

**FEBRUARY 2018**

**M.Sc. in Electrical and Electronics Engineering**

**AWAB QASIM KARAMANJI**

**UNIVERSITY OF GAZIANTEP  
GRADUATE SCHOOL OF  
NATURAL & APPLIED SCIENCES**

**IMAGE SECURING METHOD USING STEGANOGRAPHY**

**M.Sc. THESIS  
IN  
ELECTRICAL AND ELECTRONICS ENGINEERING**

**BY  
AWAB QASIM KARAMANJI  
FEBRUARY 2018**

**Image Securing Method Using Steganography**

**M.Sc. Thesis**

**In**

**Electrical and Electronics Engineering**

**University of Gaziantep**

**Supervisor**

**Assoc. Prof. Dr. Sema KAYHAN**

**By**

**Awab Qasim KARAMANJI**

**February 2018**



© 2018 [Awab Qasim KARAMANJI]

REPUBLIC OF TURKEY  
UNIVERSITY OF GAZIANTEP  
GRADUATE SCHOOL OF NATURAL & APPLIED SCIENCES  
ELECTRICAL AND ELECTRONICS ENGINEERING

Name of the thesis: Image securing method using steganography

Name of the student: Awab Qasim KARAMANJI

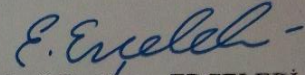
Exam date: Feb 23, 2018

Approval of the Graduate School of Natural and Applied Sciences



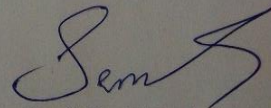
Prof. Dr. Ahmet Necmeddin YAZICI  
Director

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



Prof. Dr. Ergun ERÇELEBI  
Head of Department

This is to certify that we have read this thesis and that in our opinion; it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.



Assoc. Prof. Dr. SEMA KAYHAN  
Supervisor

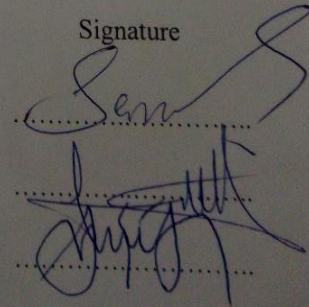
Examining Committee Members:

Assoc. Prof. Dr. Sema KAYHAN

Prof. Dr. Nuran DOGRU

Assoc. Prof. Dr. Kemal DELIHACIOĞLU

Signature



**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.**

**Awab Qasim KARAMANJI**

## **ABSTRACT**

### **IMAGE SECURING METHOD USING STEGANOGRAPHY**

**KARAMANJI, Awab Qasim**

**M.Sc. in Electrical and Electronics Engineering**

**Supervisor: Assoc. Prof. Dr. Sema KAYHAN**

**February 2018**

**58 Pages**

One of the most important factors of information technology and communication is the security of the information. This thesis presents and compares two main steganography techniques; quad-tree based steganography and peak-valley methods. The quad-tree algorithm can be considered as an improved version of the traditional histogram shifting method. The peak-valley algorithm uses the advantage of simple local distribution of pixel intensities and utilizes the zero or the minimum points of the histogram of an image. The method slightly modifies the pixel grayscale values to embed the data into the image. It can embed more data than many of the existing reversible data hiding algorithms. The performance of the presented methods, in terms of imperceptibility, the embedding rate ranges from 200 to 1000 bytes, whenever six variants images are employed as cover images. The results have revealed that the imperceptibility for both algorithms is almost identical whereby, the PSNR decreases as the embedding rate increases. The PSNR was 44.2092 dB when the embedding rate was 200 bytes and gradually decreased as embedding rates increased. Furthermore, the PSNR of Peak-valley is higher than that of Quad-tree with the embedding rate ranges from 200 to 1000 .In addition, Chi-Square attack is performed on the stego image, produced by the presented algorithms to measure the robustness of the methods. The test reveals that the probability of containing secret message is almost zero for the entire test which indicates that, there is no hidden message inside the cover image.

**Key words:** Embedding capacity maximization, Histogram, PSNR, Reversible data hiding

## ÖZET

### STEGANOGRAFI KULLANARAK GÖRÜNTÜ GÜVENLİK YÖNTEMİ

**KARAMANJI, Awab Qasim**

**Yüksek Lisans Tezi, Elektrik-Elektronik Müh. Bölümü**

**Tez Yöneticisi: Doç.Dr. Sema KAYHAN**

**Şubat 2018**

**58 Sayfa**

Bilgi teknolojisinin ve iletişiminin en önemli unsurlarından biri, bilgi güvenliğidir. Bu tezde, iki ana steganografi tekniği sunulup karşılaştırılmıştır bunlar; dörtlü tabanlı steganografi ve tepe vadi yöntemleridir. Dörtlü ağaç algoritması, geleneksel histogram kaydırma yönteminin geliştirilmiş bir versiyonu olarak düşünülebilir. Zirve-Vadeli algoritma, piksel yoğunluğunun basit yerel dağılım avantajını kullanır ve bir görüntünün histogramının sıfır veya minimum noktalarını kullanır. Yöntem, veriyi görüntüye gömmek için piksel tonlama değerlerini az miktarda değiştirir. Bu algoritmalarla mevcut geri çevrilebilir veri gizleme algoritmalarının çoğundan daha fazla veri gömülebilir. Sunulan yöntemlerin performansı, algılanamazlık açısından, örtme görüntüleri olarak altı çeşit görüntü kullanıldığında, gömme oranı 200 ila 1000 bayt arasında değişmektedir. Sonuçlar, her iki algoritmanın algılanamazlığının hemen hemen aynı olduğunu ortaya koydu. Algoritmanın gömme oranı arttıkça PSNR değeri azalmaktadır. Gömme oranı 200 bayt olduğunda, PSNR 44.2092 dB olup, gömme oranları arttıkça bu değer kademeli olarak azalmaktadır. Ayrıca, Tepe-Vadinin PSNR değeri, dörtlü tabanlı steganografi algoritmasından, 200'den 1000'e kadar olan gömme oranı için daha yüksektir. Buna ek olarak, sunulan algoritmaların sağlamlığını ölçmek için üretilen stego görüntülerine kare saldırısı testi gerçekleştirilmiştir. Bu test, gizli mesaj olma ihtimalinin tüm test için neredeyse sıfır olduğunu yani kapak görüntüsünün içinde hiçbir gizli mesaj olmadığını ortaya koymuştur.

**AnahtarKelimeler:** Gömme kapasitesi maksimizasyonu, Histogram, PSNR, Tersinir veri gizleme

## **ACKNOWLEDGEMENT**

I express my sincere gratitude to my supervisor Assoc. Prof. Dr. Sema KAYHAN for his perfect guidance and invaluable advice during this research. It was my pleasure to work under his supervision. I would not have been able to complete this work without his guidance and direction.

I would like also to thank the most special person in my life, my mother, without her support this research project would not have been possible.

My sincere appreciation also extends to my sister, brother and all my friends and to those gave me the delight of smile.



## TABLE OF CONTENT

	Page
<b>ABSTRACT</b> .....	<b>v</b>
<b>ÖZET</b> .....	<b>vi</b>
<b>ACKNOWLEDGEMENT</b> .....	<b>vii</b>
<b>TABLE OF CONTENT</b> .....	<b>viii</b>
<b>LIST OF FIGURES</b> .....	<b>x</b>
<b>LIST OF TABLES</b> .....	<b>xii</b>
<b>CHAPTER 1</b> .....	<b>1</b>
<b>INTRODUCTION</b> .....	<b>1</b>
1.1    General .....	1
1.2    Statement of the Problem .....	4
1.3    Purpose of thesis.....	5
<b>CHAPTER 2</b> .....	<b>6</b>
<b>LITERATURE REVIEW</b> .....	<b>6</b>
2.1    Introduction .....	6
2.2    Technical overview of steganography concept .....	8
2.3    Review on Encryption technique used with Steganography .....	13
2.4    Attacks on Steganography .....	15
2.5    Statistical analysis of pairs of values (histogram analysis) .....	16
2.5.1    Chi-squared attack (%2 method).....	16
<b>CHAPTER 3</b> .....	<b>24</b>
<b>RESEARCH METHODOLOGY</b> .....	<b>24</b>
3.1    Introduction .....	24
3.2    Proposed .....	24
3.2.1    Algorithm Quad Tree .....	25
3.2.2    Peak-valley method.....	35
<b>CHAPTER 4</b> .....	<b>40</b>
<b>RESULTS AND DISSCUSION</b> .....	<b>40</b>
4.1    Introduction .....	40
4.2    Dataset .....	41
4.3    Imperceptibility Result of the Proposed Method.....	42

<b>CHAPTER 5</b> .....	<b>50</b>
<b>CONCLUSION AND FUTURE WORKS</b> .....	<b>50</b>
5.1 Introduction .....	50
5.2 Summary of the work .....	50
5.3 Future Work.....	52
<b>REFERENCES</b> .....	<b>53</b>



## LIST OF FIGURES

	Page
<b>Figure 1.1</b> Image Steganography System.....	1
<b>Figure 1.2</b> Information security techniques. ....	3
<b>Figure 1.3</b> Image-based steganography.....	4
<b>Figure 3.1</b> Flowchart of the Proposed. ....	24
<b>Figure 3.2</b> Flowchart of the Quad-tree. ....	25
<b>Figure 3.3</b> Quad-tree indexing. ....	27
<b>Figure 3.4</b> Steps of the Data Hiding Process.....	28
<b>Figure 3.5</b> Quad-tree Segmentation Process. ....	29
<b>Figure 3.6</b> Quad-tree partition.....	30
<b>Figure 3.7</b> Quad-tree Structure of the Partition.....	31
<b>Figure 3.8</b> Quad-tree Partition Example for Lena. ....	31
<b>Figure 3.9</b> The Structure of Overhead1.....	32
<b>Figure 3.10</b> Flow Procedure of the Embedding Algorithm. ....	33
<b>Figure 3.11</b> A sequence of steps is performed of an algorithm. ....	34
<b>Figure 3.12</b> Data Embedding Algorithm.....	35
<b>Figure 3.13</b> The main idea in Ni et al.'s algorithm. (a) It can be a reasonable example of histogram with a peak point and a valley point. (b) Shift the interval (p, v) to the right by a unit. (c) The data and the positions with gray levels p and p + 1 were embedded. ....	36
<b>Figure 4.1</b> Dataset (a) Baboon, (b) Lena, (c) Peppers, (d) Barbara, (e) tiffany, (f) Airplane. ....	42
<b>Figure 4.2</b> Performance of the proposed method when Peak-valley of Lena image. ....	45

<b>Figure 4.3</b> Performance of the proposed method when Quad-tree of Lena image. . .	46
<b>Figure 4.4</b> Results for Chi-Squared attack on original Lina image.....	46
<b>Figure 4.5</b> Results for Chi-Squared attack on Lena stego-image that has been embedded by the proposed method using peak-valley and tested on 200 bit of the secret message.....	47
<b>Figure 4.6</b> Results for Chi-squared attack on Lena stego-image that has been embedded by the proposed method using quad-tree and tested on 200 bit of the secret message.....	48
<b>Figure 4.7</b> Results for Chi-squared attack on Lena stego-image that has been embedded by the proposed method using peak-valley and tested on 1000 bit of the secret message.....	48
<b>Figure 4.8</b> Results for Chi-squared attack on Lena stego-image that has been embedded by the proposed method using quad-tree and tested on 1000 bit of the secret message.....	49

## LIST OF TABLES

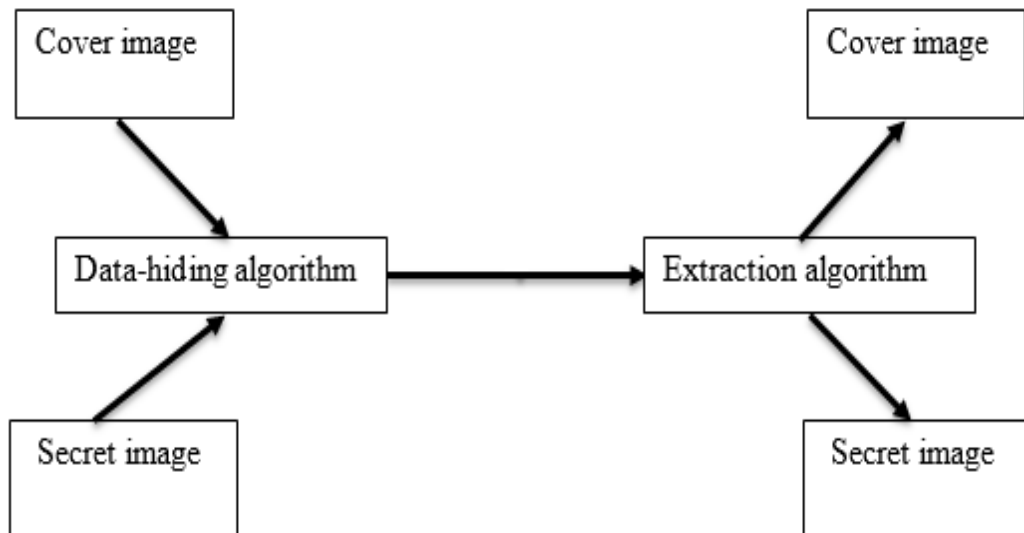
	<b>Page</b>
<b>Table 2.1</b> Summary of Literature review on Steganographic Techniques .....	17
<b>Table 2.2</b> Summary of literature survey on Encryption techniques used with Steganography .....	22
<b>Table 3.1</b> Description of overhead1 .....	32
<b>Table 4.1</b> Results of the proposed method of Lena image .....	43
<b>Table 4.2</b> Results of the proposed method of Baboon image.....	43
<b>Table 4.3</b> Results of the proposed method of Tiffany image .....	43
<b>Table 4.4</b> Results of the proposed method of Peppers image .....	44
<b>Table 4.5</b> Results of the proposed method of Barbara image .....	44
<b>Table 4.6</b> Results of the proposed method of Airplane image .....	44

# CHAPTER 1

## INTRODUCTION

### 1.1 General

The steganography techniques aimed at secretly hiding information in a multimedia system carrier like text, audio, and video, also, this technique does not raise any suspicion of change to its contents. The authentic carrier is indicated by the cover object. During this work, we will concentrate on image steganography. Subsequently, the term cover object now turns into a cover image. Figure 1.1 illustrates a basic information of hiding system in which the embedding technique takes a cover image and a secret image as inputs and produces as output a stego image, which is the seemingly does not change the cover image with the embedded data. The stego image may be sent over the communication links to the receiver who can then carry it out the extraction procedure to retrieve the secret message from the stego image.



**Figure 1.1** Image Steganography System.

Steganography and Cryptography are techniques use to operate the information to hide it. For security reason, a lot of approaches has been created while the main objective of all approaches is to secure the data and be sure it has been reached safety without being detected. The word Steganography has been translated from Greek origin [1].

As the fast growing of technology these days and especially the growing of the network and internet which let everyone to be able to share everything in easiest way in many different applications, and for protecting this information, many security approaches or methods developed and applied like encryption or steganography.

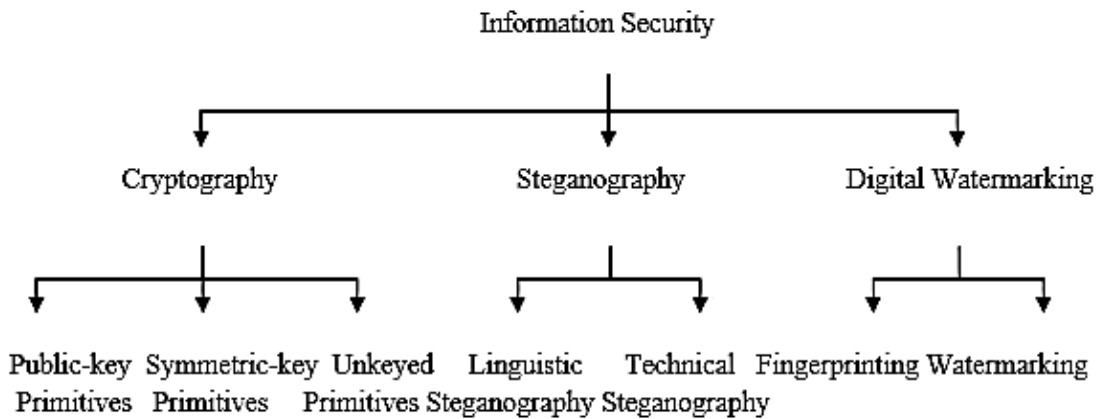
Cryptography is a science of utilizing mathematics to encrypt and decrypt information to keep messages secured by converting intelligible information type (plaintext) into the unintelligible type (ciphertext). The word "cryptography" has come from the Greek word 'kryptós' standing for 'hidden' and 'gràphin' standing for 'writing'. Therefore, the appropriate meaning of cryptography is 'hidden writing' [2, 3]. Each cryptosystem consists of plaintext, encryption algorithm, decryption Ciphertext, algorithm, and Key. Plaintext is message or information that are in their normal, legible (not encrypted) type. Encryption is the method of transforming plaintext to ciphertext via using a key. Ciphertext results from encryption via applying the encryption key in the plaintext. Decryption is that the method of retrieving the plaintext back from the ciphertext. The Key has utilized the information to dominance the cryptosystem (cipher system), and it's known via the sender and receiver solely [2, 4]. Whereas cryptography is incredibly important for securing information; the cryptanalysts might success to break the ciphers via analyzing the contents of ciphertext to get back the plaintext [2].

There are many different kinds of steganography:

- Audio and video steganography: It is a technique used to hide information while sending video data and for audio as well.
- Text steganography: is the most important method in steganography.
- Image steganography: this method has thesis worked on it and it will be explained in next chapters in details.

The differences between Steganography and Cryptography is in the way they work and evaluate. For example, the Cryptography crashes when someone attacks and detects that there is a secret combination in the medium, while Steganography crashes or stops when someone gets access to the content of the secret message [5].

The Figure below 1.2 shows main parts of the information security techniques [6].



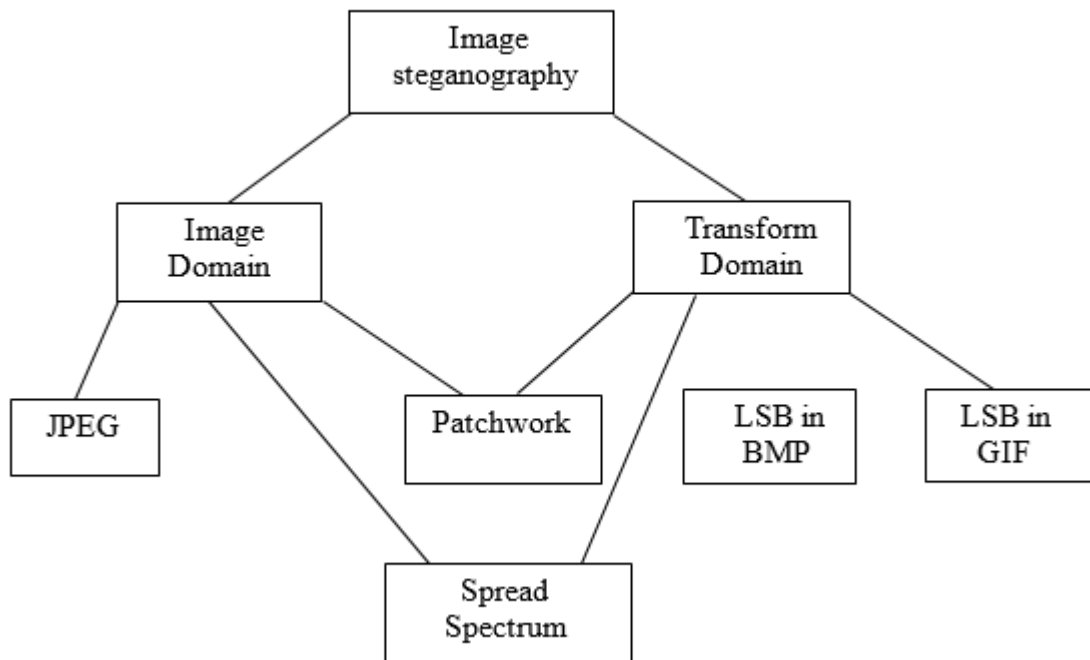
**Figure 1.2** Information security techniques.

The main structure of Steganography is three components:

- Carrier image.
- Secret Image.
- Key

Image Steganography is divided into Image Domain Steganography and Transform Domain Both types of Steganography is divided into subclasses as shown in figure1.3 given below.





**Figure 1.3** Image-based steganography.

Image domain also identified as spatial domain approaches insert data in the pixels straightly. Image domain Steganography based on bit-wise techniques that operate noise manipulation and bit insertion. Occasionally it is categorized as simple schemes. The image formats that are furthestmost applicable for image domain Steganography are lossless Steganography and the methods are generally reliant on the image format. Transform domain to identify as frequency domain Steganography techniques. In this technique, images are primary transformed and then the data is injected into the image. Transform domain Steganography includes the manipulation of image transforms and algorithms.

## 1.2 Statement of the Problem

Description of the Problem: The technique of information hiding has taken much attention in the modern years as the security of information has been a massive concern in this internet area. Despite, message sending by the Internet has some problems, like information security, copyright protection, and so on. Therefore, we need a secure communication method to send messages through the Internet. Steganography is a method that hides secret data inside cover media through modifying its insignificant

components so that an unauthorized user will not be conscious of the existence of the secret data.

### **1.3 Purpose of thesis**

The main purpose of Steganography is to hide data in a cover media so that others will not be able to notice it. In this thesis, the algorithm for image steganography has been proposed to hide a large amount of secret data conferred via secret image, three important requirements will be considered when evaluating a study scheme: data embedding rate, which is aimed to develop steganography technique which has a high capacity and to be undetectable.

In this thesis two different algorithms for Reversible Data Hiding proposed by “Quad-tree “ and “ Peak-valley“ implemented . The performance of the algorithms are evaluated using the peak signal to noise ratios (PSNRs) after embedding data

## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Introduction

The term steganography is gotten from the Greek words indicating protected writing. Before simple and advanced advances, correspondence required the physical transportation of articles amongst parties and stego-frameworks were centered on concealing data in these items secretly.

Steganography is first recorded to have been practiced through the Golden Age in Greece utilizing wax plates [7]. The wax will be dissolved away, the message would be carved within an underlying timber and after that secured again utilizing a new layer of wax giving the form of another, a fresh wax tablet that could be naturally transported. In a comparable way, a Roman sovereign Histiaëus utilized slaves to transmit secret information by shaving their heads and inking messages into their scalp [7]. Directly, when the hair gets back to its level, the slave would move to the wanted beneficiary and he shaves again his head when arriving to show the information. Later amid the fourteenth century, a few artists encoded hidden messages into their work as an interesting mark; for instance the Italian writer and author Boccaccio encoded poems into his writing as starting letters in the work [8]. In the sixteenth century, an Italian Renaissance mathematician called Jérôme Cardin [9] suggested a matrix that permitted the letters of a secret message to be realized from the seemingly-unrelated content by putting the grid over the content which would cover certain letters uncovering the secret message.

Steganography became principally valuable through wartime; for instance, [10] suggested the notable strategy of microdots utilized as a part of many fights during the nineteenth and twentieth century time. The thought was to shorten the secret message to the size of a speck of dirt that must be understood under high amplification.

The little topics were covered up in noses, ears or between fingertips and in the sides of postcards. Another, later stego-system utilized undetectable inks [9], the first was with natural fluids, for example, milk, pee or vinegar diluted in a nectar or sugar solution. The message written in this ink was hidden once the paper had dried, however, the planned beneficiary could recover the message by warming the paper. As another case, [11] proposed a steganographic standard where information is covered up in content archives by somewhat moving the lines of content up or down  $1/300$  of an inch. These delicate changes are not outwardly perceptible however they survive photocopying, enabling the message to be extracted regardless if the documents have been transcribed.

Until the early 1900s, steganography was utilized fundamentally via spies and the stego-systems were smart tricks such as the ones talked about above, with few theoretical fundamentals. With the transition of communication from analog to digital, steganography has encountered a renaissance and is now at present technical and mathematical. In the late 1990s, digital watermarking controlled research [12] because of numerous lucrative applications such as secure media distribution and authentication. With this attention, came moreover research into steganography, individually after concerns were raised that it may be utilized by culprits.

More lately, the fast growth of the Internet-connection with high bandwidth and low-cost PC hardware has driven to the rapid development of a media-sharing culture, as presented previously. That increase in digital data sharing and transport over the Internet, connected with the seemingly limitless size of content that can be uploaded, has given immense potential to covert communication. With respect to steganography specifically, information can be hidden in digital media like text, images, video, and audio. Since electronic communication is liable to eavesdropping, security and privacy are more important today than ever. Stego-systems are likewise becoming frequently compact and neat, with new attention in implementation them on mobile and embedded devices, particularly cellular phones. In [13], the authors display outcomes suggesting how steganography is utilized in mobile phones and tablets. Providing digital media objects could likewise be utilized to store malicious information like viruses [14] or that it is suspected to be utilized via terrorists to distribute data [15], research into steganography is significant not just to develop more robust data-

transferral techniques but likewise to increase the capacity to detect techniques developed via the enemy.

## **2.2 Technical overview of steganography concept**

Prashanti and K. Sandhyarani [16] both of them were completed many survey upon new implementations of LSB which was based image what so called steganography. Authors, in this article, talks about the implementations which helped in enhancing the steganographic results like high robustness, embedding capacity in addition to undetectability of the concealed data. This survey was added to two new techniques which were introduced, too. The first one used to the data in secret way inside the covers images and the second one utilized to secret grayscale within different grayscale one. There are four state tables which give pseudo random number and utilized to secret data embedding. They contain both techniques which are larger security that because the secret information was hidden on accidental that chosen location of LSBs for an image in addition to the pseudo helping arbitrary characters which delivered by the table.

Savita Goel et al. in [17] another technique for implanting mystery messages was presented in cover picture by utilizing LSB strategy in different movements. Authors make comparison of a stego image resolution of in respecting to the images cover by utilizing many images of resolution characters for instance Mean Square Error (MSE), histograms, Peak Signal to Noise Ratio (PSNR), and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). The results of theirs, namely, study and experimental refers to the suggested strategy which was more quick, highly and efficient as compared to the first one, in other words, the basic LSB methods.

Della Baby et al. [18] a "Novel DWT based Image Securing technique was proposed by utilizing Steganography". A new steganography technique has been found in their work and introduced in which various RGB image that is embedding within the separate RGB image by utilizing technique of DWT steganography. Using their method, three colors were given to the image cover spaces which were utilized because of hiding secret information. Many experimental ones have been got by utilizing corresponding system of good robustness. Estimation of PSNR and SSIM list were utilized by its creators by looking at unique cover picture and the nature of stego

picture. The present strategy contains a decent level of PSNR and SSIM file esteems. It can be said that the result of empirical work was best when compared existing methodologies by authors and have increased embedding capacity the reason is compressing of information. The comes about that general security of their approach will be huge including few detectable differences in the stego picture. Bingwen Feng, Wei Lu, and Wei Sun in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture" [19] A best in class approach of double picture steganography was purposed by the previously mentioned . The strategy proposed to limit the mutilation upon the surface. At the starting of this stenographic process of is the turn, supplement, in addition, invariant reflecting texture patterns have been taken from the image of the binary system.. In addition to that, they suggested a measurement and according to this purposes measurement. The mentioned procedure had gradually implement. Pragmatic outcomes demonstrate that suggested methods of steganography have large factual security with large stego picture resolution and large inserting limit. M. Nusrati et al. [20] was completed many studies upon a genetic heuristic algorithms according to a steganographic technique for protecting secret data in an image cover. Thus then again, ideally finds the fitting areas in cover picture to implant the concealed data by focusing on the "before inserting concealing procedures". It tries to roll out slightest improvements in the bits which prompt negligible alterations in picture histogram. To incognito the LSBs or mystery message to set of pieces, division is done in this hereditary calculation. After this calculation, it has discovered the suitable areas for implanting, the mystery pieces were installed and it produced the key record which utilized amid message extraction process.

Kazem Qazanfarei and Reza Safabakhsh [23] a enhanced adaptation of LSB++ method was proposed. In this, they enhanced LSB++ and they influence qualification among touchy pixels and they to permit shielding them from installing of additional bits, which gives in bring down contortion in the co-event frameworks. They created it to safeguard DCT coefficients of JPEG arrange pictures. This outcomes in less follows in the co-event frameworks thus ancient process of LSB++. It is additionally secured from the histogram based assaults since it doesn't roll out any improvements in the histogram and thus, histogram of two cover picture and stego picture will be same. As a result of disposal of additional piece implanting, the nature of stego pictures is likewise high.

On the in view of Huffman Coding, Amitava Nag et al. [24] a different steganographic procedure of LSB substitution was introduced. Theirs, strategies, essentially concentrates on high security, bigger inserting limit and worthy stego levels of picture resolution. The first, Huffman tree is created to encode each byte of mystery picture. Next encoding them, they partition the encoded bits into four sections and have 0 to 3 decimal esteems. Area of inserting a message in cover picture was dictated by those decimal esteems. They demonstrate that it is extremely troublesome for assailant to remove the mystery data in light of the fact that Huffman table diminishing the extent of the cover picture, to be specific, test comes about. Purposed procedures simply have satisfactory stages of PSNR esteems and lye among 32 dB to up 33.

N. Akhtar et al. in [25] the enhanced adaptation of customary LSB picture steganography strategy were displayed and actualized. Their work upgrades the nature of stego picture utilizing bit reversal strategy. Notwithstanding that they proposed two methodologies of bit reversal systems. The two, procedures settle around bit reversal strategies in which LSBs of pixels of transporter picture are altered just and just on the off chance that they emerge with particular example of pixel's bits. This prompts minor alteration in pixel was contrasted with customary LSB technique. For adjust recovery of mystery message, rearranged bits should be installed some place inside the stego picture. They, trial comes about, exhibit that PSNR estimation of stego picture has turned out to be made strides.

P. U. Deshmuk et al. [26] the edge versatile steganography in light of LSB substitution has been introduced. They implant mystery data in sharp (edges) areas of the bearer picture by utilizing versatile plan and distinction amidst the two adjoining pixels of transporter picture. The method performs superior to anything different keeps up the nature of stego picture and LSB and Pixel contrast based systems.

E. Dagar and S. Dagar [27] the steganography system for shading RGB pictures to enhance the security level of information exchange through the web was exhibited. It is 24 bit RGB picture, used as cover picture to install concealed information in many hues, for example, reddish, greenish and blue pixel. X-Box mapping and a few boxes include 16 unique esteems. Here "X" speak to any total range from 1 up to 10. After propositions esteems spared in X-Boxes, they are mapping with LSBs of bearer picture. It is not easy for the assailant for extracting the data in secret and the reason is to make

use of mapping. The mapping has provided it in high level of security to hidden information.

M. R. Modi et al. [28] a novel steganography strategy to install mystery data of LSBs of cover picture was proposed. In their technique in any event there are two noteworthy bits of edges are used to store mystery message as edge locales are great ranges to implant the mystery data than other smooth districts of cover picture. In this strategy edge locale are identified on premise of measure of mystery data, which implies it does versatile edge discovery. Test comes about examination demonstrates that their strategy performs superior to customary LSB picture steganographic strategies and has more noteworthy security against visual pasting.

D. Samidha and D. Agrawal [29] in those study article "Arbitrary Image Steganography in Spatial Domain" investigate about different image steganographic strategies and proposed an LSB based steganography technique utilizing irregular bit choice. In their methods, the inadequate importance bit is chosen arbitrarily for embedding the hidden information in the image cover. They likewise proposed some more methods in light of irregular pixels of the cover image and secret data is embedded in a randomly chosen bit of arbitrary pixels, Intensity amount, the pixel space, etc. Parameters are utilized for this reason.

In [30] researcher suggests an improved LSI algorithm for image steganography. In this suggested research they just implant secret data in blue part of the RGB color space. In their method, they select the first  $M \times N$  size cover image. After determination of cover image just blue part is utilized for inserting secret data. They likewise make utilization of pixel filter to get to the best districts to embed data in the cover image to get an ideal rate. Empirical results confirm that the method used decreases the distortion level of cover image and stego, in addition, the image proves pretty great visional quality and differences in cover image are careless to Human Visional System (HVS). The mentioned method can decrease the leap in color scale that because just blue parts are applied to embed the secret data.

S. Sachdeva and A. Kumar [31] tried to embed the secret data by vector quantization table. They perform a new technique of steganography called as JMQT according to adjusted QT (Quantization Table). They additionally contrast their proposed approach and JPEG-JSteg steganography strategy. Embedded capacity or stego image measure



are utilized as execution analyses parameters and empirical results are likewise contrasted with JPEG-JSteg technique. Empirical results proved that the private capacity and stego size get more increment. Consequently, JMQT system has enough capacity while JPEG-JSteg has better stego-size.

S. M. M. Karim et al. [32] suggested a new method that gives very good security to secret information. They utilize LSB method with the secret key. This mystery key is used to conceal the touchy information and this information is put away on different LSB bits of the picture. This steganography method use RGB genuine nature pictures for implanting operation. This strategy inserts the mystery information inside in LSB of the cover picture and mystery key is used to scramble the mystery information to keep away from sidestep get to. Depending on the secret key utilized, secret data is randomly stored in a various location of LSBs of the cover image which make this system sturdier and make hard for an attacker to an extractor the hidden secret data. Preliminary results represent that this technique generates perfect PSNR value and supply greater security to hidden data than conventional LSB based steganographic technique.

On the bases of Human visual system (HVS) X. Qing et al. [33] suggested a new method in which sensitive data is embedded in all levels of RGB components of an image. In this method, multiple plan-bit is utilized with adaptive nature of data hiding algorithm. This suggested technique has high embedding capability than traditional LSB technique and low computational difficulty. The suggested system also has a great quality of stego image.

Che-Wei Lee and Wen-Hsiang Tsai in [34] suggested a unique strategy of steganography that utilizes PNG image to hide data secretly. Shamir's strategy to secret shared was used to product fractional shares from the presented information series including an assistance some of polynomial's coefficients as information carrier for registering the shares. These partial offers are then installed into Alpha channel (clear areas) or create the stego picture that had been repetitive sound. The little prime number could be utilized to reduce the white noise. The suggested technique has successful information limit of concealing information with help security level and stego picture quality.

H. Yang et al. [35] presented another reconciling LSB based technique for image steganography. It utilizes the pixel adjustment method for best stego image quality. This adaptive LSB substitution leads to in high hidden capability. In [36] LSB based image steganography technique is suggested. To hide the information common bit pattern is utilized. According to the message and therefore the pattern bits LSB's of pixels are adjusted. This method has a low hidden capability.

### **2.3 Review on Encryption technique used with Steganography**

This segment covers a part of investigations that utilization both cryptographic and steganographic procedures in order to pick up the additional layer of security to the concealed data.

D. Debnath et al. [37] recommended a security conspire in which steganography is used alongside cryptography to supply better security to implanted data. In their procedure in the first place, data is encoded when it is implanted into cover picture using steganographic strategy. The recommended calculation changes over a message into content with the help of control tables, and afterward performs slope figure procedures to it and finally shrouds the data into green, blue, and red pixels of the cover picture. They use different picture quality parameters like NAE, AD, PSNR, SC, and MD.

D. E. M. Ahmed and O.O. Khalifa in [38] show a strategy in which LSB picture steganography is utilized alongside Elliptic Curve Cryptography (ECC) to offer more noteworthy security to information. In the proposed work sender is permitted to pick an appropriate cover picture and mystery data. In this procedure mystery data is first encoded utilizing elliptic bend cryptography and afterward this figured mystery data is implanted into cover picture utilizing slightest critical piece picture steganography technique.

Nouf A. Al-Otaibi et al. [21] designed a unique system named 2-layer security system for protecting the sensible data on pc. They sectioned the system in two-layers to be specific cryptography layer and steganography layer. For steganography layer, LSB algorithm is utilized and for cryptography layer, AES calculation is used. This system is designed on the visual basic platform. Researchers had also perform a study on developing hidden capacity by conducted several analyses. They use one- two bit of LSB to embed a secret message in the cover image. 30 various kinds of fixed size

images are employed in their research to investigate the data dependence and the method security. They found that the impact of 1LSB and 2LSB is negligible in stego image while with 3LSB to 7LSB the image is deformed to obvious levels and have slightly quality of stego image which isn't perfect for image steganography.

M. R. Islam et al. [22] suggested a brand new enhanced form of LSB picture steganography in light of proficient separating technique using status bit. Proposed work likewise utilize AES calculation for encryption demonstrating extra layer of security. In their work bitmap pictures are utilized due to of their uncompressed nature and bitmap pictures are more met all requirements for LSB based steganography. In this methodology first mystery data is encoded using AES calculation and after that this scrambled data is inserted into picture using steganographic process. Enhanced steganographic strategy is recommended which can install more mystery information using separating based calculation and for the sifting reason MSB of bitmap picture is utilized. Proposed work likewise makes usage of status bit for checking inclusion and extraction of mystery messages. Experiential outcomes exhibit that this procedure has high inserting ability than basic LSB calculation. PSNR esteems are moreover high due of high stego picture quality. All the observational results exhibit that this strategy is more practical than ordinary LSB framework for hiding the information in bitmap pictures.

S. Krishnagopal et al. [39] suggested a way as entire that comprises features of two steganographic and cryptographies. These produce utilization of Chaos founded cryptographic techniques for evolving encryptions algorithm. Scattered calculated or feline guide is utilized as a reason for these picture encryption calculation. In their technique of image encryption, the secret key is changed after encrypting all pixels for the picture within the employment of Arnold's Cat map. These ideas of modifying secret key after encryptions gives this structure more powerful versus different assaults. In the following stage, encrypted image is installed into covering picture utilizing steganography. Emulation outputs were performed based on any parameter such as SSIM average or PSNR. Result disabled that their framework has 0.981 SSIM normal esteem and 47.71 dB PSNR. So it produces the pretty great resolution of stego image, what's more, it is more common sense and secure against assaults and can be connected for real-time picture encryption and transmission.

S. Song [40] et al. suggested a really imaginative framework that will join the steganography and cryptography into one framework. There will be no different estimates for cryptography or steganography. Therefore this method requires minor estimates than existing strategies while keeping up the higher security levels center of this framework is LSB coordinating method and Boolean capacity within current figures. For steganography, dim layer pictures are used and Boolean capacities were connected for a cryptographic reason or to check the counterfeit-arbitrary augmentation and decrement of LSBs. Trial comes about demonstrates that this framework is particularly more secure from steganalysis assaults.

## 2.4 Attacks on Steganography

Steganography aims at providing a non-mistrust environment on transmission of a hidden message, which means if doubt arises its goal is not achieved and steganalysis ensures the discovering and rendering useless the covert messages. The person who applies this analysis is called the steganalysis or attacker. Hidden information are exposed to attacks and analysis of different forms such as detecting, extracting, disabling hidden information in addition to confusing them (counterfeiting or overwriting by an attacker, embedding counter information over the existing hidden information). Special attention should be given to attackers during the design of a steganography scheme. The attackers are classified depending on their capacities, they may be passive or active.

1. **Passive Attackers:** The media property of a digital media is altered or corrupted when we attempt to hide message in them, which sometime might be perceptible. This usually forms the bases for detecting the hiding information and the passive attacks of steganalysis involve the detection of these characteristics and signatures.
2. **Active Attackers:** These attackers can alter cover at the period of communication process but cannot change the cover and its meaning. However, this negligible change still keeps the original and modified cover perceptually or semantically similar.

## 2.5 Statistical analysis of pairs of values (histogram analysis)

The processing of embedding message bit in Steganography scheme can be in a sequentially or in a random approach and the message bit are selected independently of the image content. Even though the image has uniform color areas, the hiding data can still be detected after preprocessing the stego-image by plotting a bit-plane such as LSB plane and checking the bit plane. When a message is sequentially embedded in the image, people can guess the existence of steganographic messages in an image. [41] Argued that, it is impossible to differentiate noisy images from the stego-image by applying the above technique, though visual attacks are simple but hard to automate and have questionable reliability. [41] A statistical attack on any strganographic scheme is established. It is able to flip stable value pairs into each other to embed bits of message. For example, pixel values, quantized DCT coefficient, or palette indices that differ in the LSB can form (PoVs). There is an unequal allocation of the two values before embedding in the cover image and after message embedding. The value occurrences in every pair tend to be equal. It depends on the length of the message. If swapping one value into another will not alter the sum of color occurrence in the image, we can design statistical Chi-square test by using this concept and also test for the statistical significance with the mind that the value of occurrence is the same in each pair.

### 2.5.1 Chi-squared attack (%2 method)

The chi-square attack [42] can be employed in any steganogrp hic scheme with which a fixed set of Pairs of Values (PoVs), or other fixed groups of values, are flipped into each other to embed message bits. The idea of the Chi-square attack is by using the stego-image can be compared theoretically expected frequency distribution with the observation distribution to check if there is any changing inside the image [41]. By this comparison the attacker can easily compute the probability of containing secret information in the image. Let us assume that the palette colors  $c_0, c_1 \dots c_{P-1}$  are already sorted as in equation 2.14. Since  $P \leq 256$ , we have at most 128 (PoVs). For the  $i$ -th pair  $(c_{2i}, c_{2i+1})$ ,  $i = 1 \dots 127$ , we define  $n_i' = 1/2$  (number of indices in the set  $\{c_{2i}, c_{2i+1}\}$ ) and  $n_i =$  number of indices equal to  $c_{2i}$ . The value  $n_i'$  is the theoretically expected frequency if a random message has been embedded, and  $n_i$  is the actual number of occurrences of color  $c_{2i}$ . We can now perform the Chi-square test for the equality of

$n_i'$  and  $n_i$ . The number of bits one and zero for pixels of the stego-image is equal or almost equal when the embedding process used the least significant bits for the embedding.

$$E = (c\pi(0), c\pi(1)), (c\pi(2), c\pi(3)), \dots (c\pi(P-2), c\pi(P-1)) \quad (2.1)$$

In addition, this attack is not only able to determine where a message has been embedded, but also calculates the length of the message [43].

**Table 2.1** Summary of Literature review on Steganographic Techniques

Ref. No.	Year	Author(s)	Name	Description
[16]	2015	G. Prashanti and K. Sandhyarani.	“A New Approach for Data Hiding with LSB Steganography”	Authors have done survey on recent achievement of LSB based image steganography and discuss the enhancements done to improve current LSB based steganographic methods. They also proposed two new steganographic techniques.
[17]	2015	Savita Goel et al.	“Image Steganography – Least Significant Bit with Multiple Progressions”	New embedding technique is Proposed that use LSB method with different progression. Experimental results show that proposed method is fast and highly efficient as compared to traditional LSB method.
[18]	2015	Della Baby et al.	“A Novel DWT based Image Securing method using Steganography”	New method has been proposed in which multiple RGB images are embedded into single RGB image using DWT. Proposed system has high embedding capacity and security with minimal changes in stego image.

[19]	2015	Bingwen Feng et al.	“Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”	Authors presented a very latest approach of binary image steganography. This technique reduces the distortion on the textures. They also proposed a measurement scheme. They have concluded that their method has high statistical security with high data hiding capacity.
[20]	2015	M. Nusrati et al.	“Steganography in image Segments using Genetic Algorithm”	They present a new approach based on heuristic genetic algorithm, which optimally find the appropriate locations in cover image to hide data. Simulation results show that their method is more efficient than traditional LSB based method.
[23]	2014	K. Qazanfari and R. Safabakhsh	“A new steganography method which preserves histogram: Generalization of LSB++”	New improved version of LSB++ method is proposed which preserve the histogram and thus prevents the histogram analysis based attacks. This method also eliminates the embedding of extra bits thus leads to high stego image quality.
[24]	2014	Amitava Nag et al.	“A Huffman Code Based Image Steganography Technique”	Authors proposed Huffman coding based novel steganographic technique of LSB substitution. This work mainly focuses on high security and embedding capacity and acceptable level of visual quality of stego image. Experimental results demonstrate that proposed scheme has PSNR of 30 dB to 31 dB.

[25]	2014	N. Akhtar et al.	“An Improved Inverted LSB Image Stegano-graphy”	New steganographic method is proposed and implemented based on bit inversion. Experimental results represent that PSNR value of stego image is improved using this method.
[26]	2014	P. U. Deshmukh et al.	“A Novel approach for Edge Adaptive Stegano-graphy on LSB insertion technique”	Authors proposed a new edge adaptive steganography based on LSB substitution. Experimental results show that this technique is efficient than LSB and other pixel differencing methods.
[27]	2014	E. Dager and S. Dagar	“LSB based Image Steganography using X-Box Mapping”	Authors present the data hiding method for color RGB images. X-box mapping is utilized for this purpose. Their system is more secure and provides higher values of PSNR.
[28]	2013	M. R. Modi et al.	“Edge Based Stegano-graphy on Colored Images”	Authors proposed a novel data hiding method to embed data in two LSB bits of sharp regions of the cover image i.e. edge regions. Simulation results analysis shows that their method performs better than traditional LSB approach.
[29]	2013	D. Samidha and D. Agrawal	“Random Image Stegano-graphy in Spatial Domain”	New image steganographic method is proposed based on LSB substitution method using random bit selection. Pixels are selected in random fashion for embedding based on intensity values, location of pixel and so on.



[30]	2012	S.Gupta et al.	“Enhanced Least Significant Bit Algorithm for Image Steganography”	Authors proposed an enhanced LSB based hiding method in which only blue channel is utilized for data hiding. This method reduces the leap in color scale because only blue channel is used to embed secret information.
[31]	2012	S. Sachdeva and A. Kumar,	“Colour Image Steganography Based on Modified Quantization Table”	They proposed steganography method named as JMQT based on modified Quantization Table (QT). JMQT only enhances the data hiding capacity, which lead to poor stego image quality. They also compare their method to JPEG-JSteg method.
[32]	2011	S. M. M. Karim, et al.	“A New Approach for LSB Based Image Steganography using Secret Key”	In this method secret key is used with LSB method and RGB true color images to achieve good level of security. This secret key is also embedded into LSB bits of cover image. PSNR value is comparatively good and level of security of hidden data is also high.
[33]	2010	X. Qing et al.	“A High Capacity Information Hiding Algorithm in Color Image”	Author proposed a technique of information hiding in which adaptive steganography is used with RGB images to embed data in all the channel to enhance the embedding capacity of the system. Simulation results show that proposed method has high embedding capacity.

[34]	2010	Che-Wei Lee and Wen-Hsiang Tsai	“A New Steganographic Method Based on Information Sharing via PNG Images”	Author presents a new method of steganography based on Shamir’s method of secret sharing and PNG images. They only use alpha channel of PNG cover image to hide secret data. Proposed method has PSNR of 45.44 dB.
[35]	2009	H. Yang et al.	“A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”	New adaptive LSB based method of image steganography. It applies the pixel adjustment method for better stego image quality. Experimental results demonstrate that proposed system has high data hiding capacity.
[36]	2009	S. Channalli and A. Jadhav	“Steganography an Art of Hiding Data”	Authors proposed new LSB based method in which common bit pattern is used to hide the data. Proposed system has low data hiding capacity.

**Table 2.2** Summary of literature survey on Encryption techniques used with Steganography

<b>Ref. No.</b>	<b>Year</b>	<b>Author(s)</b>	<b>Name</b>	<b>Description</b>
[37]	2015	D. Debnath et al.	“An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography”	Authors proposed a new method in which both steganography and cryptography is used. Data is first encrypted using hill ciphers and then embedded into RGB cover image.
[38]	2014	D.E.M. Ahmed and O.O. Khalifa.	“Robust and Secure Image Steganography Based on Elliptic Curve Cryptography”	Their research work focuses on LSB image steganography along with elliptic curve cryptography (ECC). Secret information is first encrypted with the help of ECC and then ciphered information is embedded into cover image.
[21]	2014	N.A. Al-Otaibi, and A.A. Gutub	“2-Layer security system for hiding sensitive text data on personal computers”	They designed a modern system in view of two layers of steganography and cryptography steganography layer utilize multiple LSB bit embedding and cryptography for information.
[22]	2014	M. R. Islam et al.	“An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography”	Authors proposed a new improved version of LSB steganography based on efficient filtering using status bit. AES cryptography algorithm is applied to gain higher level security to hidden secret data. Bitmap images are used as cover images. Proposed system has high PSNR and data hiding capacity.

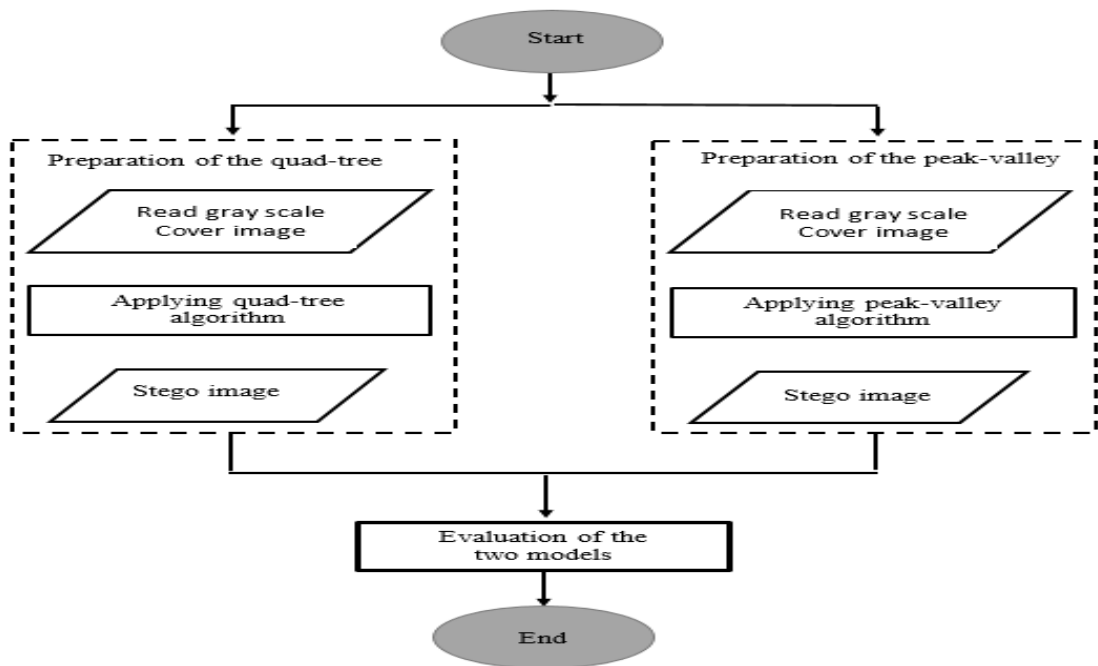
[39]	2014	S. Krishnagopal et al.	“Image Encryption and Steganography Using Chaotic Maps with a Double Key Protection”	In this proposed work Chaos based cryptography is used with steganography. Chaotic logistic and cat map are used as the base for their image encryption algorithm. Results demonstrate that proposed system has 0.981 SSIM index value and 47.71 dB PSNR.
[40]	2011	S. Song et al.	“A Novel Secure Communication Protocol Combining Steganography and Cryptography”	Authors proposed a very innovative method that combines the steganography and cryptography into one system. No separate computations will be done for these two. Hence the new system needs very few computations than existing techniques, while maintaining high security level.
[41]	2002	J Fridrich , M Goljan	“Practical Steganalysis of Digital Images – State of the Art”	Steganography is the art of hiding the very presence of communication by embedding secret messages into innocuous looking cover documents, such as digital images. Detection of steganography, estimation of message length, and its extraction belong to the field of steganalysis.
[42]	2003	J. Fridrich, Goljan, M. and D. Soukal,	“Higher-order statistical steganalysis of palette images”	A novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value Differencing (PVD) method is presented in this paper.
[43]	2003	J. Fridrich, Goljan, M. and D. Soukal,	“Higher-order statistical steganalysis of palette images”	In this paper, we describe a new higher-order steganalytic method called Pairs Analysis for detection of secret messages embedded in digital images.

## CHAPTER 3

### RESEARCH METHODOLOGY

#### 3.1 Introduction

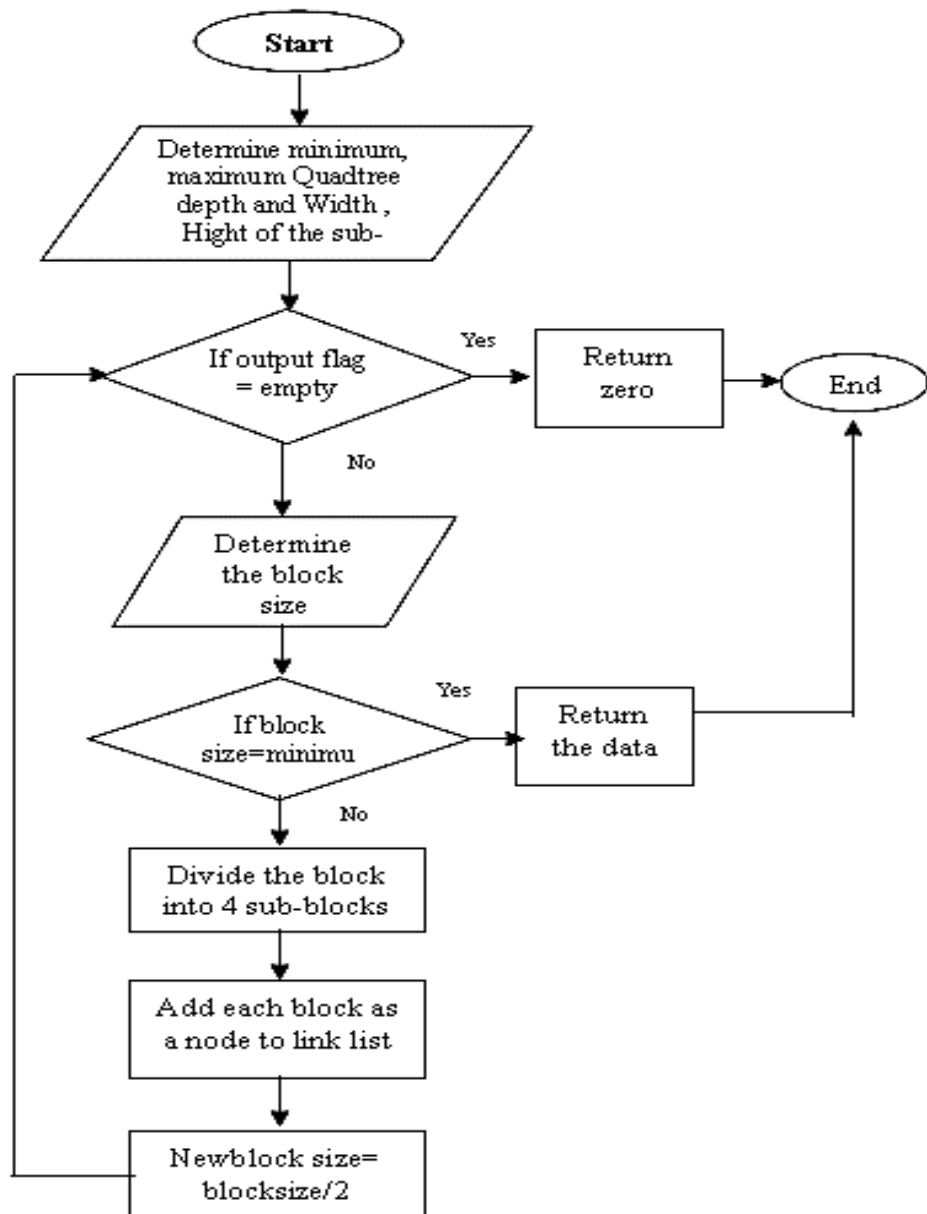
In this chapter, the methodology of this study is explained. The methodology represents the sequence of the steps which are used for accomplishing the objectives of the research. The structure of the proposed covers many steps: preparing a secret message and the cover image, embedding, and evaluation of the proposed. The methodological steps are detailed in subsequent sub-sections. Figure 3.1 illustrates the methodology of the presented.



**Figure 3.1** Flowchart of the Proposed.

#### 3.2 Proposed

This work provides a method for hiding data, where the proposed used two different techniques. At first, quad-tree. Secondly, Peak-valley.



**Figure 3.2** Flowchart of the Quad-tree.

### 3.2.1 Algorithm Quad Tree

The suggested data in the hiding scheme that comprise the elements was depicted in Figure 3.4. For instance, the hostess / image is a single byte two-dimensional matrix of numbers with a size of N via N. Split the host image as shown in Figure 3.4 first to a different size of non-nested blocks using a hierarchical hash policy. They do arranged like a segmentation formation of arbor shape namely image blocks and these, sheet junctions of the segmentation arbor, have been utilized for information hiding process, all of a leaf nodes could be sorted a tree traversal procedure into a requested arrangement of images pieces also would be represented by the division arbor structure

by utilizing a binary codes series. An ordered sequence of image blocks will be taken from the payload generation process and the secret data as input and they will be transformed into different sequence of couples for message or mass, because of structure of every message includes a portion of a secret information plus connected hanging information which will install in the relating images section. A histogram shifting scheme is used by the embed algorithm utilizes the reason is for setting every structured message for the identical image mass, including building the image (named stego-image) in respecting to the tree form bit-series data. So as to ensure a regeneration the partition arbor within the receiver head, the arbor form bit-series also was embedded utilizing moving of histogram with a stego-image. The following will clarify constituent parts. First give us a chance to characterize a few images for the simplicity of introducing the points of interest of the calculations. The image inputting is stands like  $\mathbf{b}_{N \times N}$ . Hostess image has divided for various size as masses of a quad-arbor way. The quad-arbor form has made to express that division operation, where  $\mathbf{b}(x, z_x)$  is the  $z_x$ -th block at the  $x$ -th level of the quad-arbor form. Some properties of every block  $\mathbf{b}(x, z_x)$  are selected in the proposed algorithm and clarified below as the following

$n(x, z_x)$  : Binary variable indicates whether  $\mathbf{b}(x, z_x)$  has been partitioned or not. Set  $n(x, z_x) = 1$  if  $\mathbf{b}(x, z_x)$  is decided to be divided; otherwise,  $n(x, z_x) = 0$ .

$h(x, z_x)$  : Histogram function that is computed according to block  $\mathbf{b}(x, z_x)$ .

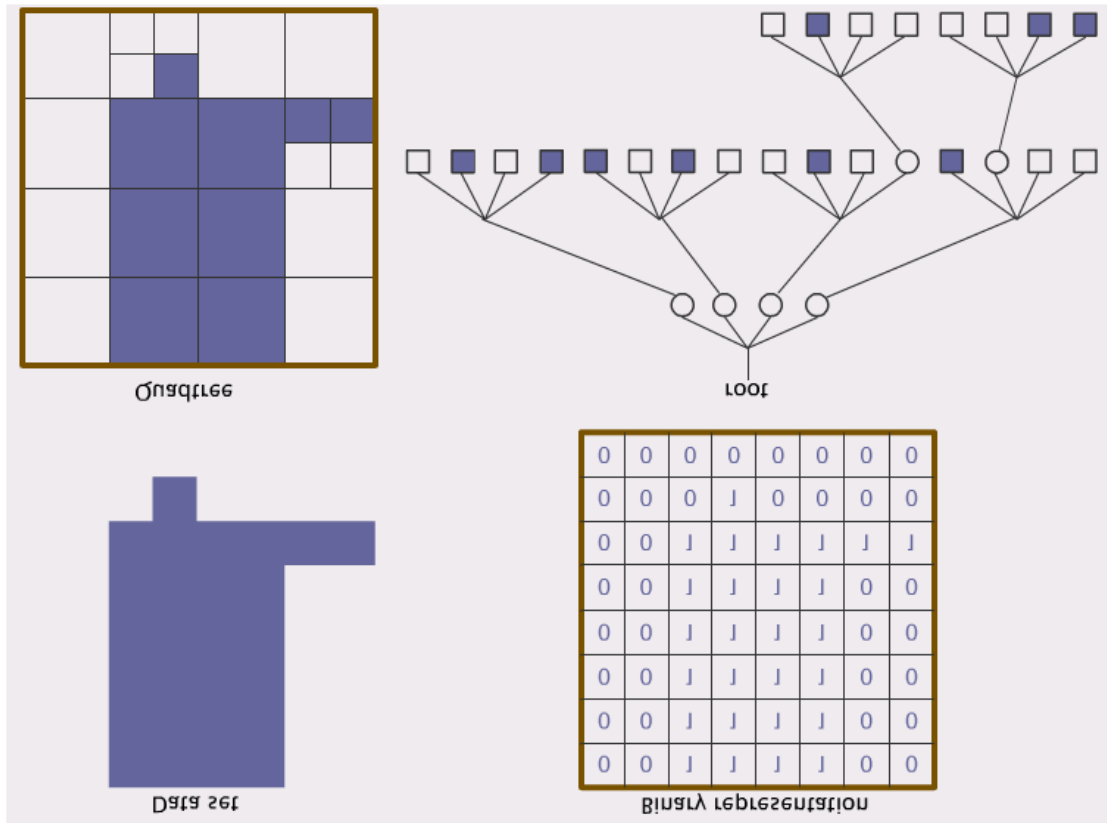
$c(x, z_x)$  : Hiding capacity function derives from  $h(x, z_x)$ .

As shown in figure 3.4 the information set would be payload generation component in addition to formed it utilizing a quad-arbor division. In those embeddable blocks, the maximum and minimum points is  $\mathbf{b}(x, z_x)$  also the byte series  $n(x, z_x)$  as wholly probable  $x$  and  $z_x$  were prepared for up information. This is so essential to be embedded with the secret data which are given through the employers inside the information image for supporting the correct recuperation of info image from the stego-image [44].

### 3.2.1.1 Quad-tree segmentation

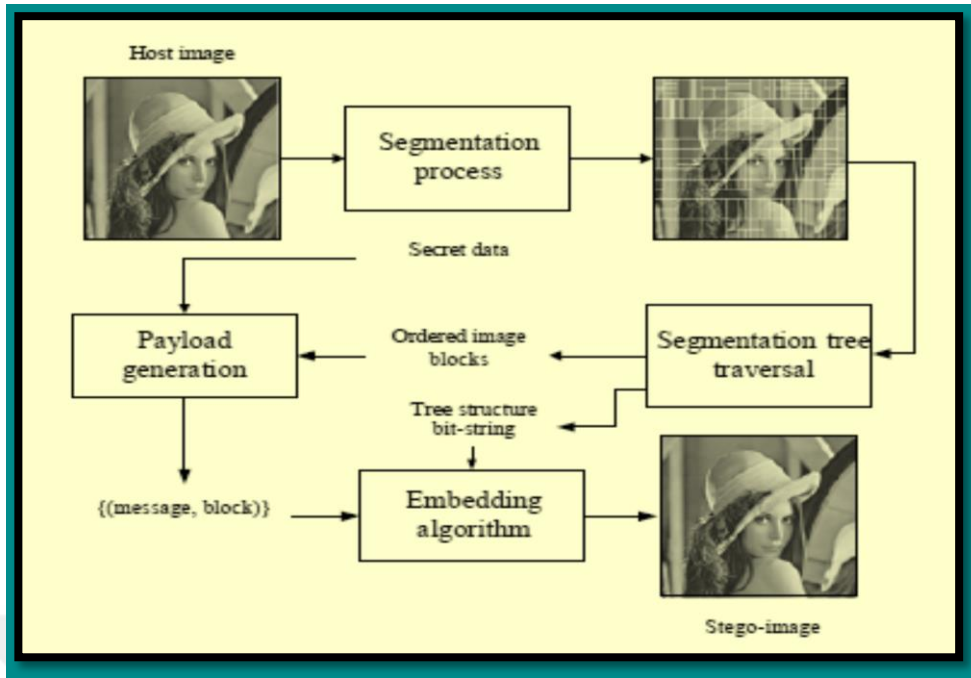
The recommended algorithm works for implanting the secret information to no-covered block of pixels utilizing histogram moving method. This is produced from division the inserted information and prepared as a structure like quad-arbor. Lower contrast blocks in addition to the idea of histogram moving procedure can adjust more

bits of information during crucial difference squares cover up generally less measure of information bits.



**Figure 3.3** Quad-tree indexing.





**Figure 3.4** Steps of the Data Hiding Process.

Here we can say that smaller sub-blocks of most of the sub-blocks has become smoother and altogether providing larger hiding capacity. It is depicted in Figure 3.5 that detail of how to do the quad-tree partition for image blocks. To start, variable  $z_x$  is initialized to be one for  $x = 0, 1, \dots, \lfloor \log_2 2 \rfloor$  and  $\mathbf{b}(0,1) = \mathbf{b}_{N \times N}$ . The first step in the partition process is making a decision on whether a further division is needed or not for any incoming block  $\mathbf{b}(x, z_x)$ . Before the decision,  $\mathbf{b}(x, z_x)$  is tentatively partitioned into four sub-blocks These  $\mathbf{b}(x+1, z_{x+1}+1)$ ,  $\mathbf{b}(x+1, z_{x+1}+2)$ ,  $\mathbf{b}(x+1, z_{x+1}+3)$ , and  $\mathbf{b}(x+1, z_{x+1}+4)$ , and the four sub-blocks in addition to the hiding capacities of the incoming block are evaluated individually as a result,

$$PS3(\mathbf{b}(x, z_x), 4) > PS1(\mathbf{b}(x, z_x)).$$

The parameter  $n(x, z_x)$  was valued as 1 also, the incoming block was determined to be divided as 4 sub-blockes; unless an incoming block is taken into account as a final node of quad-arbor formation and  $n(x, z_x)$  has valued as zero, meaning no extension distribution needed for  $\mathbf{b}(x, z_x)$ . Per of the 4 blockes has taken into account once more to be the incoming block for more quad-arbor distribution weighing the incoming block  $\mathbf{b}(x, z_x)$  was split. The method has proceeded frequently within a deepness-initial manner unto completely attainable block distributions were crossed.

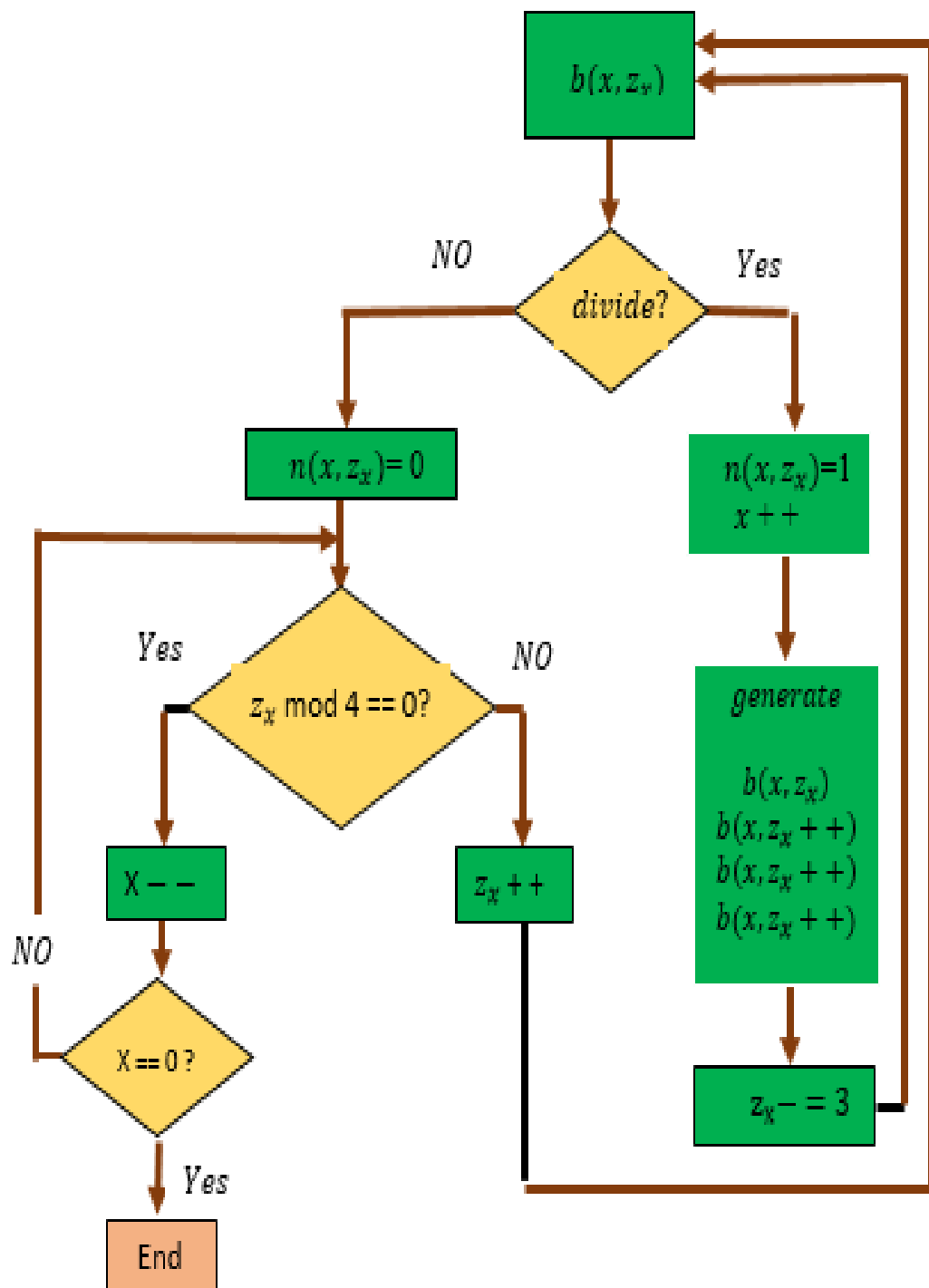
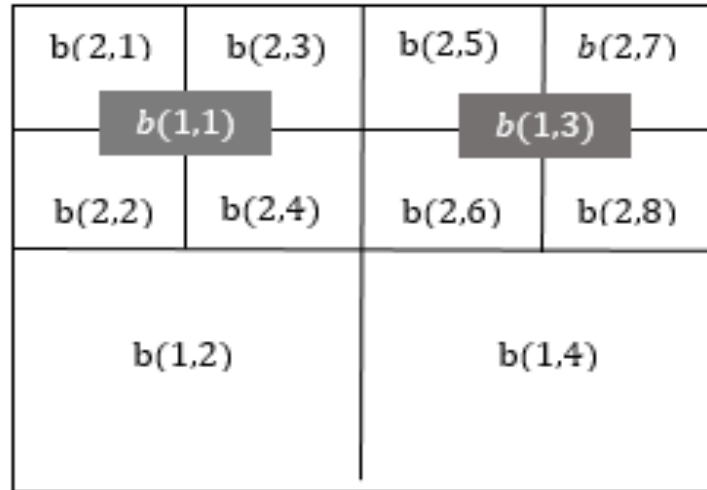


Figure 3.5 Quad-tree Segmentation Process.



**Figure 3.6** Quad-tree partition.

Figure 3.6 shows an example to demonstrate a block of pixels of quad-tree partition, while figure 3.7 shows the structure of the corresponding form of the quad-tree. Figure 3.7 needs a bit-string  $t = '1100000100000'$  to elucidation the structure of the quad-tree.

Algorithm 1 shows the creation of the bit-stream  $t$  by preorder traversal which traverses the root at the first, left sub tree and finally right sub tree alternately. The chain of the bit-stream is defined as the symbol “//”.

**Algorithm 1: Quad-tree structure traversal**

Input: Nodes  $b(x, z_x)$  Output:

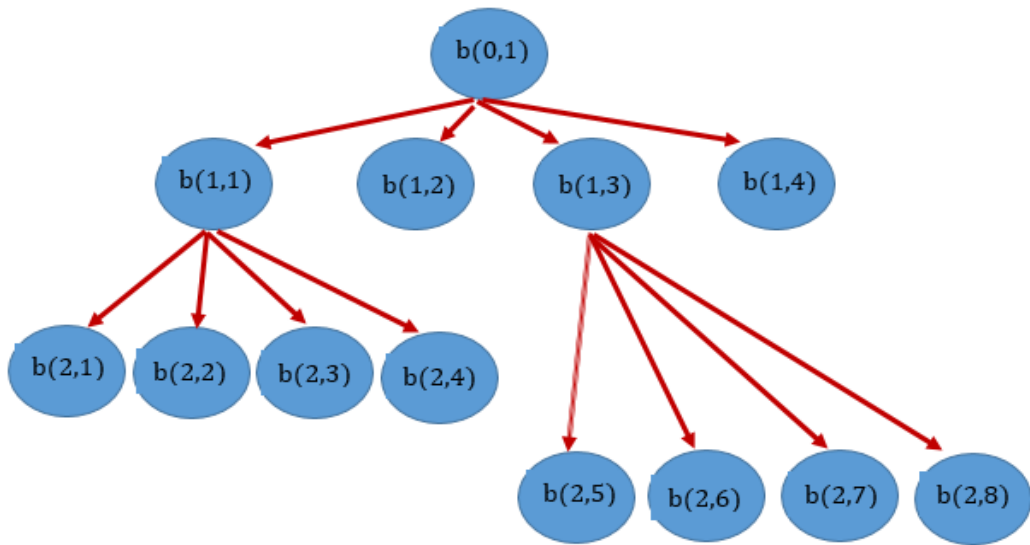
Bit-stream:  $t$  Initialization:  $b(x, z_x) = b(0, 1)$

Begin Preorder\_bitstream ( $b(x, z_x)$ )

1.  $t = t // n(x, z_x)$
  2. If  $n(x, z_x) \neq 0$
  3. Preorder\_bitstream ( $b(x, 1 + z_x)$ )
  4. Else
  5. Preorder\_bitstream ( $b(x-1, z_{x-1} + 1)$ )
  6. End if
- End

Figure 3.5 shows the applying of the quad-tree partition steps on the image *Lenna*. Figure 3.8 shows the partition results as can be seen that the smaller size blocks with simple model histogram would be partitioned to the blocks with multi-model

histogram of intensities. The smallest size block is reached to 16 by 16 pixels in this situation.



**Figure 3.7** Quad-tree Structure of the Partition.



**Figure 3.8** Quad-tree Partition Example for Lena.

### 3.2.1.2 Embedding algorithm

Figure 3.4 shows the implying of secret data in the embeddable blocks  $\mathbf{b}(x, z_x)$  from quad-tree segmentation. Figure 3.9 shows, how to do the implying process, how to elicitation the input image recovery from the stego-image and the necessities of both overhead information and secret data in the block to be implying.

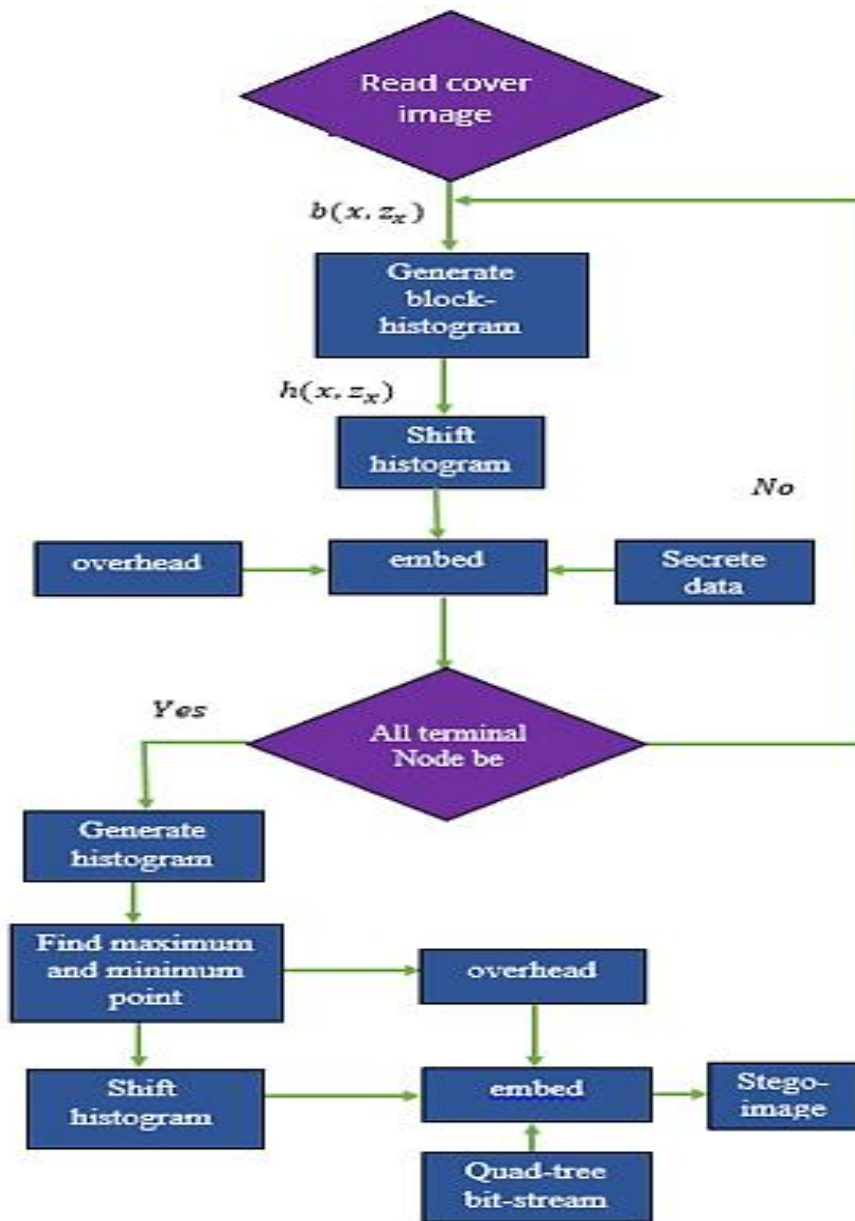
Figure 3.4 shows the overhead that is implying in each embeddable block and it's called overhead1. Overhead1 is got from payload evaluation process. Figure 3.10 shows the structure of overhead1, while table 1 shows the attributes of overhead1.

**Table 3.1** Description of overhead1

Symbol:	Purpose:	Field length
No. of min values	The length of minimum points.	8 bits
min value	The coordinates $(x, y)$ of minimum points.	optional
next max1	The grayscale of the first maximum point of the next terminal node.	8 bits
next min1	The grayscale of the first minimum point of the next terminal node.	8bits
PL	Length of payload	8bits
Payload	Part of secret data.	optional

No. of Min. Values	Min. Values $(x, y)$	Next min1	Next max1	PL	Payload

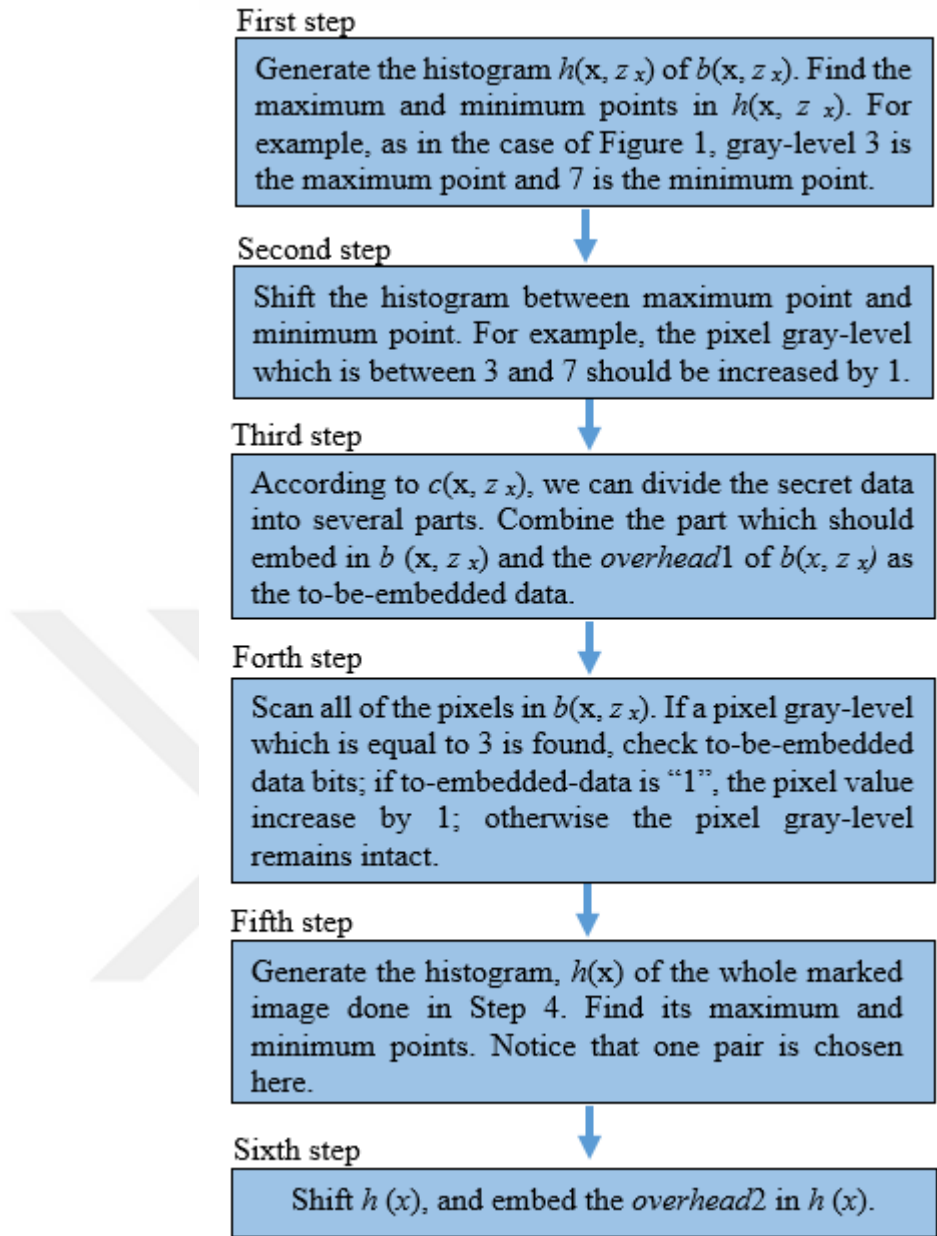
**Figure 3.9** The Structure of Overhead1.



**Figure 3.10** Flow Procedure of the Embedding Algorithm.

We register the maximum and minimum point's info of the following block the reason is to extract data block by block. Information in the final nodes of the tree only was embedded. It will be assembled by us along with the quad-tree bit-stream as data set overhead2. Above all in blocks the secret data embedded, the whole image to embed overhead2 in it using Ni's algorithm was shifted.

A sequence of steps is performed as follows scheme:



**Figure 3.11** A sequence of steps is performed of an algorithm.

### 3.2.2 Peak-valley method

Each section signals may contain specific numbers of peaks and/or valleys this called Peak-Valley (PV) identification, according to the needs of the study. This is basically helpful for fatigue time information since peaks and valleys feature mainly in rain influx counting algorithms for fatigue harm calculations [45].

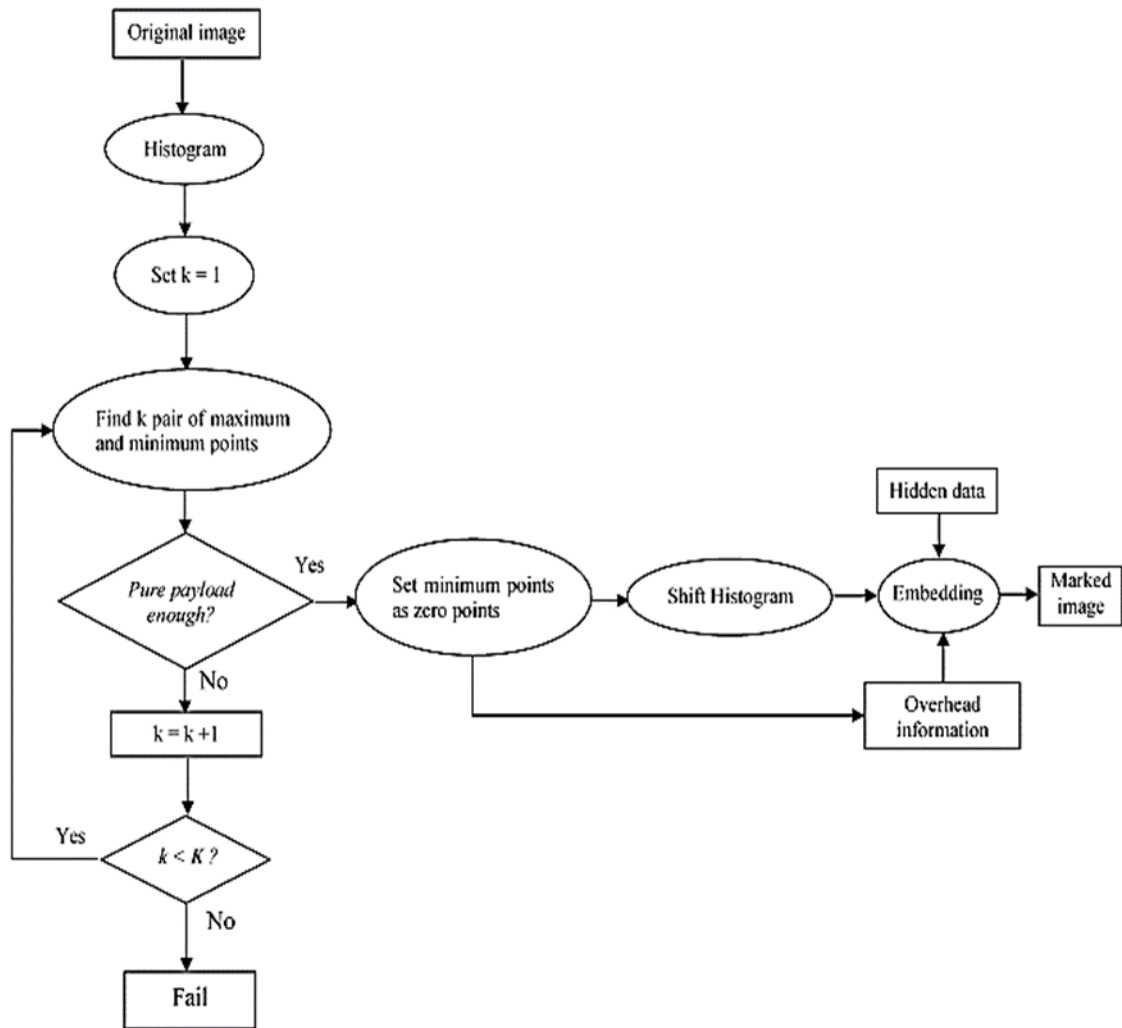
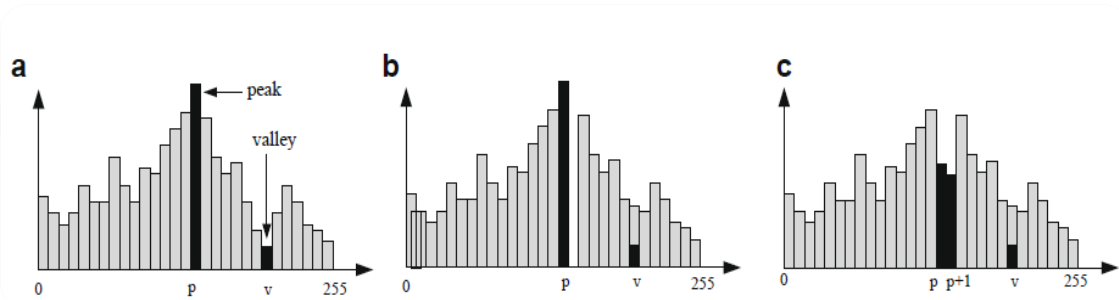


Figure 3.12 Data Embedding Algorithm.



### 3.2.2.1 Algorithm Peak-valley

In the original image, image's histogram slightly modified, so that let the data embedded with it according to Ni et al.'s algorithm [46]. For instance it can be assumed that we have an original image  $I$  and its histogram  $H(I)$  which can be clarify in Figure 3.13a. For ease of display, let  $h(x)$  denote the number of pixels with gray value  $x \in [0,255]$ . In Figure 3.12a, and also is clearly manifested that the grey value  $p$  is the peak of that point in  $H(I)$  since  $h(p) > h(x)$  for all  $x \neq p$ ; that is, the common frequently grey value is  $p$  and it has appeared in the original image  $I$ . Furthermore, gray value  $v$  is the valley point in.



**Figure 3.13** The main idea in Ni et al.'s algorithm. (a) It can be a reasonable example of histogram with a peak point and a valley point. (b) Shift the interval  $(p, v)$  to the right by a unit. (c) The data and the positions with gray levels  $p$  and  $p + 1$  were embedded.

The peak-valley pair  $(p, v), H(I)$  since  $h(v) < h(x)$  for all  $x \neq v$ . From the histogram  $H(I)$  and the hiding data, they all are represented through the binary string  $B_h$ , and in addition to that, with the aid of the following embedding technique, they may be embedded into the original photograph  $I$ :

Step one. If  $h(v) > 0$ , It can transform the positions of pixels with gray value  $v$  inside a binary string  $B_v$  in addition to that, the hidden data  $B_h$ , and  $B_v$ , are gathered together to be formed into new binary string  $B'_h$ . The binary string  $B_v$  includes the above data to restore the original image from a single tag. Step two. If  $p < v$ , conforming to the gray values within the time, move the rectangular bars  $[p + 1, v - 1]$  in the histogram to the right by one unit through the addition of one to gray pixels values with gray values within  $[p + 1, v - 1]$  (see Fig. 3.13b). If  $p > v$ , matching the gray values, move the rectangular bars within  $[v + 1, p - 1]$  in the histogram to the left by one unit by the subtraction from to the gray pixels values with gray values within  $[v + 1, p - 1]$ .

Step three. By selecting the pixels with gray value  $p$  by embedding  $B'_h$  scan the original image. selected pixel Scan the original image, its gray value remains  $p$  when the corresponding embedded bit in  $B'_h$  is 0 and is modified to  $p + 1$  (or  $p - 1$ ) as the corresponding embedded bit can be 1 for the case of  $p < v$  (or  $p > v$ ) (see Fig. 3.13c).

There are 3 steps have been mentioned above , It can be embed  $h(v) - O_{B_v}$  bits of hiding data into the peak-valley pair  $(p, v)$  where it can be  $O_{B_v}$  denotes the number of bits which is needed in the binary string  $B_v$ . The condition  $h(v) - O_{B_v} > 0$  holds the reason is that  $h(p)$  is much larger than  $h(v)$ . From the upper limit on the (MSE) in the middle of the marked image and the original image is 1, the PSNR lower bound of Ni et al.'s algorithm is  $48:13 \left( = \log_{10} \frac{255^2}{1^2} \right)$  and it is the highest of all existing data reversible hidden algorithms.

An extracting procedure can be used to and the reflected image is marked back to the initial one and extract the hidden data:

Step one: Scan the marked image in the same order which have utilized in an embedding method. For every pixel tested, a bit 0 is taken if the gray value is  $p$  and a bit 1 is taken in addition, if the gray value is  $p + 1$  (or  $p - 1$ ) for the case of  $p < v$  (or  $p > v$ ). Testing all pixels, a binary string  $B'_h$  would retrieve the hiding data string  $B_h$  and the overhead information string will be  $B_v$ .

Step two: For the case of  $p < v$  (or  $p > v$ ), decrease (or increase) the gray values of the pixels with gray values within  $[p + 2, v]$  ( $[v, p - 2]$ ).

Step three: Will be transforming the overhead information string  $B_v$  and locating the corresponding pixel positions. Reorganizing the gray value of every found pixel to  $v$  and recovering the first image.

The embedding capability naturally is bolstered via studying much more a peak-valley both for embedding the hidden information. For the first image  $I$ ,  $n$  valley points  $v_1, v_2, \dots, v_n$ , where  $0 < v_1 < v_2 < \dots < v_n < 255$ , are original taken from the histogram  $H(I)$ . The cause is the two grey values 0 and 255 are not used in Ni et al.'s algorithm, we permit  $v_0$  and  $v_{n+1}$  denote pseudo valley points where  $v_0 = \text{zero}$  and  $v_{n+1} = 255$  for no longer tough exposition; the 2 pseudo valley factors are most effective used to clarify the height-valley pair choice, in place of building the height-valley pairs. In experimental work, every valley point  $v_i, 0 < i < n + 1$ , one of both conditions  $h(p_i) -$

$h(v_i) * O_{v_i} > 0$  and  $h(p_{i+1}) - h(v_i) * O_{v_i} > 0$  must be continued where  $p_i$  and  $p_{i+1}$  denote 2 peak points in that intervals  $(v_{i-1}, v_i)$  and  $(v_i, v_{i+1})$ ;  $O_{v_i}$  is the number of bits required for recording the position of each pixel with gray value  $v_i$  and it is standed for by  $O_{v_i} = [\log_2(\max(W, H))] \times 2$  where  $W$  and  $H$  is the width and height of the input image. According to the next peak-valley pair selecting procedure,  $n$  peak-valley pairs,  $(p_1, v_1), (p_2, v_2), \dots, (p_n, v_n)$  can be prepared in a greedy way to compatible the memory requirement for the hiding information  $B_h$  and the overhead information string  $B_v$ :

Step one. For two intervals  $(v_0, v_1)$  and  $(v_n, v_{n+1})$ , select two gray values  $p_{(1)(0)}$  and  $p_{(n)(n+1)}$ ,  $v_0 < p_{(1)(0)} < v_1$  and  $v_n < p_{(n)(n+1)} < v_{n+1}$ , as two peak points.

Step two. For each interval  $(v_i, v_{i+1})$ ,  $1 < i < n$ , select two gray values  $p_{(i)(i+1)}$  and  $p_{(i+1)(i)}$ ,  $v_i < p_{(i)(i+1)} < p_{(i+1)(i)} < v_{i+1}$ , as two peak points.

Step three. For each  $v_i$ ,  $1 < i < n$ , if  $h(p_{(i)(i-1)}) > h(p_{(i)(i+1)})$ , set  $p_{(i)} = p_{(i)(i-1)}$ ; otherwise, set  $p_{(i)} = p_{(i)(i+1)}$ . Consequently,  $n$  peak-valley pairs  $(p_1, v_1), (p_2, v_2), \dots, (p_n, v_n)$  are determined [46].

While we get  $n$  top-valley pairs, running the embedding technique on every top-valley pair may embedded the hiding data  $B_h$  and the overhead records  $B_v$  into the primary photograph. Both of them are applying the extracting process to each peak-valley pair which can retrieve the hidden information  $B_h$  and recover the first image i.e the original.

### 3.2.2.2 Extraction of peak-valley algorithm

In order to be brief, we only describe the simple case of minimum and maximum points. We describe only these because the general cases of numerous pairs of maximum and minimum points can be separated i.e. the case of multiple pairs may be dealt with as a repetition of data extraction for one case.

Regarding that the grayscale value of the maximum and minimum points are  $a$  and  $b$  respectively and  $a < b$ , the size of the marked image is  $M \times N$ , every value of grayscale value  $x \in [0, 255]$ .

- 1 After scanning the marked image in the same order which is used in the embedding procedure. If a pixel with its grayscale  $a + 1$  value is found, a bit “1” is got. If a pixel with its value is found, a bit “0” is got.
- 2 Scan the image again, the pixel value is subtracted by 1 for any pixel whose grayscale value  $x \in (a, b)$ .
- 3 Set the grayscale value pixel (whose coordinate  $(a, b)$  is saved in the overhead) as  $b$  if the above bookkeeping information is found in the extracted data.



## CHAPTER 4

### RESULTS AND DISSCUSION

#### 4.1 Introduction

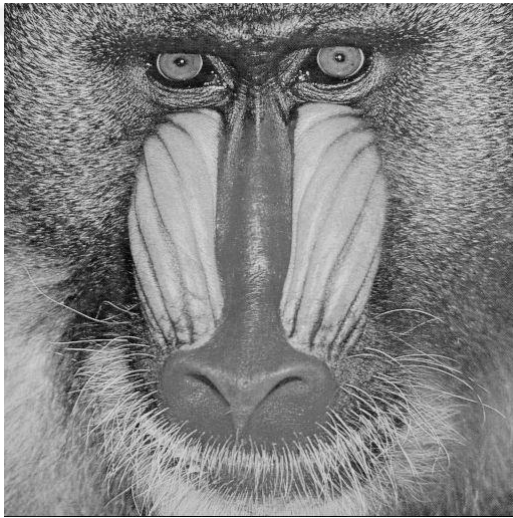
The main aim of this work is to hide an outsized quantity of secret message with a high secrecy and at an equivalent time protective the cover image's quality. In this chapter, the experimental results, which depend on two tests, will be discussed. They include peak signal-to-noise ratio (PSNR) and Chi-Square ( $\chi^2$ ). Thus, while the former is the first test and when the value for this test is high the human eye cannot recognize the change of the image after the embedding process and vice versa. And the latter test applies the attack on the stego-image to check the probability whereas the image contains the secret message.

The comparisons are done with previous studies to evaluate proposed method depending on three factors which are explained below.

- 1 Imperceptibility – This factor is measured by famous PSNR metric.
- 2 Capacity – all previous studies and proposed method are tested on the same images with the same payloads.
- 3 Robustness – This factor is tested by applying Chi-square attack technique on the stego-images that created by the proposed technique

## 4.2 Dataset

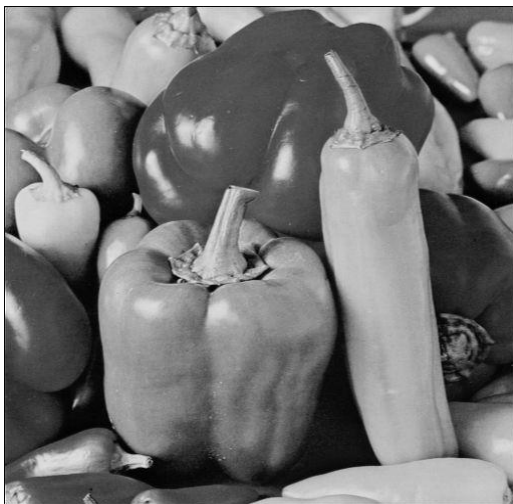
The data used in this study will be explained briefly. These data included six standard grayscale images of 512\*512 pixels. These include: Lena, tiffany, Baboon, Airplane, Peppers, and Barbara. These images are used as cover images. In addition, these images contain different grayscale and help to obtain precise results for evaluating the imperceptibility. Then, the attack is applied to these images after the embedding process. Usually, these images are used in all studies that deal with data hiding. Figure 3.1 depicts these images.



a



b



c



d



e



f

**Figure 4.1** Dataset (a) Baboon, (b) Lena, (c) Peppers, (d) Barbara, (e) tiffany, (f) Airplane.

Furthermore, an arbitrary plain text is used as the secret message. To evaluate the quality of stego-image, the following peak signal-to-noise ratio (PSNR) is employed:

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \quad (4.1)$$

$$\text{MSE} = \sum_{i=1}^{r*c} \frac{(g_i - g'_i)^2}{(r*c)} \quad (4.2)$$

Where,  $r$  and  $c$  size of image,  $g_i$  and  $g'_i$  is the cover and stego-image respectively.

### 4.3 Imperceptibility Result of the Proposed Method

The proposed method ensures that all the decimal codes of the quad-tree and Peak-valley are hidden inside the segmented cover. The proposed method is based on the imperceptibility of the system and Tables 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6 below show the result of the proposed method process.

**Table 4.1** Results of the proposed method of Lena image

Embedding rate		200	400	600	800	1000
		200	400	600	800	1000
PSN	Quad-tree	44.2092	44.1674	44.1257	44.0832	44.0401
	Peak-valley	58.8289	58.7137	58.6015	48.2631	48.2529

**Table 4.2** Results of the proposed method of Baboon image

Embedding rate		200	400	600	800	1000
		200	400	600	800	1000
PSN	Quad-tree	46.2596	46.2238	46.1874	46.1499	46.1122
	Peak-valley	50.507	48.2004	48.1904	–	–

**Table 4.3** Results of the proposed method of Tiffany image

Embedding rate		200	400	600	800	1000
		200	400	600	800	1000
PSN	Quad-tree	49.4765	49.4408	49.4054	49.369	49.3346
	Peak-valley	50.3106	50.2942	–	–	–



**Table 4.4** Results of the proposed method of Peppers image

Embedding rate		200	400	600	800	1000
		200	400	600	800	1000
PSN	Quad-tree	45.6523	45.614	45.5735	45.5359	45.4961
	Peak-valley	50.1913	48.2083	48.1982	-	-

**Table 4.5** Results of the proposed method of Barbara image

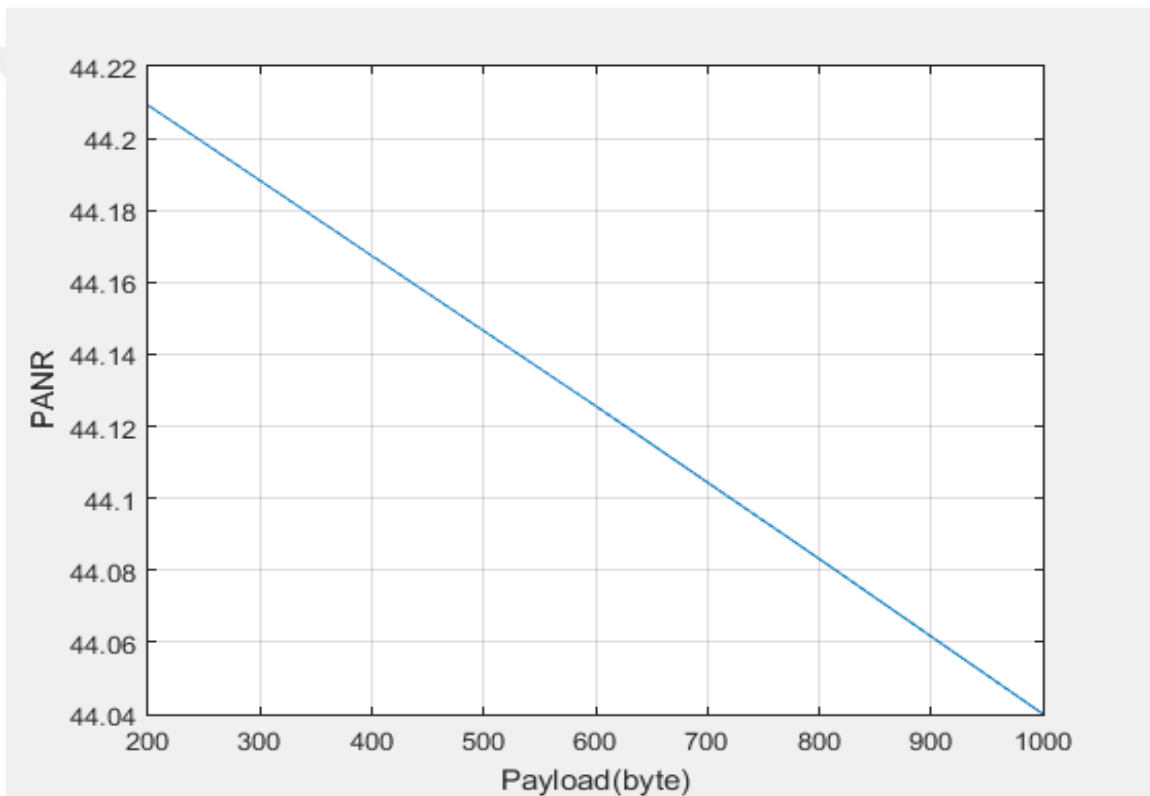
Embedding rate		200	400	600	800	1000
		200	400	600	800	1000
PSN	Quad-tree	45.2819	45.241	45.1997	45.1589	45.1183
	Peak-valley	52.2264	48.195	48.185	-	-

**Table 4.6** Results of the proposed method of Airplane image

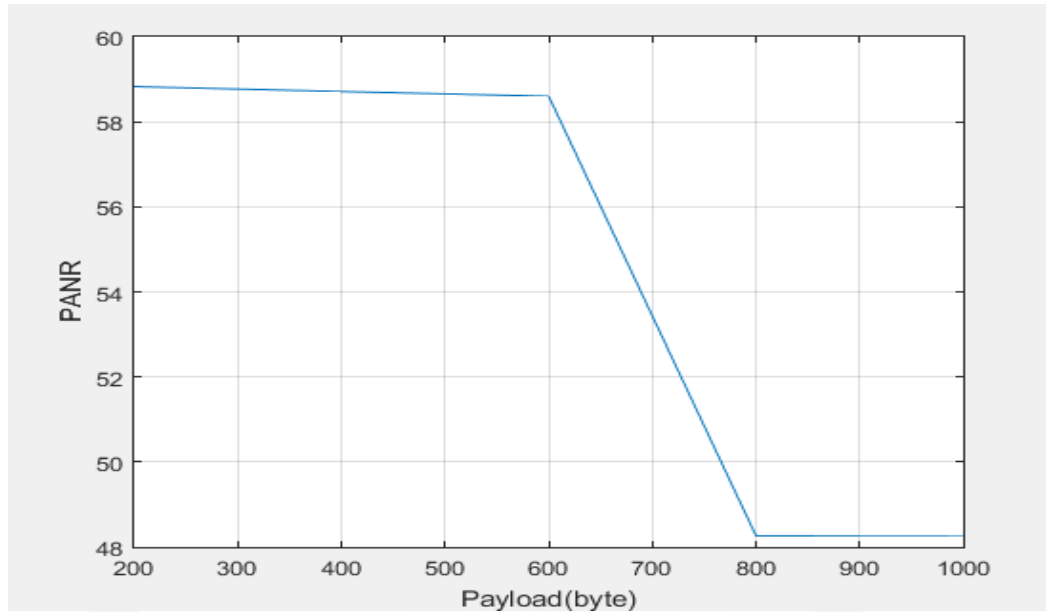
Embedding rate		200	400	600	800	1000
		200	400	600	800	1000
PSN	Quad-tree	48.4608	48.4228	48.3852	48.3491	48.314
	Peak-valley	54.0576	54.1361	54.0967	54.0576	54.0189

Tables 4.1 to 4.6 depict the results of the proposed method in terms of imperceptibility for two different algorithms i.e., Quad-tree and Peak-valley, with embedding rate ranging from 200 to 1000 bytes, and six variants images namely, Lena, Baboon,

Tiffany, Barbara, Peppers, and Airplane are employed as host images. The results have revealed that the imperceptibility for both algorithms is almost identical whereby, the PSNR decreases as the embedding rate increases. For example, in Table 4.1, Figures 4.2 and 4.3, the PSNR was 44.2092 dB when the embedding rate was 200 bytes and gradually decreased as embedding rates increased. Furthermore, the PSNR of Peak-valley is higher than that of Quad-tree with the embedding rate from 200 to 1000. However, the payload for the Peak-valley starts to overflow when the embedding rate is more than 1000 byte. This is due to the fact that the payload is more than the capacity that the cover image can accommodate i.e. maximum is 1/13 of 512\*512 pixels of the cover image).



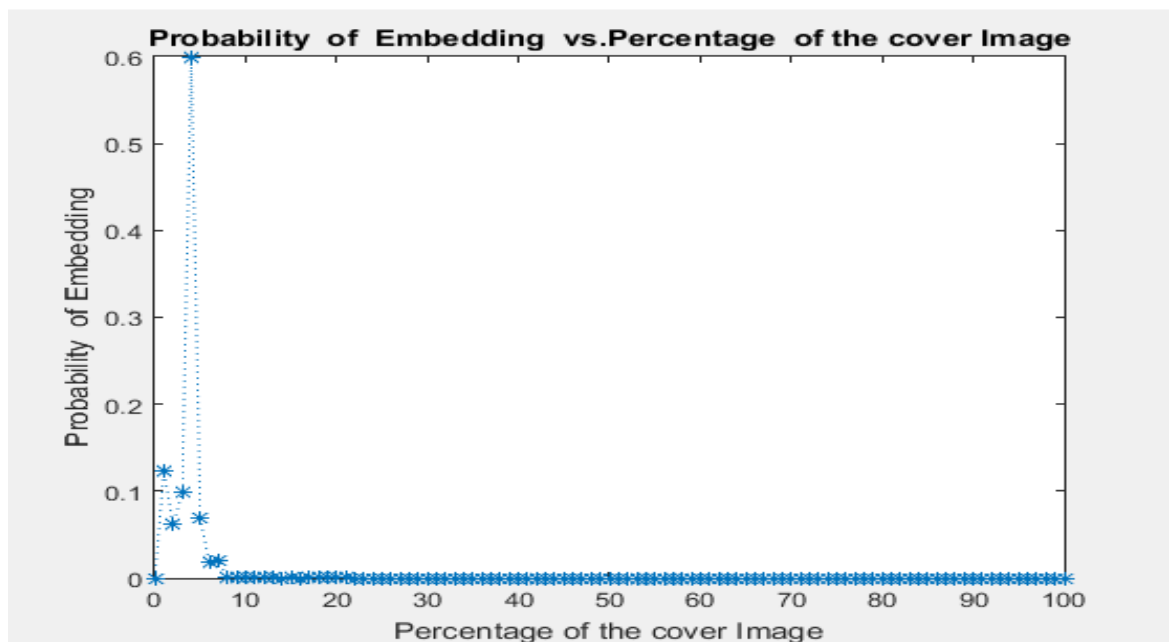
**Figure 4.2** Performance of the proposed method when Peak-valley of Lena image.



**Figure 4.3** Performance of the proposed method when Quad-tree of Lena image.

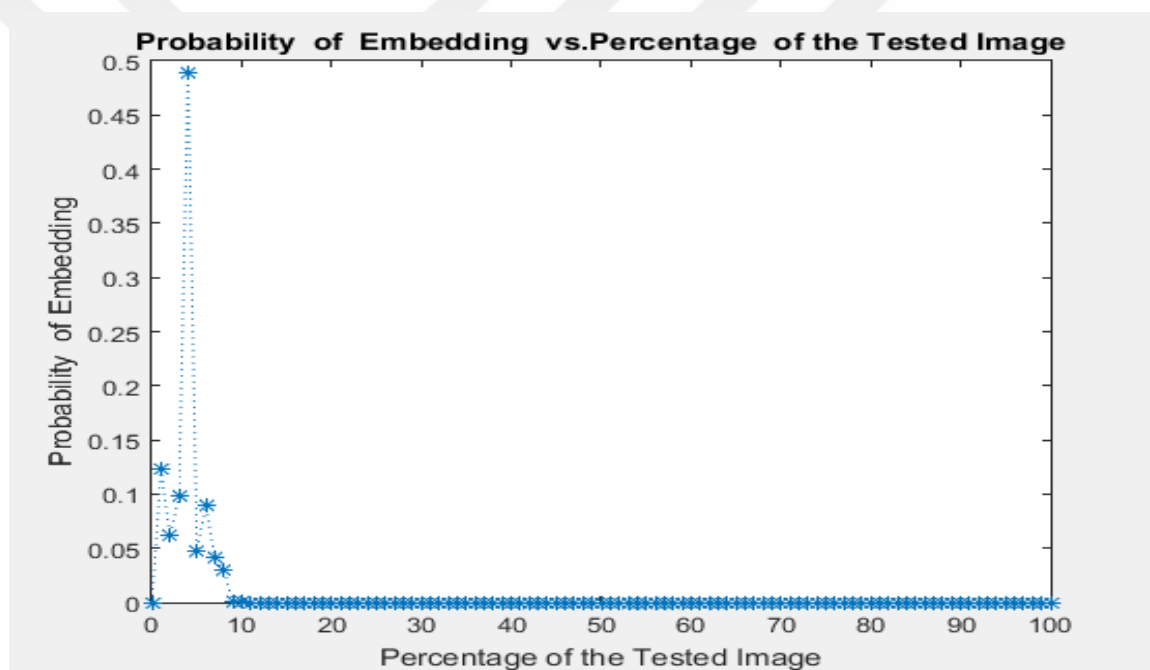
### 4.3. Chi-Square Measure for Robustness

Chi-Square attack is one of the most severe statistical attacks that have been used to reveal the existence of the secret message hidden inside the stego-image (Lee, 2009). This attack differs from other attacks because it is capable of computing the probability of containing the secret information without any physical changes on the image and therefore is considered very dangerous. Thus, this attack is applied in this study in order to evaluate the performance of the proposed method in terms of robustness [47].

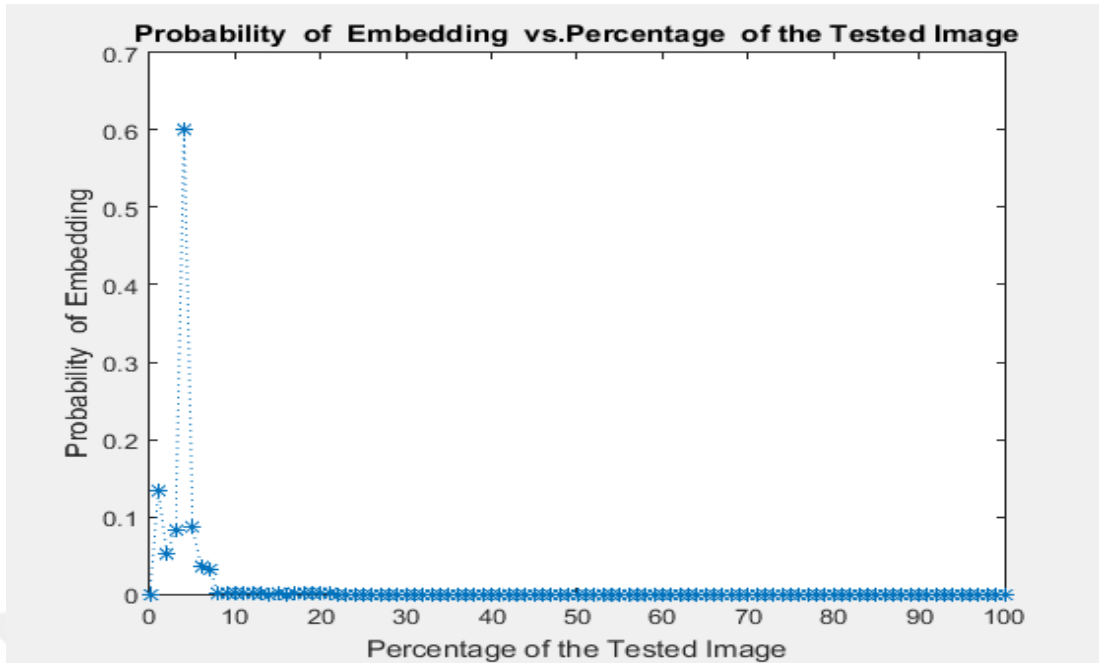


**Figure 4.4** Results for Chi-Squared attack on original Lina image.

Lena image is chosen in this test because of the precise result that can be obtained when the attack is applied to this image. As shown in Figure 4.4, the tested percentage of the image starts from 0 to 100, where 100% refers to the testing of the whole image. In contrast, the probability of the containing secret message starts from zero until the result of the Chi-Square attack. If the probability equals zero, this means that this image does not contain a secret message and vice versa when the probability equals one. The above Figure 4.4, depicts that the probability is almost zero for the entire test (except for the first 2% of the cover image; a sudden surge occurred due to Chi-Square initial behavior, and therefore can be ignored). This indicates there is no hidden message inside the cover image. In actual fact, this is always true since the cover is actually the original Lena image.

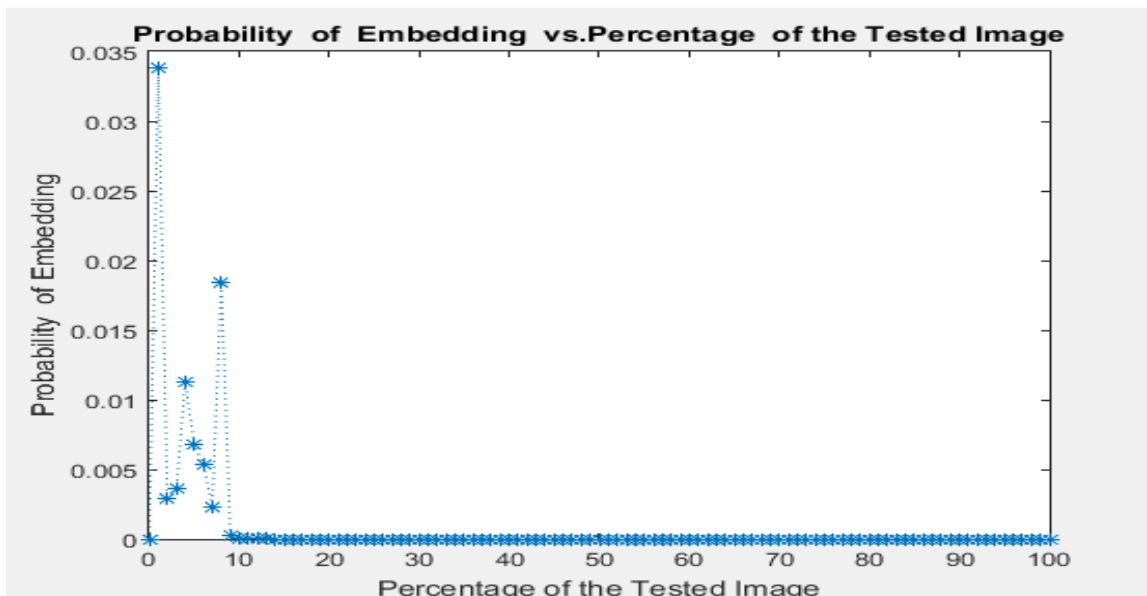


**Figure 4.5** Results for Chi-Squared attack on Lena stego-image that has been embedded by the proposed method using peak-valley and tested on 200 bit of the secret message

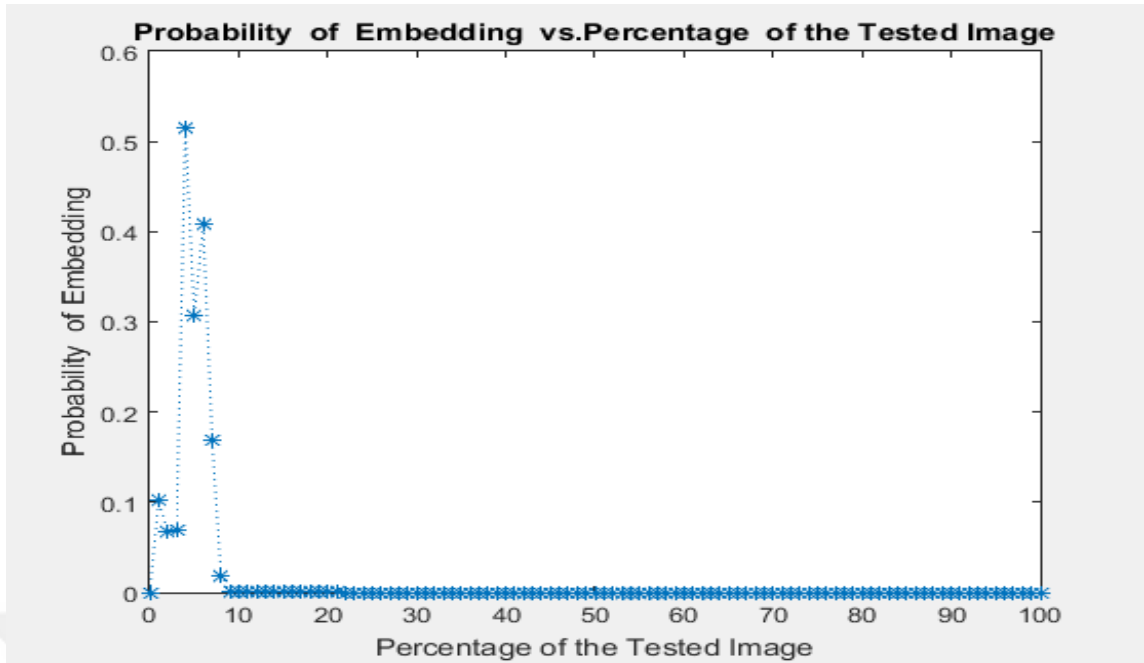


**Figure 4.6** Results for Chi-squared attack on Lena stego-image that has been embedded by the proposed method using quad-tree and tested on 200 bit of the secret message.

Similarly, the graph patterns of Figures 4.5, 4.6, 4.7 and 4.8 resemble that of Figure 4.4, which indicates that there is no hidden message found (but, actually there was a secret message hidden inside the stego-image). Therefore, it can be summarized that the proposed method is capable to withstand the Chi-Square attacks.



**Figure 4.7** Results for Chi-squared attack on Lena stego-image that has been embedded by the proposed method using peak-valley and tested on 1000 bit of the secret message.



**Figure 4.8** Results for Chi-squared attack on Lena stego-image that has been embedded by the proposed method using quad-tree and tested on 1000 bit of the secret message.

## CHAPTER 5

### CONCLUSION AND FUTURE WORKS

#### 5.1 Introduction

The contribution of this thesis is an investigation of the limits of information hiding: how low a level of distortion can be carried out with a given length of the embedded message. The guiding belief of pursuing minimal distortion is that (a) reduce distortion is preferable in many applications, chiefly with current trends of favoring large size high-quality pictures, and (b) minimal distortion to stego objects while leading to their being less detectable. The main goals were represented in this thesis through comparison between two main steganography techniques; quad-tree based steganography and peak-valley methods. The conclusions drawn from the current experimental study can be summarized as follows:

1. The quad-tree algorithm can be considered as an improved version of the traditional histogram shifting method. Whilst peak-valley algorithm uses the advantage of simple local distribution of pixel intensities and utilizes the zero or the minimum points of the histogram of an image
2. The method slightly modifies the pixel grayscale values to embed the data into the image. It can embed more data than many of the existing reversible data hiding algorithms.
3. The performance of each methods has been investigated, in terms of imperceptibility, the embedding rate ranges from 200 to 1000 bytes, whenever six variants images are employed as cover images. The results have revealed that the imperceptibility for both algorithms is almost identical whereby, the PSNR decreases as the embedding rate increases.

4. The PSNR was 44.2092 dB when the embedding rate was 200 bytes and gradually decreased as embedding rates increased. Furthermore, the PSNR of Peak-valley is higher than that of Quad-tree with the embedding rate ranges from 200 to 1000 .In addition, Chi-Square attack is performed on the stego image, produced by the presented algorithms to measure the robustness of the methods.
5. The test reveals that the probability of containing secret message is almost zero for the entire test which indicates that, there is no hidden message inside the cover image.

## **5.2 Summary of the work**

This research has fully evolved by using the methodology, as mentioned in chapter three and implemented, as discussed in chapter four. The steps involved in achieving the steganography system are as follows:

- Read secret message.
- Read cover image.
- Find the histogram of the image and determine the max and min values.
- Evaluate the performance of the robustness of the stego-image by applying the Chi-Square attack.
- Extract the secret codes by applying inverse quad-tree method and peak-valley.



### 5.3 Future Work

Knowledge in a permanent continuation does not stop as long as life goes on, just like the human mind in a work in progress. This research comprises of a lot of work so the following issues are suggested as future work:

- Apply this technique on different types of image formats such as gif and bmp format with different sizes of the cover image.
- The embedded data are randomly selected which include letters and numbers.
- Try to apply other kinds of attack to check the robustness of the embedding process such as histogram.



## REFERENCES

- [1] Nivedhitha R, Meyyappan DT, Phil M. Image security using steganography and cryptographic techniques. *International Journal of Engineering Trends and Technology*. 2012; **3(3)**:366-71.
- [2] K. R. Babu et al, "A Survey on Cryptography and Steganography Methods for Information Security," *International Journal of Computer Applications* (0975 – 8887), **12 (2)**, PP. 13-17, November 2010
- [3] R. Oppliger, "SSL and TLS: Theory and Practice," ARTECH HOUSE, 2014.
- [4] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)," pp. 1–1027, January 1996.
- [5] Km. Pooja, Arvind Kumar, "Steganography- A Data Hiding Technique" *International Journal of Computer Applications* ISSN 0975 – 8887, **9 (7)**, November 2010.
- [6] Petitcolas et al., 1999] Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. (1999). Information hiding — a survey. *Proceedings of the IEEE*, **87(7)**:1062–1078.
- [7] Herodotus. (1992).the Histories. In Herodotus, the Histories (pp. Chapter 5 - Terpischore). New York: J.M. Dent & Sons, Ltd.
- [8] Wilkins, E. (1954). A History of Italian Literature. London: Oxford University Press.
- [9] Kahn, D. (1996). The Rise of the West. In D. Kahn, the Code Breakers - The Comprehensive History of Secret Communication from Ancient Times to the Internet (pp. 106-125). New York: Scribner.

- [10] Brewster, D. (1857). Microscope, volume XIV. Encyclopedia Britannica or the Dictionary of Arts, Sciences, and General Literature - Application of photography to the microscope. Edinburgh.
- [11] Brassil, J., Low, S., Maxemchuk, N., & O'Gorman, L. (1995). Hiding information in document images. Proceedings of the Conference on Information Sciences and Systems, CISS (pp. 482-489). Baltimore: John Hopkins University.
- [12] Fridrich, J. (2010). Introduction. In J. Fridrich, Steganography in Digital Media - Principles, Algorithms, and Application (pp. 6-7). New York: Cambridge University Press.
- [13] Stanescu, D., Stangaciu, V., & Stratulat, M. (2010). Steganography on new generation of mobile phones with image and video processing abilities. 2010 International Joint Conference on Computational Cybernetics and Technical Informatics (ICCC-CONTI), (pp. 343-347 ). Timisoara.
- [14] Debattista, K. (2010, January 11). TalkTechToMe. Retrieved November 24, 2011, from The Threats of Steganography. Available at: <http://www.gfi.com/blog/threats-steganography/>
- [15] McCullagh, D. (2001, February 7). Wired. Retrieved November 29, 2011, from Bin Laden: Steganography Master?. Available at: <http://www.wired.com/politics/law/news/2001/02/41658?currentPage=all>
- [16] G. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2015, pp. 423-430.
- [17] S. Goel, S. Gupta, N. Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions", Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer 2014-2015, pp. 105-112.
- [18] D. Baby, J. Thomas, G. Augustine, E. George, N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on

Information and Communication Technologies (ICICT), *Procedia Computer Science*, April 2015, pp. 612-618.

[19] B. Feng, W. Lu, and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", *IEEE transactions on Information Forensics and Security*, Feb. 2015.

[20] M. Nusrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm", 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), Feb 2015, pp. 102-107.

[21] N. A. Al-Otaibi, and A. A. Gutub, "2-Layer Security System for Hiding Sensitive Text Data on Personal Computers", *Lecture Notes on Information Theory*, June 2014, pp. 151-157.

[22] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", *IEEE International Conference on Informatics, Electronics & Vision (ICIEV)*, May 2014, pp. 1-6.

[23] K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", *Elsevier International Journal of Information Sciences*, Sept. 2014, pp. 90-101.

[24] A.Nag, J.P. Singh, S. Biswas, D. Sarkar, and P.P. Sarkar, "A Huffman Code Based Image Steganography Technique", 1st International Conference on Applied Algorithm (ICAA) , Jan. 2014, pp. 257-265.

[25] N. Akhtar, S. Khan and P. Johri, "An Improved Inverted LSB Image Steganography", *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Feb. 2014, pp. 749-755.

[26] P.U. Deshmukh and T.M. Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique" *IEEE International Conference on Information Communication and Embedded Systems (ICICES)*, Feb. 2014, pp. 1-5.

- [27] E. Dagar and S. Dagar, "LSB based Image Steganography using X-Box Mapping", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 2014, pp. 351-355.
- [28] M. R. Modi, S. Islam and P. Gupta, "Edge Based Steganography on Colored Images", 9th International Conference on Intelligent Computing (ICIC), July 2013, pp. 593-600.
- [29] D. Samidha and D. Agrawal, "Random Image Steganography in Spatial Domain" IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), Jan. 2013, pp. 1-3.
- [30] S. Gupta, G. Gujral and N. Aggarwal, "Enhanced Least Significant Bit Algorithm for Image Steganography", International Journal of Computational Engineering & Management, July 2012, pp. 40-42.
- [31] S. Sachdeva and A. Kumar, "Colour Image Steganography Based on Modified Quantization Table", Proceedings of IEEE 2nd International Conference on Advanced Computing & Communication Technologies, Jan. 2012, pp. 309-313.
- [32] S. M. M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th IEEE International Conference on Computer and Information Technology, Dec. 2011, pp. 286-29.
- [33] X. Qing, X. Jianquan and X. Yunhua., "A High Capacity Information Hiding Algorithm in Color Image", Proceedings of 2nd IEEE International Conference on E-Business and Information System Security, May 2010, pp. 1-4.
- [34] Che-Wei Lee and Wen-Hsiang Tsai, "A New Steganographic Method Based on Information Sharing via PNG Images", IEEE 2nd International Conference on Computer and Automation Engineering (ICCAE), Feb. 2010, pp. 807-811.
- [35] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", *Journal of Radio Engineering*, **18(4)**, pp. 509-516, 2009.

- [36] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering (IJCSE), 2009 pp. 137-141.
- [37] D. Debnath, S. Deb, N. Kar, "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography", IEEE International Conference on Computational Intelligence and Networks (CINE), Jan. 2015, pp. 178-183.
- [38] D. E. M. Ahmed and O.O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography", IEEE International Conference on Computer and Communication Engineering (ICCCE), Sept. 2014, pp. 288-291.
- [39] S. Krishnagopal, S. Pratap, and B. Prakash, "Image Encryption and Steganography Using Chaotic Maps with a Double Key Protection", 4th International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing, Dec. 2014, pp. 67-78.
- [40] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advanced in Control Engineering and Information Science, Dec. 2011, pp. 2767-2772.
- [41] Fridrich J, Goljan M, editors. Practical steganalysis of digital images-state of the art. Proceedings of SPIE; 2002.
- [42] Wu, H. C., Wu, N. I., Tsai, C. S. and Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Vision, Image and Signal Processing, IEE Proceedings -, **152(5)**, 611-615.
- [43] Fridrich, J. Goljan, M. and Soukal, D. (2003). Higher-Order Statistical Steganalysis of Palette Images. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V, Santa Clara, California, 178-190.

- [44] Lin Y-C, Li T-S. Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram Shifting. *Journal of multimedia*. 2011; **6(4)**: 349-58.
- [45] Xiong, J.J. and Shenoi, R.A., A Load History Generation Approach for Full-scale Accelerated Fatigue Tests, *Engineering Fracture Mechanics*, **75**, 2008, pp. 3226-3243.
- [46] Chung K-L, Huang Y-H, Yang W-N, Hsu Y-C, Chen C-H. Capacity maximization for reversible data hiding based on dynamic programming approach. *Applied mathematics and computation*. 2009; **208(1)**:284-92.
- [47] Ahmad AM, Sulong G, Rehman A, Alkawaz MH, Saba T. Data hiding based on improved exploiting modification direction method and Huffman coding. *Journal of Intelligent Systems*. 2014; **23(4)**:451-9.