. Figure 3.15 (a) clearly displays different contrast and crossover from the low contrast at the upper left corner to the high contrast at the bottom right corner. The sharp diagonal edge located in the same (Figure 3.15 (b)) contrast when moved between two adjacent pixels with different large values. Due to the little variation between each pair, the best location to embed the secret message is shown in Figure 3.15 (d). Human eye can recognize the difference in the contrast around 30 pixel values. However, insertion in such area often differs as the maximum of two pixel values.

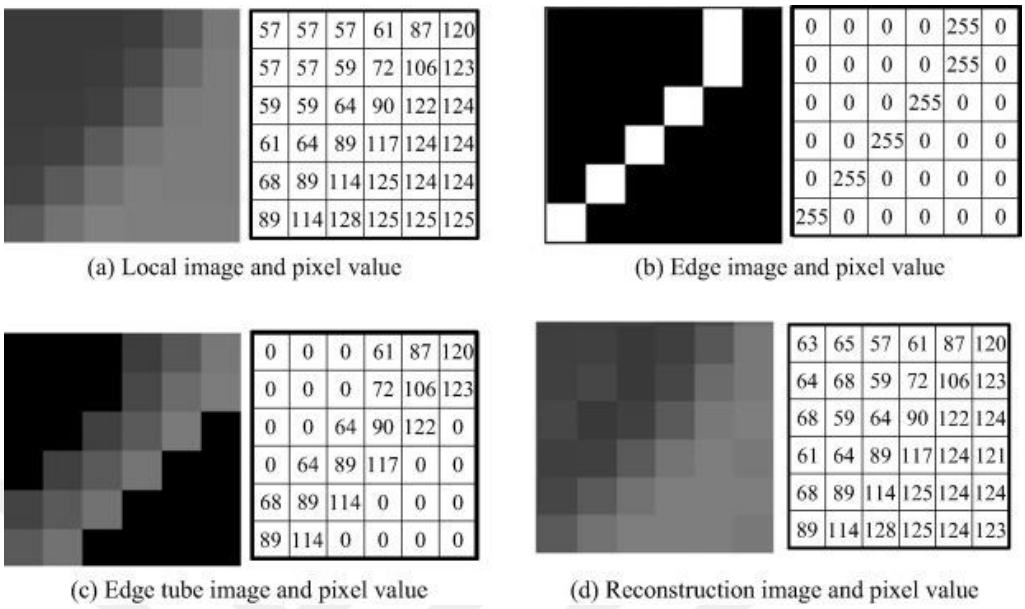


Figure 3.15: Location of the contrast value with the corresponding pixel value.

The colour image is consisted of three values for each pixel such as the Red, Green, and Blue (RGB). These pixels are represented by 24-bits (3 bytes) with one byte for each colour channel. The embedment in such area is more flexible because of the ability to jump over these three bytes. Therefore, the embedment in the colour image is more complex than grey image because three channels need to be checked by comparing three pixel values. When the condition for the pixel embedment is satisfied, then the system is ready for covering the secret bit. Figure 3.16 illustrates colour images with the corresponding pixel values.

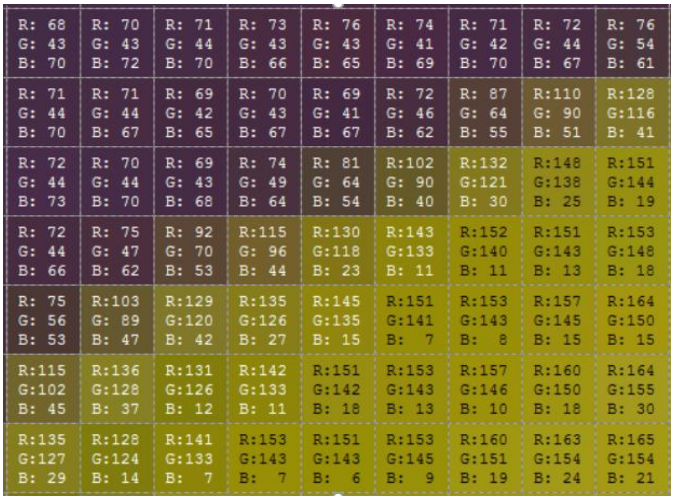


Figure 3.16: Colour image representations in terms of pixel values.

To vary the contrast in the colour image, one must check three values per pixel and find the appropriate one to host the secret key. Often, the varying contrast is located in three channels and positioning a fraction of it in one channel is not easy that need to pass many conditions. Critical condition leads to the robust embedding method that takes care of the condition and thresholding becomes essential.

The two processes within the embedding stage (block selection and data embedment) were performed simultaneously to insert or hide the text into a given cover image (gray or RGB colour) that consisted of 512×512 pixels. As the initial stage, the image was divided into 8×8 blocks each with 64×64 pixels. First, the block was selected then from this block the pixels were chosen for the embedding purpose as shown in Figure 3.17 where the partitioning of the 262.144 pixels (512×512) were performed. The random process was responsible for dividing the cover image into sub-blocks, where three rounds of the random function were used in this process to select the use of the first pixel for the embedding. For the high security issues regarding the proposed scheme, the Henon random function is used. This random function was beneficial in term of increasing the complexity of the aimed blocks or pixels selection processes up to 10^{30} round steps (theoretically).

The behaviour of the dynamic Henon map function was chaotic which operated with two control parameters (a =1.4 and b = 0.3). This function depended primarily on a and b parameters and illustrated as the coordinate point (X_n, Y_n) in the plane. The new points were concluded from this equation through the relation:

$$\begin{cases} x_{n+1} = 1 - a\, x_n^2 + y_n \\ y_{n+1} = b\, x_n \end{cases} \tag{3.2}$$

The primary objective of using these three steps (for block and pixel) of a random map was to increase the security of the message embedded in the cover image. In order to get the random distribution of the pixels, matching pixel values with secret data value was needed. The embedding stage consisted of two main processes those run simultaneously to insert the secret bits into the image pixels as shown in Figure 3.17.

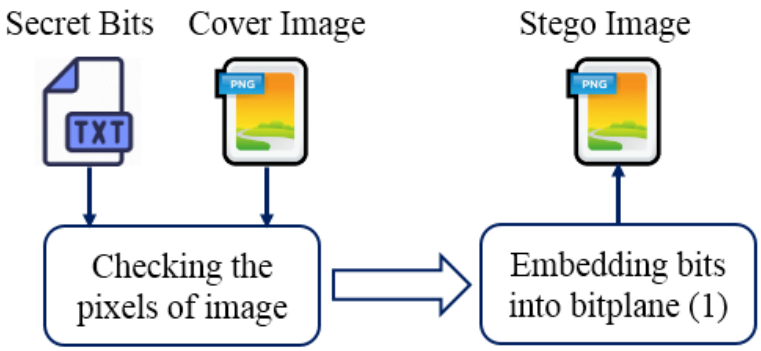


Figure 3.17: The embedding process of the ISS.

In the 2D image matrix, the use of general invariant sets of a dynamic system for selecting the random function was very useful. The Henon function described the dynamic properties for different values using two parameters (a and b $\in$ R), which was worthy for the selection of the blocks inside the image and pixels distributed over the block. In the proposed study the Henon map function was utilized in two rounds. The first one was the selection of the block from 64 blocks of the image that occurred under the Henon map function which produced one value randomly because the chaotic behaviour of the Henon function. For the first time, the Henon map function was utilized to select the block. In the second round, the pixel was selected from the 4096 pixels (64×64) belong to one block. This stage was somewhat complex because of some procedures that arranged the orders of the secret bits and corresponding pixels. The distribution of the Henon map produced good chaotic features due to the use of two control parameters those led to an increase in the complexity of the generated random number as presented in Figure 3.18.

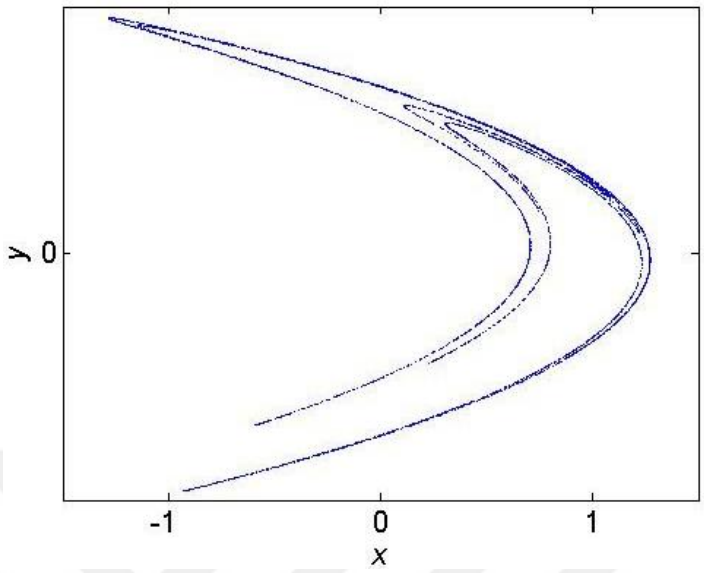


Figure 3.18: Henon map with a≤1.4 and b≤0.3.

In the Henon function (Figure 3.20), the default initial values were a =1.4 and b = 0.3[56]. For $a < 1$ it was easy to recognize that the chaotic space was first affected and then produced the random number to select the block or pixels. Within the 64 blocks of the image (8× 8), one block was selected to take the effect of the next procedures for the pixels' selection. Every selected block stored its location in the key called the stego key that was responsible for storing all the events to be used in the other part (receiver) for the information extraction.

As aforementioned, any embedding method consists of two processes such as the pixel selection and pixel insertion processes. The pixel selection is responsible for achieving the enhanced security and imperceptibility of the data hiding system. In this perception, present study aimed to maintain these two criteria. The pixel selection was accomplished in two stages. First stage was the movement around the image via single movement strategy. Second stage checked the condition for embedding. These two stages actually operated simultaneously, and one completed the other. The selected pixels were accumulated in one vector. Upon completing the selection process, these pixels were randomly rearranged according to the new random technique while keeping the index for each pixel. The 8 neighbour's strategy was used to move over the image according to one condition related with contrast value. These 8 neighbours covered the image and moving vertically, horizontally, and diagonally as illustrated in Figure 3.19.

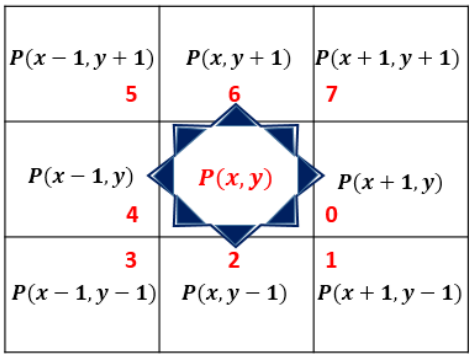


Figure 3.19: The 8 neighbours' pixel movement strateg.

Certain pixels were considered as the coordinate position in the image matrix where such pixel could move in every direction by increasing or decreasing the x-axes and y-axes. The proposed scheme compared the values of the centre pixel (x,y) and its neighbours (±x, ±y). When these pixel values differed according to the threshold, then the position of this pixel was saved in the vector form and moved accordingly. Otherwise, it was skipped to the other pixel coordinate. Consequently, the pixel was positioned in the middle of two areas of high and low contrast; wherein the embedment of the secret bit was in the side of near brightness. For example, when the difference between two pixels' value was according to the threshold chosen experimentally (such as the 4 decimal value) then the secret bit was embedded in two pixels beside the certain pixel. Conversely, when the secret bit was 0, then the secret bit was either embedded with the high value or else (secret bit 1) with the low contrast value and so on as explained in Figure 3.20. The contrast level check of each pixel enabled to scan the entire image for choosing the suitable location (pixel) to hide the secret bit. Subsequently, this method produced high imperceptibility and high security, indicating the success of the proposed steganography scheme. In addition to the pixel selection strategy the pixel replacement must be applied to further enhance the imperceptibility and security of the data hiding algorithm which is discussed below.

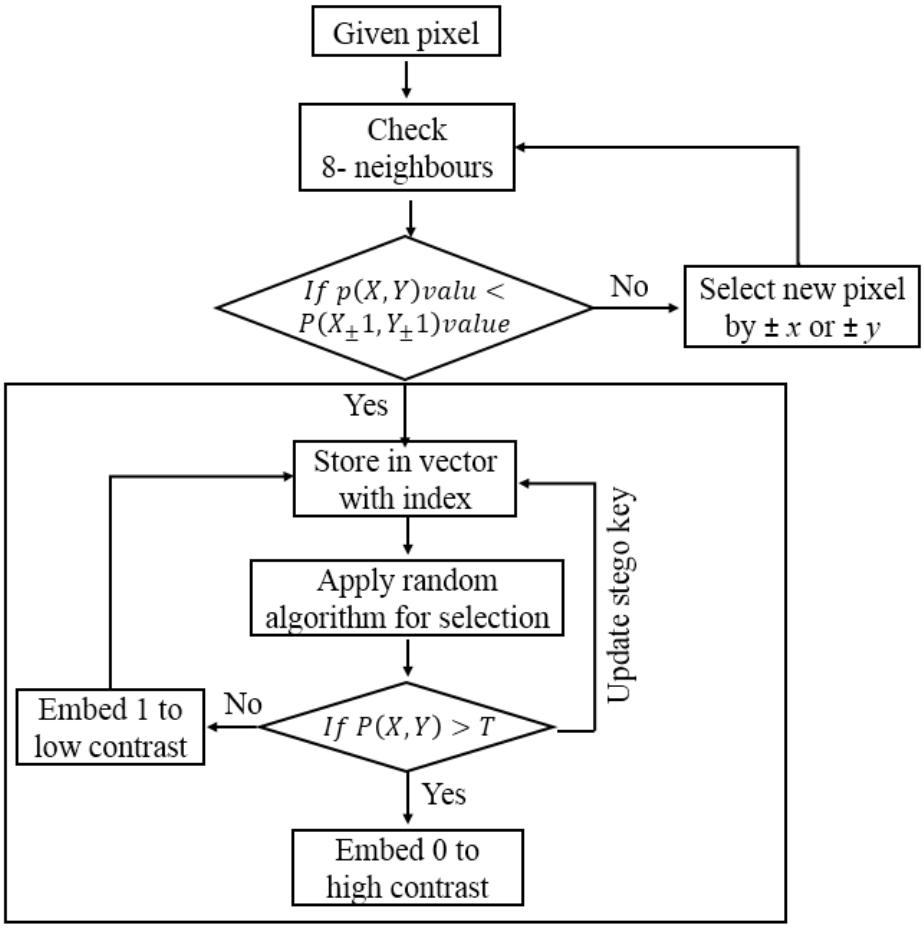


Figure 3.20: The proposed embedding strategy.

Another objective of the proposed image steganography system was concerning the image visual quality (imperceptibility). Figure 3.21 depicts a general embedding process (without Fibonacci) using the proposed method wherein just the Fibonacci LSB of bitplane (0) was affected. This implied that the standard embedding of the first bit in the LSB was increased, decreased or stayed the same.

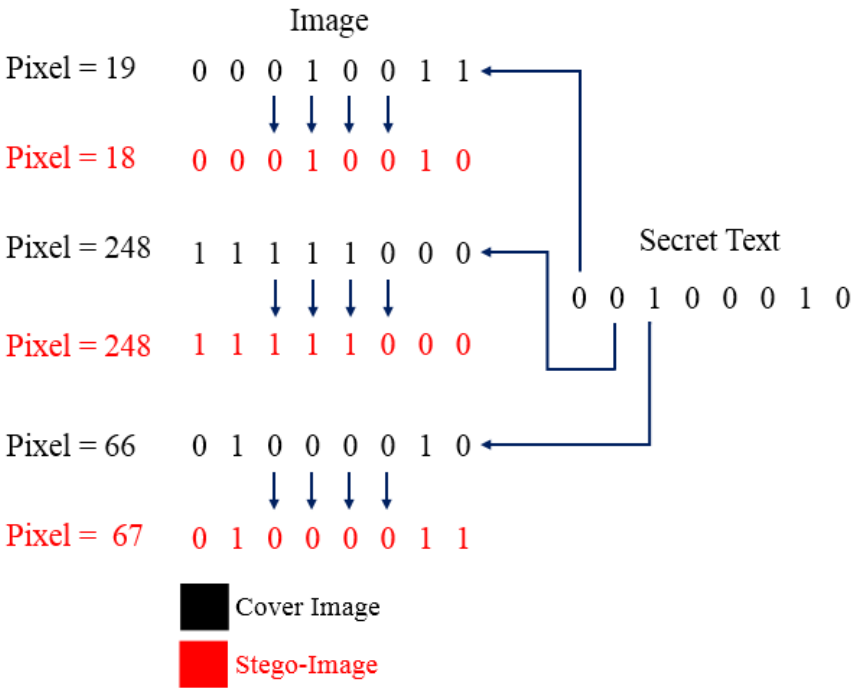


Figure 3.21: A conventional embedding process of the secret bits into image pixels.

It is clear (Figure 3.21) that the embedment of the value 0 from the secret bits to the value 1 of the cover image pixels led to a decrease in the value of the stego image pixels by one and vice-versa. However, in the second case the embedment of a value of 0 from the secret text to the value 0 of the cover image pixels kept the value of the stego image pixel same. In addition, the change in the value of the pixel led to change the LSB of the pixel, thereby altering just in the bitplane 0 without affecting the other bits. This operation was significant in the ISS because less change implied the attainment of the high imperceptibility (high image quality). The change in the Fibonacci LSB of the pixel did not affect too much the quality of an image. However, the human eyes can recognize a difference in the pixel intensity around 30. For instance, when the pixel value was 125 and the change was less than 30 (for example 115) or more than 30 (say 143) the human eyes could not recognize that difference. However, the computer algorithms can detect any such change mathematically by the special evaluation criteria. Thus, the main aim was to reduce the change as little as possible to keep the image same as the same original without any variation.

All information related to the secret message preparation, image partitioning, and embedding procedures were stored in the stego key. When this key was stored inside the image it was called

the implicit stego key and when stored outside the image it was known as the explicit stego key. There was an agreement between the parties regarding this key (produced by the sender and used by the receiver) to extract the secret message form the image. The stego image could stand against various attacks and therefore many tests were applied to the image before sending it to the other part or receiver. These attacks or evaluations were carried out in the sender part and presented in Chapter 4.

3.7 IMAGE TRANSFER IN SENDING AND RECEIVING PROCESS

In the information hiding area, the data transmission must be through the digital media. Six types of digital media have been used so far in the field of steganography. The proposed scheme used an image as the carrier of the digital media because an image has several advantages including the high information carrying capacity, easy analyses, wide usages and high reliability. However, once it held a secret message it became a stego image that with the secret message inside. Usually, the transmission of the images from the sender side to the receiver side occurs in two ways either via a trusted digital channel such as the internet or by physical equipment like (CD or memory or any other hard drives). Before sending a stego image through these media one must check the robustness of the stego image by different evaluation criteria to ensure its robustness against any attack. The receiver gets the stego image and extracts the useful information (secret message) via the stego key that is attached with a stego image. Extraction of the information from the stego image is the reverse process of the embedding. Figure 3.22 illustrates the sending and receiving processes using the ISS.

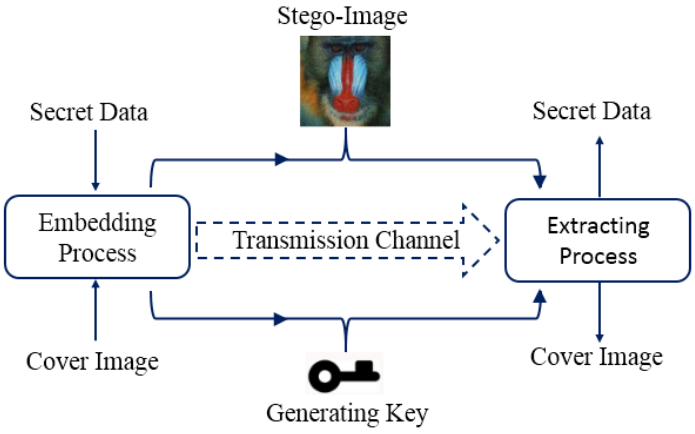


Figure 3.22: The general procedures for the image transfer in the ISS.

The main goal of the ISS is the security so that the transferred image via the internet remains undetectable by the intruders or attackers. The statistical methods are always used by an attacker to detect the presence or absence of a secret text inside the stego image. Some changes may occur in the pixels of an image during the data embedding that often appear as a weak point in the image. It is this weakness that is detected by the intruders by analysing the stego image via some statistical methods. To avoid such shortcomings, the proposed ISS fabricated a highly secure stego image and evaluated its legitimacy to determine the effects of such change on the stego image. In short, to keep the stego image free from the attacks the proposed ISS maintained high imperceptibility and security with ultimate payload capacity during the embedding and extracting procedures. The undertaken security in the extraction stage of the proposed ISS is discussed below.

3.8 EXTRACTING STAGE

The central objective of the extracting stage is to get the embedded data (secret bits) from the LSB pixels and simultaneously follow the procedure designed in the embedding stage. Most of the information related to the extracting stage is made by the agreement between the sender and receiver. The rest of the information used by the implicit stego key that considered variable information based on image nature and environment. The main objectives of steganography (security and imperceptibility) was achieved in the proposed embedding and extracting stages. The embedding and extracting stages were responsible for keeping the image quality (imperceptibility) as high as possible. Meanwhile, the security of the proposed ISS was reflected in the two processes that worked together as one process such as the partitioning of the image and the randomization of both blocks and pixels selection. These were considered as the major objectives in the proposed scheme for increasing the capacity that was achieved in the pre-processing or preparation stage. The cover image hosted the secret message selected from the SIPI standard dataset.

In the proposed ISS, the extracting process was performed at the receiver side where the image pixels were decomposed according to the agreed algorithm between the sender and receiver in advance. The entire algorithm of embedding and extracting stages was known but some information was needed to specify the index pixels' location and the size of partitioning that were not agreed in advance. This extra information was carried out by the stego key during the

embedding process immediately. In this case, the stego key was updated until the finish of the embedding process. The extraction followed two procedures wherein the first one was the general algorithm that revered the procedure of the embedding as seen in Figure 3.23. Conversely, the extraction used three processes that worked as a reverse of those in the embedding process (reassigned the pixels and check the certain condition of the pixel).

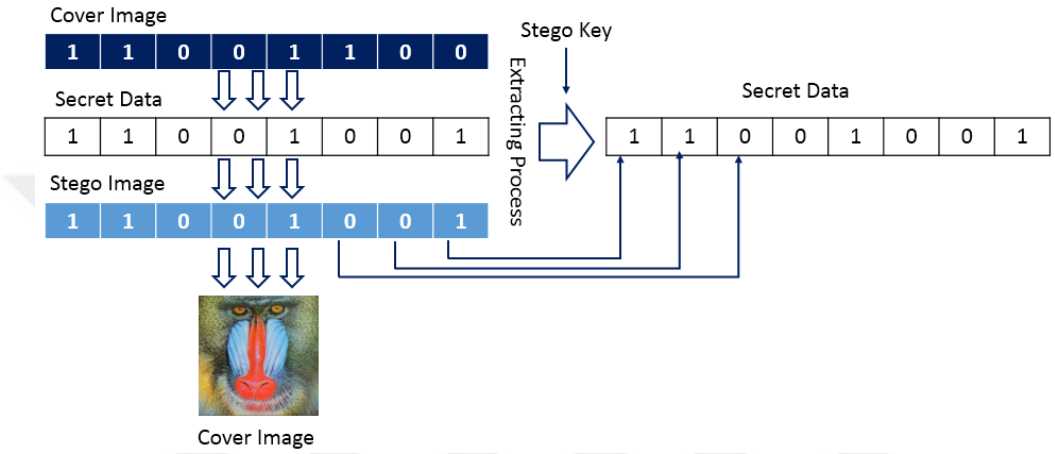


Figure 3.23: The extracting process in the proposed ISS.

Any given pixel value may decrease, increase or stay the same according to the general algorithm, secret key and stego key information. If the pixel value was increased by one it meant the secret bit as 1. If pixel value was decreased by one it implied the secret bit as 0 and if the pixel value stayed the same it signified that the secret bit and the cover image value were the same. The section below present the results obtained using the proposed ISS when implemented on the standard dataset followed by the detail analyses and discussion.

4. SECURITY AND EVALUATION ATTACKS

4.1 INTRODUCTION

In the field of information hiding, the network communication between two clients over the far distance are commonly evaluated based on three major issues namely the quality, security and capacity. This chapter presented the experimental results, analyses, discussion and comparison obtained from the proposed steganography method. Three main criteria were presented to evaluate the finding where it addressed the most important issues in the steganography scheme. These include the capacity and robustness enhancement using a new decomposition technique that was not familiar to the hacker. The system security was improved via the introduction of the new embedding method that is based on the CLV method. Numerous types of attacks face the steganography systems such as the Human Visual System (HVS), Peak Signal to Noise Rate (PSNR) and structural similarity index (SSIM). The security performance of the newly proposed scheme was evaluated against these attacks. The first one is based on human eye detection and the others is fully based on statistical systems. Evaluation is made by different amounts of capacity embedded into the system. The objective of security and robustness is underscored. First, the new intelligent security method was performed and secondly, the robustness of the stego image was carried out.

4.2 RESULT AND DISCUSSION

The applied processing via the proposed ISS that affected the image quality and led to some information loss was ascertained through various evaluation measures. The evaluation procedures of the stego image can be objective and subjective. The objective methods depended on finding the differences by applying the numeric criteria and using several criteria such as ground truth or prior knowledge of statistical issue. Conversely, the subjective methods depended on the observation of humans and judgment without any referred criteria. The present study considered the standard evaluation measures (objective methods) to validate the proposed ISS including the embedding capacity (EC), peak signal to noise ratio (PSNR) and structural similarity index (SSIM). The EC value can be defined as ratio of the number of message bits to the number of cover pixels [43] which is directly related with the number of pixels used in the

proposed scheme. Different number of message bits were embedded by one pixel and the EC is expressed as:

$$EC = \frac{\text{The number of message bits}}{\text{The number of cover images's pixels}} \quad (4.1)$$

The following parameters were used in the simulation:

i) For a given image of dimension (512×512) pixels, 16384 bytes corresponded to 6.25%, meaning that every two pixels represented 16 bits, thus 1/16 = 6.25% when 1 bit of two pixels was embedded.

ii) For a given image of dimension (512×512) pixels, 32768 bytes were equal to 12.5%, implying that every pixel corresponded to 8 bits, so that 1/8 = 12.5% when 1 bit of one pixel was embedded.

iii) For a given image of dimension (512×512) pixels, 49152 bytes corresponded to 18.75%, signifying that every two pixels were assigned to 16 bits, accordingly 3/16 = 18.75% when 1.5 bit of one pixel was embedded.

To evaluate the image quality, PSNR was calculated after the embedding process and a comparison was made between the original and stego images. The process of data embedding was considered to be imperceptible to the HVS when the result of the PSNR was ≥ 30 db[11]. The value of PSNR was calculated using the expression:

$$PSNR = 10.log_{10}(\frac{255^2}{MSE}) \quad (4.2)$$

with

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (4.3)$$

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 corresponding original and noisy pixel.

The PSNR value was based on the MSE that affected adversely. The parameters of PSNR allowed normalizing the equation for all methods and image types. During the implementation of the proposed ISS two important stages were involved namely the training and testing. In the

conventional image processing, the imperceptibility of the stego image is determined using the PSNR measures [57]. By applying the PSNR measures, the fidelity of the stego image can be evaluated against the original carrier image. In other words, the level of distortion in the stego image can be measured against the carrier image in the units of decibel (dB). A higher score of the PSNR corresponds to the high quality image, thereby minimizes the detection probability of the attack using the HVS [58]. Using the training phase, the PSNR became less when the MSE was large, implying that the mismatching was increased between the original image and stego message. For high MSE, the result was not satisfactory in terms of the PSNR because of their inverse relationship. This problem was overcome in the testing stage and the achieved results were better than the one obtained by others.

Thus, to measure the similarity between the original image and the stego image the value of SSIM was used [48]. The value of SSIM (ranged from - 1 to 1, wherein 1 indicated no difference between the original image and stego image) was calculated via:

$$SSIM = \frac{(2P_O Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2 Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2)} \quad (4.4)$$

where$P_{O,}P_O^2$ and σ_O^2 corresponding to the original image as well as Q_S, Q_S^2 and σ_S^2 for the the stego image denote the respective mean pixel value, variance and standard deviation. The covariance between the original image and stego image is represented by σ_{OS}. C_1 = k_1L and C_2 = k_2L are constants with k_1 = 0.01, k_2= 0.03, and L = 255 for the grayscale image.

Table 4.1, 4.2 and 4.3 illustrates the obtained PSNR values for the three types of embedding (simple LSB, and CLV) used to evaluate the performance of the proposed ISS with different EP for colour standard SIPI images (Lena, Baboon and Tiffany (512×512)).

Table 4.1: The values of PSNR for the color Baboon image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)	
	Simple LSB	Proposed method
6.25 %	59.910	70.080
12.5 %	57.919	68.402
18.75 %	55.999	67.849

Table 4.2: The values of PSNR for the color Lena image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)	
	Simple LSB	Proposed method
6.25 %	57.001	67.425
12.5 %	54.998	65.520
18.75 %	54.888	64.211

Table 4.3: The values of PSNR for the color Tiffany image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)	
	Simple LSB	Proposed method
6.25 %	57.999	69.276
12.5 %	56.998	67.464
18.75 %	54.339	65.909

Generally, the calculated PSNR values for the color images are lower than the gray scale images due to the representation of color pixels image with 24-bits for one pixel as opposed to only 8-bits for the gray scale. Figure 4.1 (a, b and c) depicts graphically different results for the imperceptibility obatined using the colour Baboon, Lena, and Tiffany (512×512) images with different payload capacity.

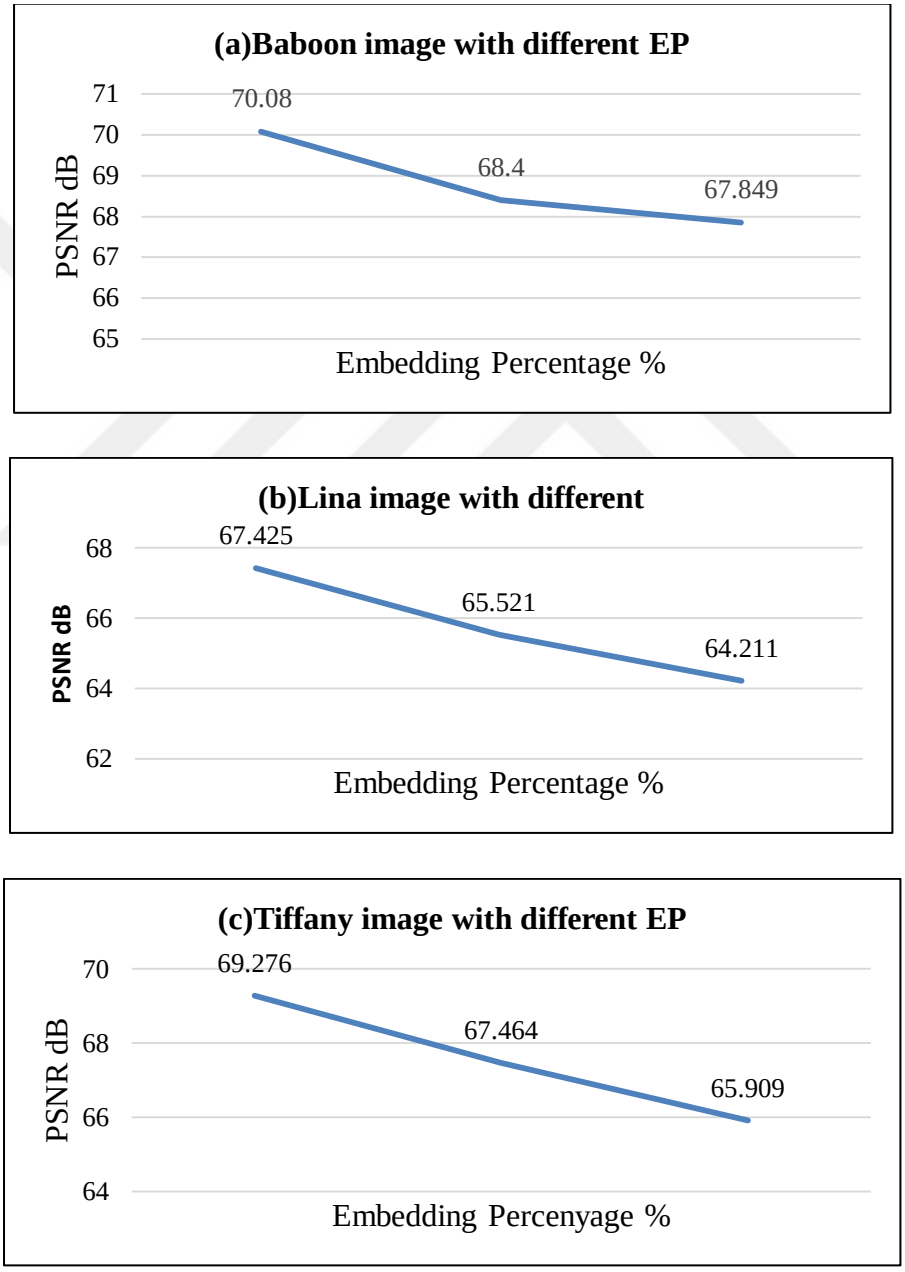


Figure 4.1: The PSNR outcomes of the proposed CLV method for the colour images (a)Baboon, (b)Lina and (c)Tiffany with different EP values.

The primary goal of the proposed ISS was to keep the stego image same as the original image as viewed by the naked human eye or via the statistical methods when using a limited payload capacity. In the proposed method used different evaluation tools like PSNR and SSIM, to check the stego image before sending it to the authorized receiver to ensure that familiar attacks like HVS, Chi-square and Histogram were unable to detect the secret message. Figure 4.2 shows the similarities between the stego images and the original image with different Paylaod capacity.

Figure 4.2: The stego and original images' resemblance with different paylaod capacity.

The original image appeared like a stego image with an acceptable amount of embedding such as the second row of the figure. However, when it exceeded the embedding limit the image was destroyed and was detectable to the hacker easily as indicated by the last row in the figure. The efficiency and quality of the proposed scheme was tested on diverse stego images with different amount of EP. Table 4.4 displays the results for the standard colour (Lina, Baboon and Tiffany (512×512)) images.

Table 4.4: Different evaluation tools with different amount of EP for colour images

Lina	6.12%	12.5%	18.75%
	SSIM	SSIM	SSIM
	1	1	0.9999
Baboon	6.12%	12.5%	18.75%
	SSIM	SSIM	SSIM
	1	0.9999	0.9998
Tiffany	6.12%	12.5%	18.75%
	SSIM	SSIM	SSIM
	1	1	0.9999

The results obtained using the proposed ISS were compared with the exisiting state of the art techniques (Table 4.5 and Figure 4.3). The evaluation results of the proposed method were found to be better than those reported in the literatures. This indicated that the tools used for the pre-processing and embedding stages in the proposed ISS allowed to improve the results.

Table 4.5: Result comparison between the proposed scheme and the state of art

Reference / Code	**Image/ Dataset**	**EP %**	**PSNR (dB)**	**SSIM**
[14] / **(A16)**	USC-SIPI 512×512	6.25%	46	0.899
[36] / **(B16)**	USC-SIPI 512×512	6.25%	65.9	0.996
[44] / **(C17)**	USC-SIPI 512×512	6.25%	54.5	0.978
[32]/ (D18)	USC-SIPI 512×512	6.25%	50.21	0.957
[8] / **(E19)**	USC-SIPI 512×512	6.25%	51.22	0.968
[48] / **(F20)**	USC-SIPI 512×512	6.25%	58.22	0.981
Proposed Study / (P20)	USC-SIPI 512×512	6.25%	70.08	0.999

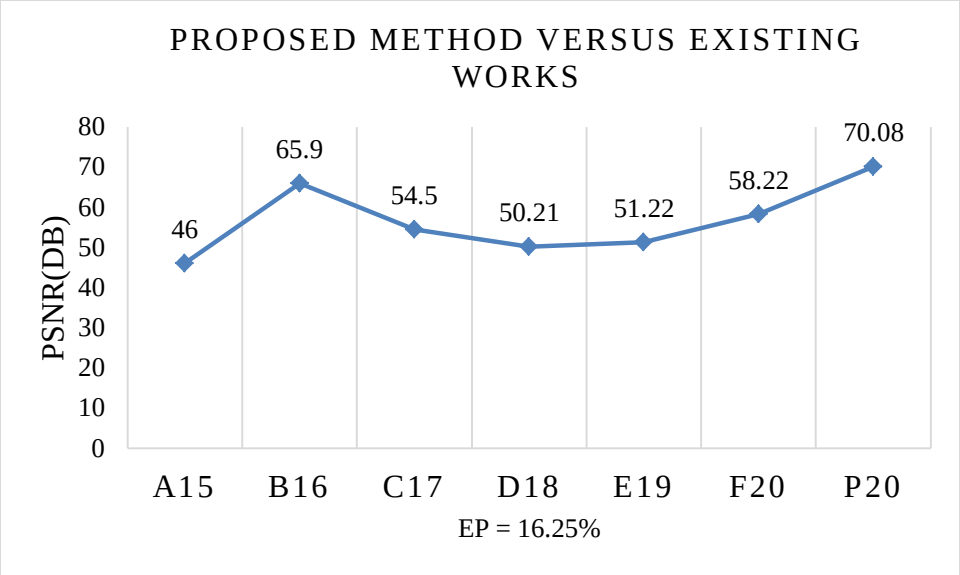
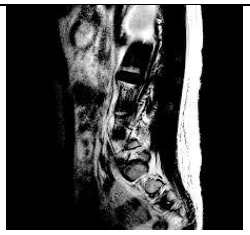
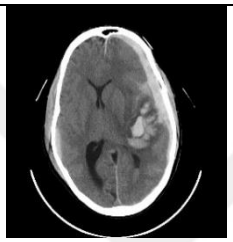
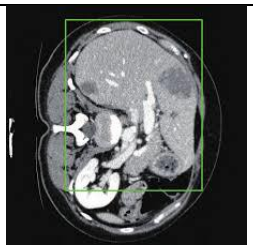
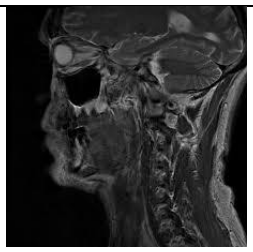


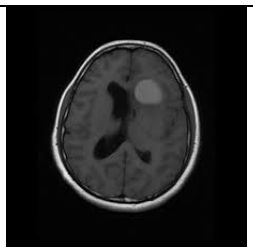
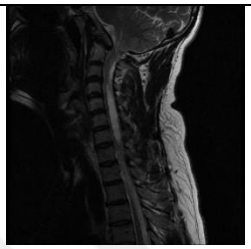
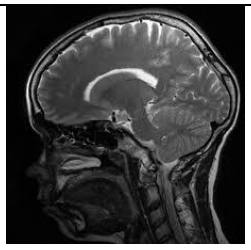
Figure 4.3: Comparison study of CLV method versus the existing state of the art methods.

Based on the outstanding experimental results obtained using the proposed ISS when compared with the existing state of the art methods, an inverse relationship between the PSNR and EP was established. An increase in the EP value led to distort the image visual quality and thus reduced the percentage of the PSNR. It was asserted that all the existing methods maintained the balance between the capacity and PSNR by developing an embedding method or improving the secret data before embedding.

Based on the findings it was concluded that more than 80000 bytes embedment can distort the image and make it visible to the human eye. This further indicated that the image had less imperceptibility. Thus, embedment of 16000-30000 bytes can be more reasonable because of the high PSNR values that are unnoticeable to many attacks. It was affirmed that an increase in the payload can cause a reduction in the PSNR values and vice versa. In addition to implementing the proposed scheme on the SIPI standard image dataset, different medical images were taken from [47][48] in order to test the system performance. The test images were evaluated the performance of the system with different evaluation parameters as seen in Table 4.6.

Table 4.6: Test medical images used to evaluate the performance of the system

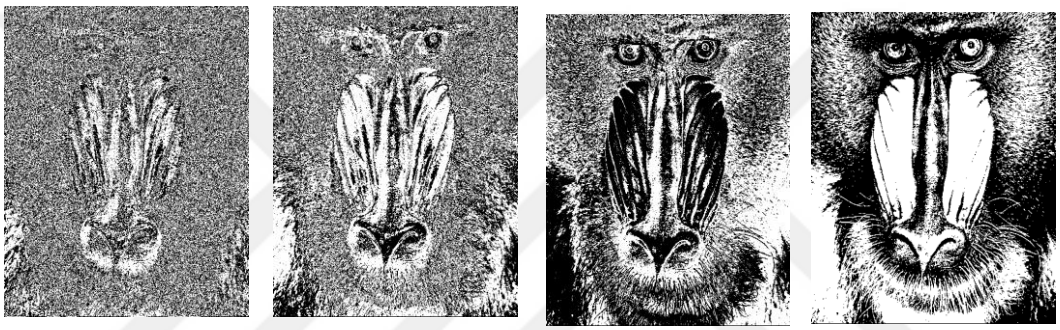
Medical image	EP %	PSNR (dB)	SSIM
	6.25%	66.21	0.9999
	6.25%	65.11	0.9999
	6.25%	67.13	1
	6.25%	66.23	0.9999
	6.25%	66.87	1

	6.25%	64.14	0.9999
	6.25%	65.12	0.9999
	6.25%	63.45	0.9999
	6.25%	66.20	0.9999
	6.25%	66.52	0.9999

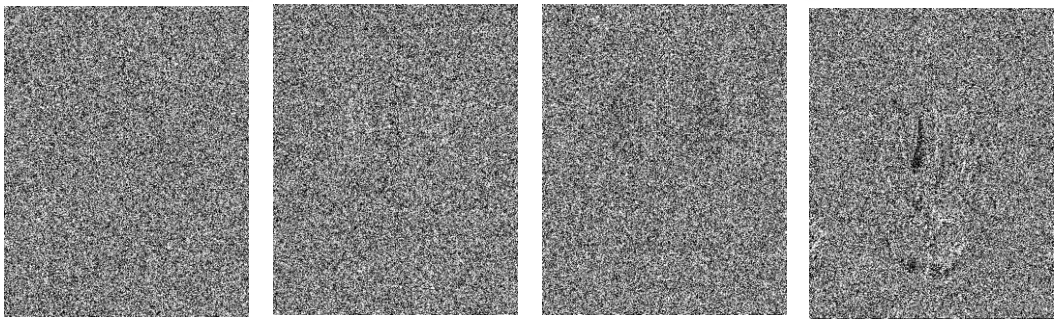
4.2.1 Human Visual System Attack

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 (4.4 a and b).

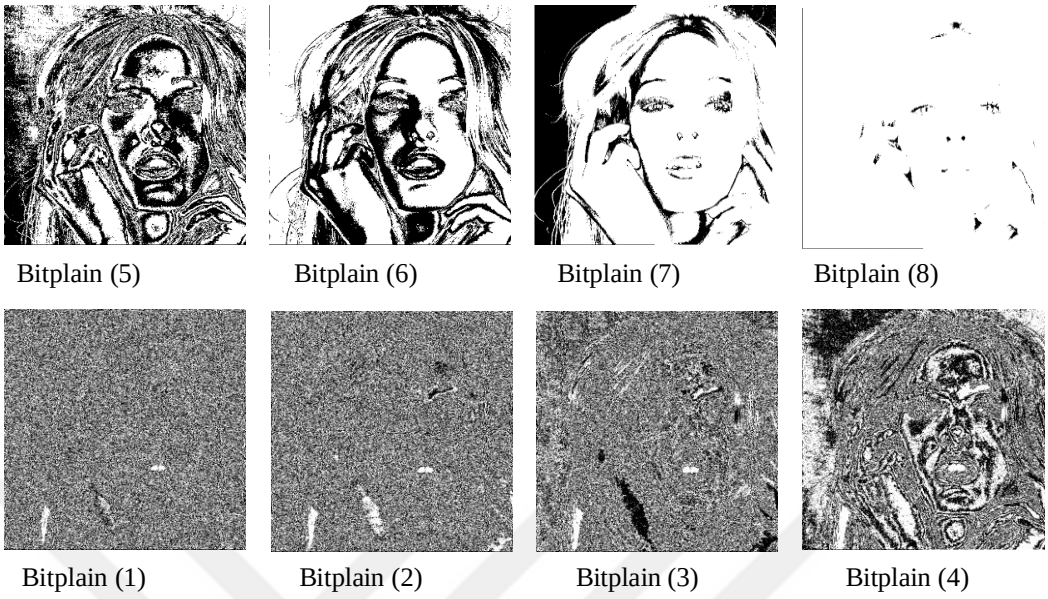


Bitplain (5) Bitplain (6) Bitplain (7) Bitplain (8)



Bitplain (1) Bitplain (2) Bitplain (3) Bitplain (4)

(a)



(b)

Figure 4.4: The demonstration of the visual attacks with different bit planes for the peppers.

The eight-bit planes HVS attack can detect only the LSBs and the rest are ignored. In Figure 6.13 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 these two pixels hidden information are 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 scheme, three methods were applied to the images so that it was easy to determine the differences when compared. Figure 4.5 depicts these three methods including the simple LSB, Fibonacci, and proposed CLV method.

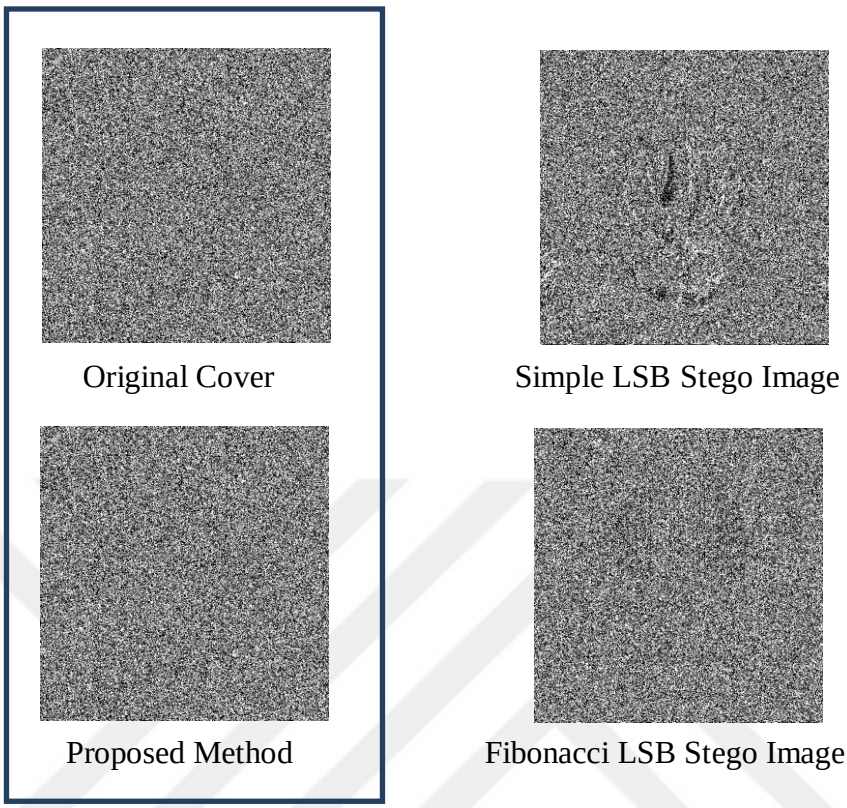


Figure 4.5: The performance of three methods against HVS attack for the original Baboon image

It is observed (Figure 4.5) 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 from the results that are very close to the original image. In short, the proposed method (Figure 4.9) produced more similar outcome (after embedding) to the original image (before embedding) than other methods due to the arbitrary distribution ofthe bits. Moreover, it kept the values of the original image bits identical by mapping the secret bits before embedding.

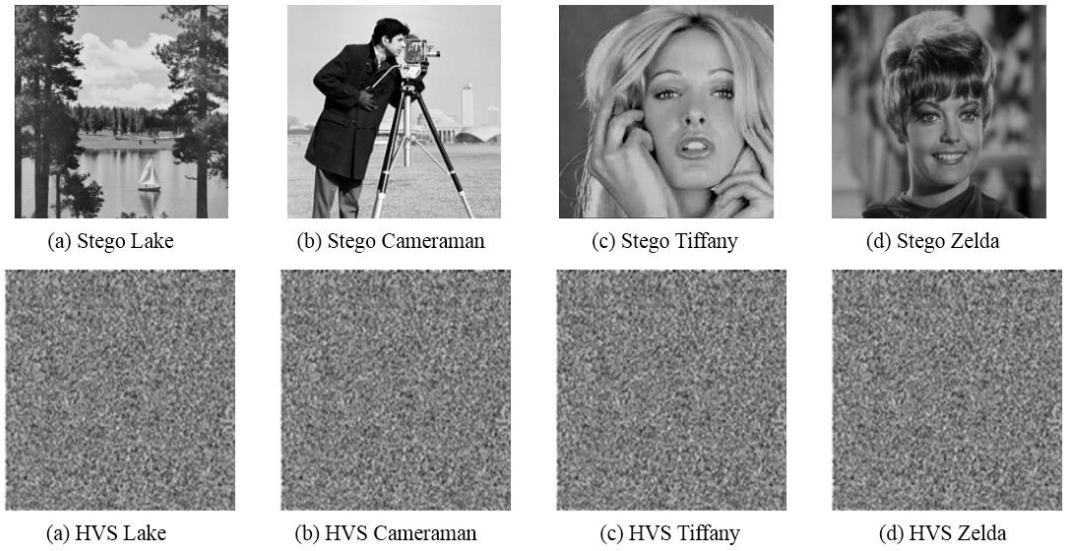


Figure 4.6: The attack attempts tothe image into bits to see where the encrypted message.

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 4.6 (a-d). This training was for the bit plane (1) of the LSBs and the results were almost identical to the original image. The HVS attack are 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 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.

5. CONTRIBUTIONS AND FUTURE WORK

5.1 INTRODUCTION

This chapter summarizes the contribution of the proposed study, experimental evaluation of the newly developed steganography scheme and future outlook related to some new research directions emerged from the present work.

5.2 CONTRIBUTIONS OF THE STUDY

This study aimed to build an immune steganography scheme that can withstand different types of attacks, thereby improving its security with the high degree of imperceptibility. The notion of the capacity was also emphasized in the scheme and performed due to its immense significance in the steganography systems [48]. Notably, the imperceptibility and security are mandatory for any steganography system [43], [60]. Accordingly, they are carefully considered in this study and made several noteworthy contributions in the field of steganography as explained below.

5.2.1 Pixels Disparity Value Utilization

The proposed *CLV* method returns to the spatial domain based steganography. In this work, the massive change in the embedding strategy was considered based on the distinction in the grade value of the pixels in order to keep the quality of the image identical to the original one without any suspicion even in the presence of a text inside, thus preserving the image from the human eye perception. In fact, a little change among the pixels cannot be recognized (less than 30 value) by the human eyes but substantial dissimilarities can be easily recognized. The idea behind the proposed method was to meticulously embed the secret bits when the difference in the grade value of the pixels was less than 30 such that no one can see any alteration in certain images. Consequently, these differences were exploited to improve the robustness of the newly introduced steganography scheme.

5.2.2 Capacity and Robustness Enhancement

Categorically, the capacity and robustness are among the main criteria of a successful steganography system. Therefore, the researchers have made dedicated efforts to enhance these

two criteria at the maximum possible extent. To achieve this perspective, *an enhanced Huffman coding algorithm* was utilized to compress the secret message before embedding and removing the redundant letters through the secret messages after the compression to exploit the chaotic letters within the text.

5.2.3 Security System Integrity Enrichment

The security of steganography method is one of important issue that must be achieve. The security was solved using the improved Henon map function for the randomness which selected the correct position for the embedment based on two control parameters. In this regard, the integrity of these two issues made the proposed steganography scheme more immune against any attack.

5.3 FUTURE WORK

The improvement of the steganography system is a never-ending process. In this study, though all the objectives have been accomplished, but the personalized results remain incomplete which need further investigations. This work opened up several new avenues that are worth doing for the future. For instance, the security can be enhanced by mixing the frequency domain and special domain. This may achieve better results in terms of the security and robustness. In addition, the proposed method can be combined with the DWT and embedding may results in high coefficients based on the obtained findings. Many methods have already used high coefficients for the embedding. However, the use of CLV may yield better results in terms of the security and imperceptibility. The most important gap in the steganography system is related to the capacity improvement of the secret message. The limitation of the secret message with PSNR makes the steganography difficult to improve. In such scenario, it is better to handle the secret message before embedding and to make it dynamic with the embedding method, thereby making the pre-processing step interactive with the embedding process.

REFERENCES

[1] P. Chowdhuri, B. Jana, and D. Giri, 'Secured steganographic scheme for highly compressed color image using weighted matrix through DCT', *International Journal of Computers and Applications*, 2018.

[2] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, 'Image steganography in spatial domain: A survey', *Signal Process. Image Commun.*, 2018.

[3] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, 'A New Payload Partition Strategy in Color Image Steganography', *IEEE Trans. Circuits Syst. Video Technol.*, 2020.

[4] G. Swain, 'Adaptive and non-adaptive PVD steganography using overlapped pixel blocks', *Arab. J. Sci. Eng.*, vol. 43, no. 12, pp. 7549–7562, 2018.

[5] N. G. Aroukatos, K. Manes, and S. Zimeras, 'Social Networks Medical Image Steganography Using Sub-Fibonacci Sequences', in *mHealth Ecosystems and Social Networks in Healthcare*, Springer, 2016, pp. 171–185.

[6] T. Tuncer and E. Avci, 'A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images', *Displays*, 2016.

[7] L. D. Singh and K. M. Singh, 'Implementation of Text Encryption using Elliptic Curve Cryptography', in *Procedia Computer Science*, 2015.

[8] A. K. Sahu and G. Swain, 'An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function', *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 159–174, 2019.

[9] N. G. Kini, Gautam, and V. G. Kini, ‘A parallel algorithm to hide an image in an image for secured steganography’, in *Studies in Computational Intelligence*, 2019.

[10] R. Shanthakumari and S. Malliga, ‘Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment’, *Sadhana - Acad. Proc. Eng. Sci.*, vol. 44, no. 5, pp. 1–12, 2019.

[11] A. M. Fadhil, ‘Bit Inverting Map Method For Improved Steganography Scheme’. *Universiti Teknologi Malaysia*, 2016.

[12] W. C. Kuo, C. C. Wang, and H. C. Hou, ‘Signed digit data hiding scheme’, *Inf. Process. Lett.*, 2016.

[13] K. Gaurav and U. Ghanekar, ‘Image steganography based on Canny edge detection, dilation operator and hybrid coding’, *J. Inf. Secur. Appl.*, vol. 41, pp. 41–51, 2018.

[14] T. D. Nguyen, S. Arch-Int, and N. Arch-Int, ‘An adaptive multi bit-plane image steganography using block data-hiding’, *Multimed. Tools Appl.*, vol. 75, no. 14, pp. 8319–8345, 2016.

[15] M. Li, K. Mu, P. Zhong, J. Wen, and Y. Xue, ‘Generating steganographic image description by dynamic synonym substitution’, *Signal Processing*, 2019.

[16] M. A. F. Al-Husainy and D. M. Uliyan, ‘A secret-key image steganography technique using random chain codes’, *Int. J. Technol.*, vol. 10, no. 4, pp. 731–740, 2019.

[17] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, ‘A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image’, *Multimed. Tools Appl.*, 2016.

[18] M. Douglas, K. Bailey, M. Leeney, and K. Curran, ‘An overview of steganography techniques applied to the protection of biometric data’, *Multimed. Tools Appl.*, 2018.

[19] S. Shen, L. Huang, and Q. Tian, ‘A novel data hiding for color images based on pixel value difference and modulus function’, *Multimed. Tools Appl.*, vol. 74, no. 3, pp. 707–728, 2015.

[20] C. C. Chang, Y. H. Chen, and C. C. Lin, ‘A data embedding scheme for color images based on genetic algorithm and absolute moment block truncation coding’, in *Soft Computing*, 2009.

[21] P. Maniriho and T. Ahmad, ‘Information hiding scheme for digital images using difference expansion and modulus function’, *J. King Saud Univ. - Comput. Inf. Sci.*, 2019.

[22] I. R. Grajeda-Marín, H. A. Montes-Venegas, J. R. Marcial-Romero, J. A. Hernández-Servín, V. Muñoz-Jiménez, and G. D. I. Luna, ‘A New Optimization Strategy for Solving the Fall-Off Boundary Value Problem in Pixel-Value Differencing Steganography’, *Int. J. Pattern Recognit. Artif. Intell.*, vol. 32, no. 1, pp. 1–17, 2018.

[23] C.-W. Huang, C. Chou, Y.-C. Chiu, and C.-Y. Chang, ‘Embedded FPGA Design for Optimal Pixel Adjustment Process of Image Steganography’, *Math. Probl. Eng.*, 2018.

[24] E. R. L. Yadav, E. C. Kumar, and E. R. Yadav, ‘High Capacity Embedding And Secured Steganography Model By Using GA And Integer Wavelet Transform’, no. July, 2019.

[25] M. Kaur and M. Juneja, ‘Adaptive Block Based Steganographic Model with Dynamic Block Estimation with Fuzzy Rules’, in *Innovations in Computer Science and Engineering*, Springer, 2017, pp. 167–176.

[26] B. Mondal, T. Mandal, P. Kumar, and N. Biswas, ‘A secure partial encryption scheme based on bit plane manipulation’, *2017 7th Int. Symp. Embed. Comput. Syst. Des. ISED 2017*, vol. 2018-Janua, pp. 1–5, 2018.

[27] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, ‘CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method’, *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 8597–8626, 2017.

[28] I. R. Grajeda-Marín, H. A. Montes-Venegas, J. R. Marcial-Romero, J. A. Hernández-Servín, and G. De Ita, ‘An optimization approach to the TWPVD method for digital image steganography’, in *Mexican Conference on Pattern Recognition*, 2016, pp. 125–134.

[29] S. Rajendran and M. Doraipandian, ‘Chaotic map based random image steganography using LSB technique’, *Int. J. Netw. Secur.*, vol. 19, no. 4, pp. 593–598, 2017.

[30] H. Nyeem, ‘Reversible data hiding with image bit-plane slicing’, *20th Int. Conf. Comput. Inf. Technol. ICCIT 2017*, vol. 2018-Janua, no. December, pp. 1–6, 2018.

[31] R. Kaur and B. Singh, ‘A Hybrid Image Steganography Using Chaotic Maps in DCT Domain’, in *Advances in Intelligent Systems and Computing*, 2020.

[32] D. R. I. M. Setiadi and J. Jumanto, ‘An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection’, *Cybern. Inf. Technol.*, vol. 18, no. 2, pp. 74–88, 2018.

[33] N. Mukherjee, G. Paul, S. K. Saha, and D. Burman, ‘A PVD based high capacity steganography algorithm with embedding in non-sequential position’, *Multimed. Tools Appl.*, pp. 1–31, 2020.

[34] A. ALabaichi, M. A. A. Al-Dabbas, and A. Salih, ‘Image steganography using least significant bit and secret map techniques.’, *Int. J. Electr. Comput. Eng.*, vol. 10, 2020.

[35] K. Karampidis, E. Kavallieratou, and G. Papadourakis, ‘A review of image steganalysis techniques for digital forensics’, *J. Inf. Secur. Appl.*, 2018.

[36] S. A. Seyyedi, V. Sadau, and N. Ivanov, ‘A Secure Steganography Method Based on Integer Lifting Wavelet Transform.’, *IJ Netw. Secur.*, vol. 18, no. 1, pp. 124–132, 2016.

[37] D. A. Huffman, ‘A Method for the Construction of Minimum-Redundancy Codes’, *Proc. IRE*, 1952.

[38] G. Savithri, S. Mane, and J. S. Banu, ‘Parallel Implementation of RSA 2D-DCT Steganography and Chaotic 2D-DCT Steganography’, in *Proceedings of International Conference on Computer Vision and Image Processing*, 2017, pp. 593–605.

[39] S. Sun, ‘A novel edge based image steganography with 2k correction and Huffman encoding’, *Inf. Process. Lett.*, 2016.

[40] M. Raeiatibanadkooki, S. R. Quchani, M. M. KhalilZade, and K. Bahaadinbeigy, ‘Compression and Encryption of ECG Signal Using Wavelet and Chaotically Huffman Code in Telemedicine Application’, *J. Med. Syst.*, 2016.

[41] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, ‘A new adaptive image steganography scheme based on DCT and chaotic map’, *Multimed. Tools Appl.*, vol. 76, no. 11, pp. 13493–13510, 2017.

[42] V. Kumar and D. Kumar, ‘A modified DWT-based image steganography technique’, *Multimed. Tools Appl.*, vol. 77, no. 11, pp. 13279–13308, 2018.

[43] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, 'Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research', *Neurocomputing*, vol. 335, pp. 299–326, 2019.

[44] S. Alam, T. Ahmad, and M. N. Doja, 'A Novel Edge Based Chaotic Steganography Method Using Neural Network', in *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, 2017, pp. 467–475.

[45] M. Islam, A. Roy, and R. H. Laskar, 'Neural network based robust image watermarking technique in LWT domain', *J. Intell. Fuzzy Syst.*, vol. 34, no. 3, pp. 1691–1700, 2018.

[46] D. Jude Hemanth, J. Anitha, D. E. Popescu, and L. H. Son, 'A modified genetic algorithm for performance improvement of transform based image steganography systems', *J. Intell. Fuzzy Syst.*, vol. 35, no. 1, pp. 197–209, 2018.

[47] R. Biswas and S. K. Bandyapadhay, 'Random selection based GA optimization in 2D-DCT domain color image steganography', *Multimed. Tools Appl.*, pp. 1–20, 2019.

[48] I. J. Kadhim, P. Premaratne, and P. J. Vial, 'High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform', *Cogn. Syst. Res.*, vol. 60, pp. 20–32, 2020.

[49] A. Saeed. *Ali asi*, 'An accurate texture complexity estimation for quality-enhanced and secure image steganography', *IEEE Access*, vol. 8, pp. 21613–21630, 2020.