SPATIAL DOMAIN IMAGE STEGANOGRAPHY BASED ON RIGHT MOST DIGIT REPLACEMENT AND PARITY BIT DIFFERENCING

MEHDI HUSSAIN

FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2017

SPATIAL DOMAIN IMAGE STEGANOGRAPHY BASED ON RIGHT MOST DIGIT REPLACEMENT AND PARITY BIT DIFFERENCING

MEHDI HUSSAIN

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2017

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: Mehdi Hussain

Matric No: WHA140027

Name of Degree: Doctor of Philosophy

Title of Thesis: ("Spatial Domain Image Steganography Based On Right Most Digit Replacement and Parity Bit Differencing")

Field of Study: Computer Science (Information Security)

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:

Subscribed and solemnly declared before,

Witness's Signature Date:

Name: Dr.Ainuddin Wahid Abdul Wahab

Designation: Sen. Lecturer, FSKTM, University Malaya

UNIVERSITI MALAYA

PERAKUAN KEASLIAN PENULISAN

Nama: Mehdi Hussain

No. Matrik: WHA140027

Nama Ijazah: Doctor of Philosophy

Tajuk Tesis: ("Spatial Domain Imej Steganografi Berdasarkan Penggantian Digit Paling Kanan Dan Pembezaan Bit Pariti")

Bidang Penyelidikan: Computer Science (Information Security)

Saya dengan sesungguhnya dan sebenarnya mengaku bahawa:

(1) Saya adalah satu-satunya pengarang/penulis Hasil Kerja ini;
(2) Hasil Kerja ini adalah asli;
(3) Apa-apa penggunaan mana-mana hasil kerja yang mengandungi hakcipta telah dilakukan secara urusan yang wajar dan bagi maksud yang dibenarkan dan apa-apa petikan, ekstrak, rujukan atau pengeluaran semula daripada atau kepada mana-mana hasil kerja yang mengandungi hakcipta telah dinyatakan dengan sejelasnya dan secukupnya dan satu pengiktirafan tajuk hasil kerja tersebut dan pengarang/penulisnya telah dilakukan di dalam Hasil Kerja ini;
(4) Saya tidak mempunyai apa-apa pengetahuan sebenar atau patut semunas
(5) abahnya tahu bahawa penghasilan Hasil Kerja ini melanggar suatu hakcipta hasil kerja yang lain;
(6) Saya dengan ini menyerahkan kesemua dan tiap-tiap hak yang terkandung di dalam hakcipta Hasil Kerja ini kepada Universiti Malaya ("UM") yang seterusnya mula dari sekarang adalah tuan punya kepada hakcipta di dalam Hasil Kerja ini dan apa-apa pengeluaran semula atau penggunaan dalam apa jua bentuk atau dengan apa juga cara sekalipun adalah dilarang tanpa terlebih dahulu mendapat kebenaran bertulis dari UM;
(7) Saya sedar sepenuhnya sekiranya dalam masa penghasilan Hasil Kerja ini saya telah melanggar suatu hakcipta hasil kerja yang lain sama ada dengan niat atau sebaliknya, saya boleh dikenakan tindakan undang-undang atau apa-apa tindakan lain sebagaimana yang diputuskan oleh UM.

Tandatangan Calon Tarikh:

Diperbuat dan sesungguhnya diakui di hadapan,

Tandatangan Saksi Tarikh:

Nama: Dr.Ainuddin Wahid Abdul Wahab

Jawatan: Sen. Lecturer, FSKTM, University Malaya

ABSTRACT

The rapid advancement in digital computation, communication and exponential proliferation of the Internet has now become the easiest and economical way of data transmission. This evolution has gained the drawbacks in the advancement of forgery tools and application that enable perpetrators to steal, alter and destroy information during transmission. However, encryption and steganography are the most effective solutions to secure sensitive data to avoid malicious and forgery activities. In encryption, sensitive information transforms into meaningless data with observable existence, while steganography embeds the secret information inside an object (i.e. image, video, text, and audio) with invisible existence. There has been noteworthy research on image based steganography techniques to overcome the various challenges i.e. lower embedding capacity, imperceptibility, embedding efficiency and robustness against steganalysis detection attacks. However, most of the existing embedding algorithms are incapable of overcoming the adverse effects of the challenges simultaneously. In general, high capacity based methods i.e. LSB substitution, employed the multi-bit-planes for concealing the secret data that eventually modify the cover pixel values and becomes more prominent although human vision are not able to identify those changes. Consequently, these pixels changes generate various detectable artifacts i.e. dissimilarity or significant difference errors between cover and stego-pixels, that eventually leads the steganalysis methods to exploit these effects to expose the presence of secret data. The proposed right most digit replacement (RMDR) method deals with these challenges by substituting the digits instead of bits. The closest selection of digits substitution reduces the differences error between cover and stego-pixels. Furthermore, the RMDR has proven to be the best alternative to the existing LSB-based substitution techniques with enhanced imperceptibility and security against regular and singular (RS) steganalysis. The second proposed method is Parity Bit adjustment in Pixel Value Difference (PBPVD). The PBPVD method efficiently exploits the Pixel Value Difference (PVD) adjustment process to conceal extra secret data with the correlation of parity bits. Consequently, it improves the embedding capacity while retaining the imperceptibility. Furthermore, the PBPVD adjustment process would be ideal to exploit in all existing PVD-based techniques to enhance its capacity without degrading the visual quality. Finally, this research proposed hybrid embedding methods by integrating the above RMDR and PBPVD techniques to achieve the optimal steganography objectives. A comparative study presented between the proposed and the existing steganographic techniques. For imperceptibility, distortion between cover and stego-images assessed by utilizing the Peak signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) and Universal Quality Index analysis (Q) matrices. For security aspect, the robustness against steganalysis detection attacks evaluated by RS, pixel difference histogram, and bit-plane analysis. Results from the above evaluations have proven that proposed methods achieved the optimal performance regarding general steganography objective/challenges. In addition, the proposed methods have proven the robustness against powerful modern SPAM feature based steganalysis detection attacks at low embedding rate.

ABSTRAK

Perkembangan yang pesat dalam pengiraan digital, komunikasi dan Internet menjadikan penghantaran data bagi interaksi kerajaan, perdagangan dan sosial lebih mudah dan menjimatkan. Sementara itu, kemajuan dalam aplikasi dan alat pemalsuan juga boleh mengubah, mencuri dan memusnahkan maklumat semasa penghantaran. Walau bagaimanapun, penyulitan dan steganografi merupakan penyelesaian yang paling berkesan untuk melindungi data sensitif. Dalam penyulitan, maklumat sensitif ditukar menjadi data sifer yang tidak boleh difahami tanpa menyembunyi kewujudannya, manakala steganografi menyembunyikan kewujudan maklumat rahsia di dalam objek seperti imej, video, teks, dan audio). Sementara itu, terdapat kajian dalam teknik steganografi imej untuk mengatasi pelbagai cabaran iaitu pembenaman berkapasiti tinggi, ketakbolehkelihatan, kecekapan pembenaman dan keteguhan terhadap serangan pengesanan steganalisis. Walau bagaimanapun, teknik pembenaman yang sedia ada tidak dapat mengatasi cabaran yang dinyatakan secara serentak. Secara umumnya, teknik-teknik berasaskan kapasiti tinggi seperti penggantian LSB, menggunakan pelbagai bit-planes untuk menyembunyikan data rahsia yang akhirnya mengubah suai nilai piksel dan menjadi ketara walaupun penglihatan manusia tidak dapat mengenal pasti perubahan tersebut. Akibatnya, perubahan nilai piksel menghasilkan pelbagai artifak yang boleh dikesan iaitu perbezaan atau ralat perbezaan yang ketara antara stego dan piksel yang membolehkan teknik steganalysis untuk mengeksploitasi kesan-kesan ini untuk mendedahkan steganografi. Penggantian angka digit paling kanan (RMDR) yang dicadangkan mengatasi cabaran ini dengan menggantikan nilai digit dari menggantikannya dengan nilai bit. Pemilihan digit yang terdekat bagi penggantian mengurangkan ralat perbezaan antara stego dan piksel. Selain itu, RMDR juga terbukti sebagai alternatif terbaik kepada teknik berdasarkan penggantian LSB dengan peningkatan ketakbolehkelihatan dan keselamatan terhadap serangan pengesanan steganalisis statistikal regular dan singular (RS). Teknik kedua yang dicadangkan adalah pelarasan Parity Bit dalam Pixel Value Difference (PBPVD). Kaedah PBPVD cekap mengeksploitasi proses pelarasan Pixel Value Difference (PVD) untuk menyembunyikan data rahsia tambahan dengan korelasi bit parity. Hasilnya, ia meningkatkan kapasiti pembenaman sambil mengekalkan ketakbolehkelihatan. Tambahan pula, proses pelarasan PBPVD boleh dieksploitasi dalam teknik yang berasaskan PVD yang sedia ada untuk meningkatkan kapasiti mereka tanpa mengurangkan kualiti visual. Akhir sekali, kajian ini mencadangkan teknik pembenaman hibrid dengan mengintegrasikan teknik RMDR dan PBPVD bagi mencapai objektif-objektif steganografi yang optimum. Selain itu, satu kajian perbandingan dibentangkan antara teknik steganografi yang dicadangkan dan teknik steganografi yang sedia ada. Bagi ketakbolehkelihatan, herotan antara penutup dan stego-imej dinilai menggunakan matrik Peak signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) dan Universal Quality Index analysis (Q). Bagi aspek keselamatan, keteguhan terhadap serangan pengesanan statistik steganalysis dinilai oleh RS, perbezan pixel histogram dan bit-plane analisis. Di samping itu, keteguhan terhadap steganalysis moden iaitu ciri-ciri SPAM berdasarkan klasifikasi ensemble juga dinilai. Keputusan dari penilaian diatas telah membuktikan bahawa teknik yang dicadangkan mencapai prestasi optimum bagi objektif / cabaran umum steganografi. Selain itu, teknik yang dicadangkan dapat bertahan moden ciri SPAM berdasarkan serangan pengesanan steganalysis yang hebat pada kadar pembenaman yang rendah.

ACKNOWLEDGEMENTS

First, I would like to thank **ALLAH THE MOST GRACIOUS AND MERCIFUL**, **WHO** gave me health and energy to successfully complete my PhD study. I would like to express sincerest gratitude towards my supervisor Dr.Ainuddin Wahid Abdul Wahab, for providing me the opportunity to work under his calm and healthy research environment. Similarly, my co-supervisors Dr. Mohd Yamani Idna Idris and Dr. Noman Javed also supported throughout my PhD journey. Without my supervisors' guidance, motivation and support, this thesis would never come to light. I cannot forget the name of Prof. Dr. King Jung, for his valuable comments, suggestions and discussion regarding publications.

Furthermore, I would like to gratitude to my parents (Mukhtar Hussain, Kausar Mukhtar), for their prayers and support in each and every aspect of my life. My sincere gratitude also goes to my wife Rida Zahra and sons (Muwahid Mehdi, Wasam Mehdi) for their patience and goodwill. I would also thanks to rest of my family (Mahwish Mukhtar, Muzamil Hussain, Mahreen Mukhtar and Imtiaz Hussain) for their moral support.

Finally, I would like to gratitude to the National University of Science and Technology (NUST), Islamabad, Pakistan, for sponsoring my postgraduate study. Also special thanks to University of Malaya (UM) for giving me the chance to complete my PhD study.

TABLE OF CONTENTS

CHAPTER 6: CONCLUSION AND FUTURE WORK 182

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

ALSB	:	Adaptive Least Significant Bit
bpp	:	Bits Per Pixel
dB	:	Decibel
DCT	:	Discrete Cosine Transform
DFT	:	Discrete Fourier Transform
DIH	:	Difference Image Histogram
EMD	:	Exploiting Modification Directions
GLM	:	Gray Level Modification
GLSB	:	Generalized Least Significant Bit
LSB	:	Least Significant Bit
LSBM	:	Least Significant Bit Matching
LSBR	:	Least Significant Bit Replacement
MBNS	:	Multi-Base Notation System
ML	:	Machine Learning
MLE	:	Multi-Level Encryption
MPE	:	Modification of Prediction Error
MSB	:	Most Significant Bit
MSE	:	Mean Square Error
OPAP	:	Optimal Pixel Adjustment Process
PSNR	:	Peak Signal-to-Noise Ratio
PPM	:	Pixel Pair Matching
PVD	:	Pixel Value Differencing
RMSE	:	Root Mean Square Error
RS	:	Regular and Singular
SPAM	:	Subtractive Pixel Adjacency Matrix
SVM	:	Support Vector Machine

CHAPTER 1: INTRODUCTION

In this chapter, an introduction to information hiding and the motivation behind this research work is presented. Next, the problem statement, research questions, research objectives, and scope defined. A brief description of the contribution and significance of this research work is also highlighted. Finally, the outline of the thesis is described.

1.1 Introduction

The evolution of the internet has led to the rapid communication of information using digital content (i.e. images, audio, textual documents, and videos). This evolution has gained the drawbacks in the advancement of forgery tools and applications that enable perpetrators to steal alter and destroy information in the process of transmission. In order to address the security of information and preventing it from manipulation, a security system is introduce to provide two main disciplines: information encryption and information hiding (Figure 1.1).

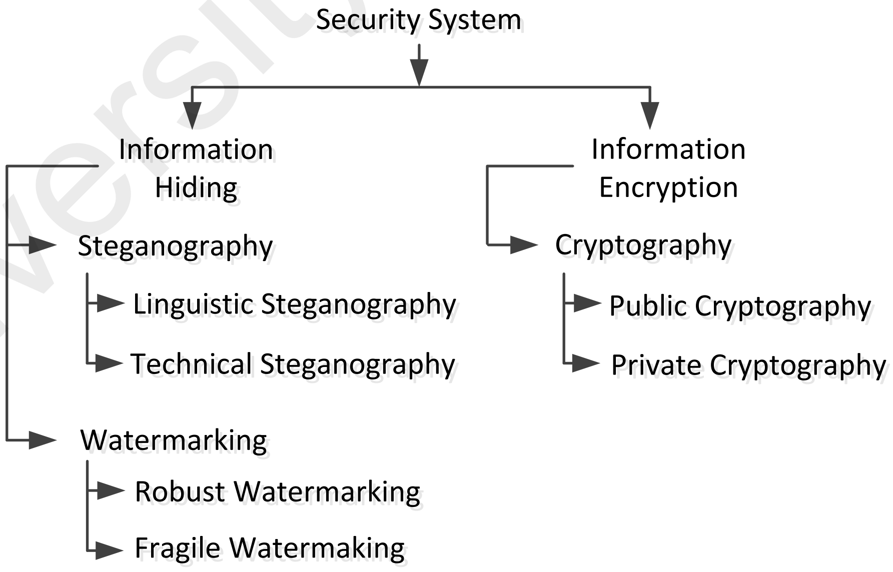


Figure 1.1: General Classification of the Security System

Information encryption known as cryptography that scrambles the secret information into an unreadable string of characters that can only be decoded by intended recipient using "agreed upon" procedure. However, cryptography is not full proof from scamming activities in the sense that an unauthorized intruder may inject and incorporate unintended data to the information, which can tamper the transmitted information. In addition, in some cases, it is always incompetent of encrypting secret information because it may potentially draw attention. Therefore, it requires an invisible communication in some cases. This is the main reason why information hiding mechanism is needed.

Information hiding is the art and science of concealing secret message in such a way that its presence cannot be detected (Katzenbeisser & Petitcolas, 2000). This can be achieved by steganography and watermarking, as shown in Figure 1.1. The steganography and watermarking are closely related to each other, but both based on different objectives. The watermarking protects the integrity of secret data with or without concealing the existence of communication, generally used to protect the intellectual copyrights. In contrast, the main concern of steganography is to conceal the existence of communication and protect the secret data from unauthorized access (Katzenbeisser & Petitcolas, 2000; Subhedar & Mankar, 2014).

Recently, steganography has commonly become a popular mechanism for protecting sensitive communications. For example, Armed forces may exchange military secret maps or surveillance video in a hostile environment (Jenifer, Yogaraj, & Rajalakshmi, 2014). Modern health care system protects patients' critical information during exchanging or storing his or her medical images i.e. X-ray, MRI (J. Liu, Tang, & Sun, 2013). Similarly, financial and commercial organizations i.e. banks can prevent customers' account data from being illegally accessed by unauthorized users. Hence, aforementioned communication systems require the application of digital steganography that can protect its secret data efficiently. In addition, the interest of academic researchers in steganography and counterpart as steganalysis domain is depicted in the graph (Figure 1.2). The overall graph shows the amalgam of up and downs of interest, but since 2010 this field again depicting more and consistent interest of the scientific community by the increasing number of published articles.

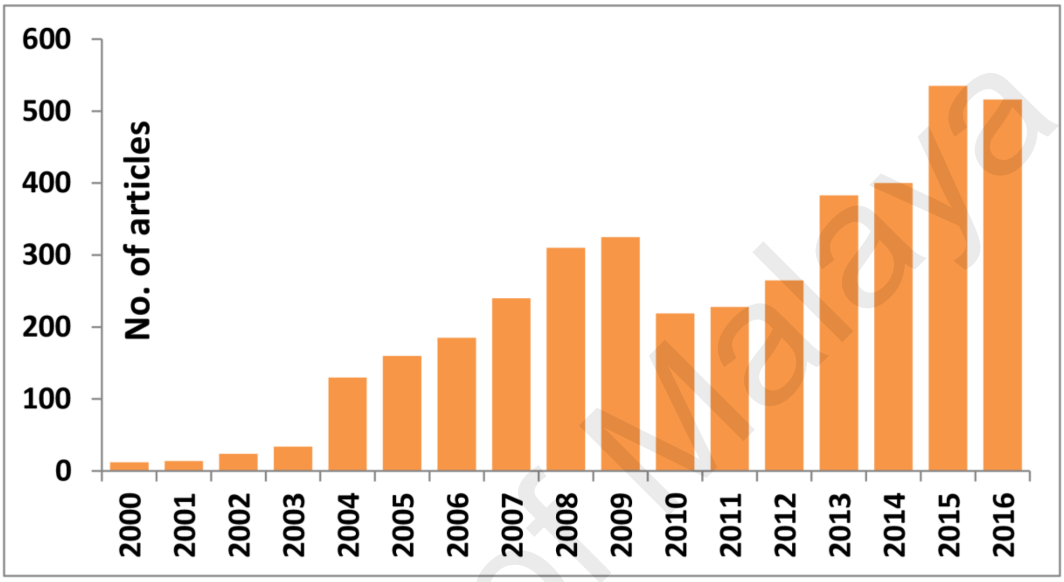


Figure 1.2: The Number of "Web of Science" Annual Journal and Conference Publications containing the words 'Steganography' or 'Steganalysis'.

However, in steganography mechanism, the selection of the medium plays a vital role. According to (Zielińska, Mazurczyk, & Szczypiorski, 2014), the best medium for embedding secret information must possess two features. The medium should be popular and the modification in the medium should not be visible to the third party. To the best of our knowledge, the image is the most widely used medium in existing digital steganography literature. Meanwhile, the images are easily available due to advanced and low-cost devices with inexpensive internet technology. Furthermore, the image has high frequency of redundancy, which allows concealing the secret data with invisible effects. Therefore, the focus of this research is on image-based steganography. In Chapter 2, detailed accounts of image steganography components and its classifications i.e. spatial and transform domain will be given.

The most common success criteria for any image-based steganography method are evaluated by the following key objectives: First, embedding payload, how maximum the embedding capacity can be achieved in stego-image? Second, imperceptibility, how much the stego-image is perceptually identical to its original/cover image? Third, security, how can a stego-image resist the different steganalysis detection attacks? Therefore, the ideal steganographic method must fulfill the above objectives simultaneously or at least keep balance to maintain the highest ratio of capacity, visual quality, and security.

In literature, there are different types of image steganography techniques that are employed to achieve the aforementioned steganographic objectives. The common steganography methods include the least significant bit (LSB), pixel value differencing (PVD), exploiting modification directions (EMD), pixel pair matching (PPM), prediction error, edge based, histogram based and even integration of all the methods as hybrid steganographic algorithms (Subhedar & Mankar, 2014).

In this study, the main focus will be on LSB substitution, pixel value differencing and its integration as hybrid steganography methods. This is because substitution and pixel value differencing techniques are more common and are widely employed in spatial domain image steganography to achieve the success criteria of steganographic objectives (Cheddad, Condell, Curran, & Mc Kevitt, 2010).

1.2 Problem Statement

There are numbers of substitution and pixel differencing based steganographic algorithms found in the literature to achieve high capacity, imperceptibly and security. In substitution based steganography, the LSB embedding method is considered the most common and well-known, that directly replaces the *k*-rightmost LSBs of a pixel with *k* secret bits (Chan & Cheng, 2004). Similarly, various LSB-based methods have been proposed by adopting the different embedding strategies. Similarly, LSB-based hybrid schemes also introduced to tackle or achieve the steganographic objectives. For example, an adaptive LSB (H. Yang, Sun, & Sun, 2009) method employs the variable LSBs based on edge and smooth image regions. As a result, it achieves the higher visual quality +39 (as peak signal to noise ratio PSNR dB), while the embedding capacity drops by -0.20 bits per pixel (bpp) as compared to conventional LSB embedding technique. Similarly, another edge based adaptive LSB embedding (H.-W. Tseng & Leng, 2014), also achieves the acceptable +38 dB PSNR, while reducing the embedding -0.60 bpp. Recently, an improved LSB-based scheme (Xu, Chang, Chen, & Wang, 2016) employs the modulo three strategy to embed the ternary secret data. In comparison to conventional LSB method, it improved the +0.16 bpp and maintains the higher visual quality, while unable to resist the modern steganalysis detection attack at +0.25 bpp embedding rate. Generally, to obtain a high rate of embedding capacity in LSB-based methods, this employs the maximum/multiple LSBs with secret data bits, which indirectly reflect the maximum modification difference value between cover and stego-pixels. This result in, *the maximum modification difference reduces the visual quality and increases the risk of steganalysis attacks*. However, existing high capacity based LSB schemes shows its own strengths and limitations with the trade-off in steganographic objectives (see Chapter 2).

Similarly, pixel value difference (PVD) (D.-C. Wu & Tsai, 2003) method is also considered as a well-known spatial domain steganography approach. The PVD technique readjusts the non-overlapped consecutive pixels differences for secret data embedding, that retains the higher visual quality +40 dB PSNR but achieves the +1.50 bpp as lower embedding payload. In literature, to enhance the embedding payload, a number of variations of PVD-based embedding methods are proposed. For example, Tri-way PVD, that employs the 2 pixels groups into three pixels pairs, which result in enhancing the embedding payload, while reducing the visual quality around -5.0 dB PSNR. Recently, the multi-pixel differencing (C.-H. Yang, Wang, & Weng, 2010), modulus function (F. Pan, Li, & Yang, 2011), and octonary PVD (Balasubramanian, Selvakumar, & Geetha, 2014) methods are proposed to improve the capacity and finds the tradeoff in steganographic objectives. Meanwhile, most of the PVD based methods employ the identical difference readjustment strategy where it enables the data to be embedded by adjusting new differences between the pixels group. *However, inefficient difference adjustment procedure indirectly limits the embedding payload of all PVD-based methods*. Furthermore, the rest of PVD-based schemes discussed in Chapter 2.

Recently, researcher tried to evolve the hybrid embedding methods to achieve the steganographic objectives. It was done by embedding the hybrid methods to utilize the advantages of existing singular steganographic methods such as for larger payload of LSB and high imperceptibility of PVD methods (Jung, 2010; M Khodaei & Faez, 2012; S.-Y. Shen & Huang, 2015; Swain, 2016; Y.-Y. Tsai, Chen, & Chan, 2014; H-C Wu, Wu, Tsai, & Hwang, 2005). To some extent, hybrid steganographic methods are considered as more secure, because many steganalysis detection attacks are specifically designed for targeting a singular steganography method (Fillatre, 2012; Jessica Fridrich, Goljan, & Du, 2001; Zaker & Hamzeh, 2012). *However, some of these hybrid steganographic algorithms are still vulnerable by non-structural steganalysis* (Pevny, Bas, & Fridrich, 2010).

Based on this discussion, we can say that *in high capacity based substitution methods; the problem of reducing cover and stego-pixels differences to enhance the visual quality and security has not been addressed. Similarly, in pixel value difference steganography based methods; the inefficient difference readjustment procedures between pixels group limits the embedding payload. Moreover, to achieve the optimal* *steganographic objectives in substitution and pixel value differencing methods is still challenging.*

Furthermore, the main benefit of proposing the above solutions to address the problems that may indirectly increase the visual quality, capacity and security of all existing substitution and pixel differencing methods. Subsequently, there is a need to achieve a novel way of embedding solutions that are able to simultaneously achieve optimal output for high payload (that employ the efficient embedding characteristics), good visual quality (by minimizing the difference error between cover and stego-pixels), and improve the security that reduces the steganalysis detection artifacts.

The sub-research problems are as follows:

1- Almost, all the high capacity substitution based embedding algorithms produce low visual quality of stego-image without considering the difference errors between cover and stego-pixels.

2- Inefficient usage of pixel difference adjustment process limits the embedding capacity of existing pixel value differencing algorithms.

3- Lack of maintaining the acceptable/optimal balance between capacity, imperceptibility, and security, this becomes less suitable for real-time applications.

1.3 Research Questions

This research is formulate to answer the following questions for substitution and pixel value differencing based image steganography methods in spatial domain that comes up with optimal/simultaneously enhancing visual quality, capacity and reducing the structural/statistical steganalysis detection artifacts respectively:

1. Substitution based image steganography
    i. How does substitution based image steganography method in spatial domain improve the visual quality and security against steganalysis while retaining the high embedding capacity?
    ii. How does the selection of closest/similar stego-pixels against respective cover-pixels affect the visual quality of substitution-based stego-images?
    iii. Can a new substitution embedding method efficiently integrate as a hybrid adaptive steganography in order to enhance the visual quality and/or capacity while reducing structural/statistical steganalysis detection artifacts?
2. Pixel differencing based image steganography
    i. How does a pixel value difference image steganography method improve the embedding capacity and security against steganalysis while retaining the acceptable visual quality?
    ii. How can parity bit difference adjustment process of stego-pixels against secret data bits affect the embedding capacity of pixel value difference based stego-image?
    iii. Can a new pixel difference adjustment method efficiently integrate as a hybrid adaptive steganography in order to enhance the capacity and security while maintaining the acceptable visual quality?

1.4 Research Objective

The aim of this study is to propose novel substitution and pixel differencing based singular and hybrid spatial domain image steganography methods. The following objectives that are to be achieved in order to attain the aim of this research:

1. To propose spatial domain image steganography methods based on digits substitutions with the increase of similarity between cover and stego-pixels. The sub-objectives under this main objective include:
   a. To investigate the issues in high embedding capacity based LSB substitution steganography methods.
   b. To design and implement the singular and hybrid steganography methods to enhance the visual quality and embedding capacity using digit substitution.
   c. To evaluate the performance of the proposed methods against existing singular and hybrid LSB-based substitution techniques over larger and various textures based image datasets.
2. To propose spatial domain image steganography methods based on parity bit pixel value differencing with the correlation of secret bits. The sub-objectives under this main objective include:
   a. To investigate the issues in high visual quality and high embedding capacity based PVD steganography methods.
   b. To design and implement the parity bit singular and hybrid steganography methods to improve the embedding capacity and security without degrading the visual quality of existing PVD-based methods.
   c. To evaluate the performance of the proposed methods against existing singular and hybrid PVD-based steganography techniques over larger and various textures based image datasets.

1.5 Thesis Contribution

This study proposed efficient image-based data hiding methods in the spatial domain to enhance the embedding capacity, visual quality and reduce the steganalysis detection artifacts of stego-images. The contributions are as below:

1. The literatures expose the limitations of existing singular and hybrid spatial domain image steganographic methods.
2. A new spatial domain image steganographic method is implemented using digits substitution to enhance the visual quality and security without sacrificing the embedding capacity.
3. A new spatial domain image steganographic method is implemented to improve the embedding capacity of existing PVD-based methods with similar visual quality and security.
4. This research proposes two new hybrid steganography methods by integrating the above-proposed techniques to achieve optimal performances in embedding capacity, security, and imperceptibility.
5. Finally, future research directions in the spatial domain of digital image steganography are provided.

1.6 Significance of Research

This research provides novel image based steganography algorithms in the spatial domain. The current limitations associated with existing image-based steganographic methods are highlighted. The output of this research will benefit the intelligent services, government agencies, e-commerce industry to secure financial credentials. Furthermore the multimedia industry as an access control system for digital content distribution, and are able to optimize Web image search engine through digital image indexing using steganography. Furthermore, the proposed methods of this research can be applied in existing applications that require the optimal steganography objectives (in term of high capacity, acceptable visual quality, security against structural/statistical steganalysis detection attacks). In addition, new researches in this field can apply the proposed methods as a benchmark for designing new upcoming steganography methods.

1.7 Thesis Organization

This thesis contains six chapters. Chapter 2 reviews related work of image steganography methods in spatial domain in order to investigate the embedding capacity, visual imperceptibility, and steganalysis detection attacks. Chapter 3 presents a general discussion of the research methodology that is employed in carrying out the research study. The proposed digit substitution based singular and its hybrid version of image steganography algorithms are presented in Chapter 4. In Chapter 5, the second proposed method of parity bit pixel values differencing with its hybrid embedding variation are presented. Finally, Chapter 6 summarizes and concludes the research findings. The complete thesis organization can be seen in Figure 1.3.

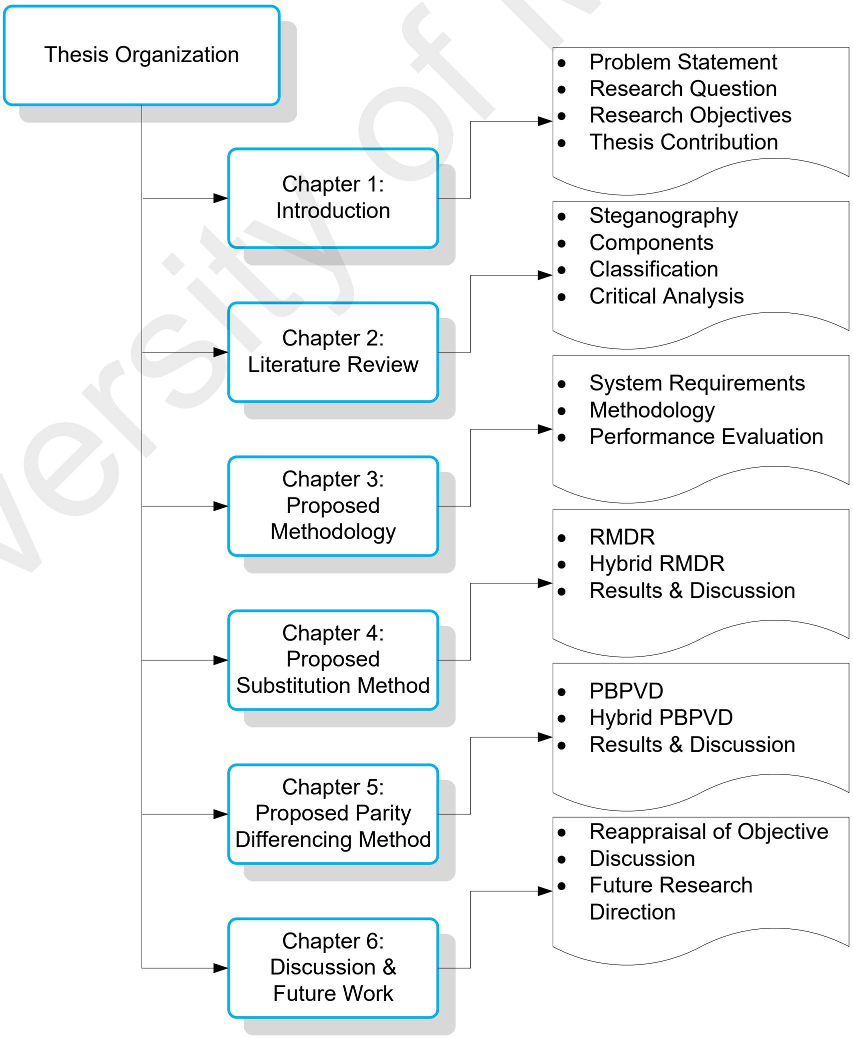


Figure 1.3: Thesis Organization Chart

CHAPTER 2: LITERATURE REVIEW

In this chapter, knowledge of digital steganography, basics of image steganography, including components and classifications are discussed to effectively understand the remaining chapters of the thesis. The general steganography objectives are highlighted with its most common performance evaluation metrics. Furthermore, the literature review related to the substitution and pixel value differencing techniques are presented. Meanwhile, we exploited the other most common steganography approaches that are directly or indirectly involved in the research problem. Subsequently, we presented the comprehensive analysis of all existing steganography techniques based on its embedding capacity, visual quality and security aspects. We highlighted the issues with respect to improving embedding capacity and quality. Furthermore, this chapter presented the overview of proposed techniques. Finally, summarized the chapter with conclusive remarks.

2.1 Digital Steganography

The word ‘Steganography’ derived from the Greek words “stego” and “graphia” which means “covered” “writing”. There are various ancient steganography mechanisms exist e.g. in 440 B.C. Histiaeus shaved the head of his most trusted slave and tattooed it with a secret message which disappeared after the hair had regrown and used for communication etc. (Petitcolas, Anderson, & Kuhn, 1999).

In modern days, the steganography is employed by different digital communication mediums, such as images, videos, audios, text documents and even with different digital services and devices (Figure 2.1). Generally, digital mediums utilize its various characteristics for embedding secret data. For example, text-based steganography uses the line/word shift (Alattar & Alattar, 2004) encoding and recently employs the emoticons in textual chat to achieve secret communication (Y. Liu, Yang, & Xin, 2015). Generally, a phase coding, spread spectrum, and low-bit encoding are employed in audio based steganography (Djebbar, Ayad, Meraim, & Hamam, 2012). For network protocol based steganography methods, directly embed the secret data into packet payload, packet headers (Murdoch & Lewis, 2005) and even utilize the behavior of acknowledgment and retransmission of packets known as retransmission steganography (Mazurczyk, Smolarczyk, & Szczypiorski, 2011). DNA-based steganography, characteristics of randomness in DNA can be employed to embed the secret data, e.g. recently a technique uses the numerical mapping table to map the DNA sequence for encoding secret data (Santoso, Suk-Hwan, Hwang, & Ki-Ryong, 2015). In video steganography, the combination of image and audio steganography are often used, where it also has more depth to achieve the maximum secret data embedding because the video is considered as a combination of images (Sadek, Khalifa, & Mostafa, 2015). The area of concern for the present thesis is image-based steganography and is dealt in detail in the next section.

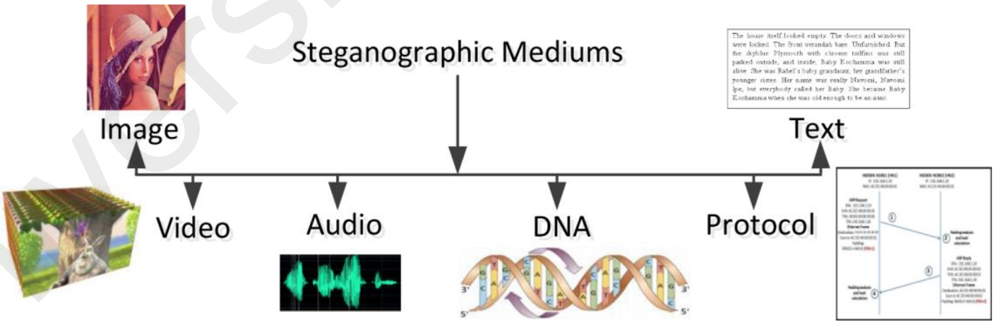

Steganographic Mediums
Image
The house itself looked empty. The doors and windows were locked. The front verandah bare. Unfurnished. But the skyblue Plymouth with chrome tailfins was still parked outside, and inside, Baby Kochamma was still alive. She was Rahel's baby grandaunt, her grandfather's younger sister. Her name was really Navomi, Navomi Ipe, but everybody called her Baby. She became Baby Kochamma when she was old enough to be an aunt.
Text
Video
Audio
DNA
3'
5'
3'
5'
Protocol

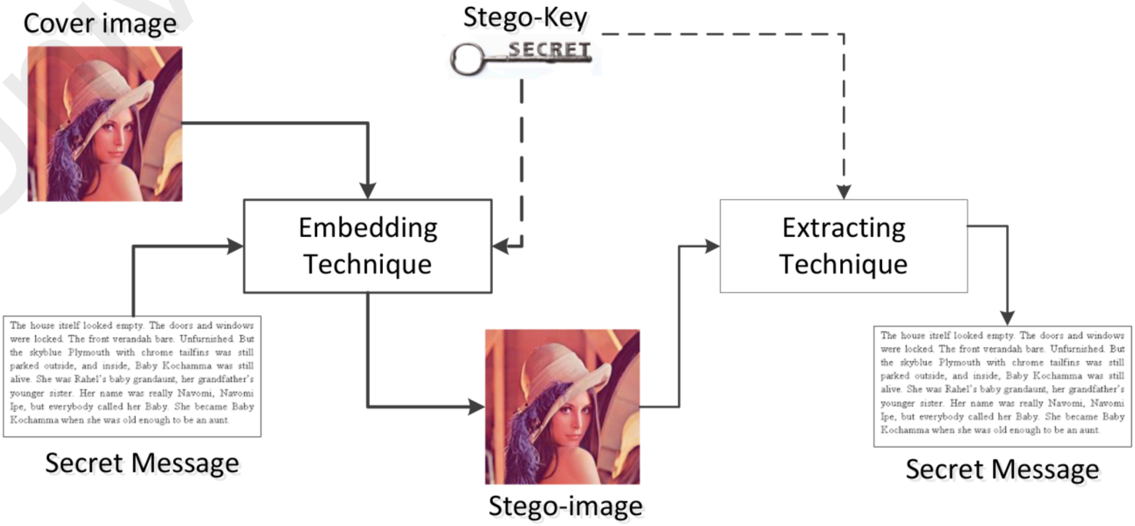
Figure 2.1: General Steganography Mediums

2.2 Image Steganography

In image steganography, the image is used to conceal the secret/sensitive information. It has received more popularity in recent years, perhaps with the advent of low-cost digital cameras and high-speed distribution channels as an inexpensive internet and advanced technology. As mentioned earlier, (Zielińska et al., 2014) highlighted that the selection of the best medium for steganography must have two properties. First, before and after concealing the secret data the medium is able to maintain the high imperceptibility. Second, it should be common and popular because that creates the less attention to the third party. Therefore, in the literature of digital steganography, the image is found to be the most common/popular medium due to having a high frequency of redundancy and also able to conceal the secret data inside together with invisible effects.

2.2.1 Components of Image Steganography

In this section, the basic component of image-based steganography is discussed. As shown in Figure 2.2, the term “secret message” is the sensitive data that is used to communicate secretly. The “cover image” is the original image which is used to hide the “secret message”. The “embedding technique” is actually the procedure or algorithm that is used to hide the “secret message” inside the “cover image” namely “stego-image”. The “stego-key” contains the embedding and extracting algorithm characteristics that used for concealing and recovering of “secret message”. The “stego-image” denotes the final output image that conceals the secret information. Similarly, the counterpart of embedding is the extraction, where “extraction technique” is the process to recover the “secret message” from “stego-image” using optional “stego-key”.



The house itself looked empty. The doors and windows were locked. The front verandah bare. Unfurnished. But the skyblue Plymouth with chrome tailfins was still parked outside, and inside, Baby Kochamma was still alive. She was Rahel’s baby grandaunt, her grandfather’s younger sister. Her name was really Navomi, Navomi Ipe, but everybody called her Baby. She became Baby Kochamma when she was old enough to be an aunt.

The house itself looked empty. The doors and windows were locked. The front verandah bare. Unfurnished. But the skyblue Plymouth with chrome tailfins was still parked outside, and inside, Baby Kochamma was still alive. She was Rahel’s baby grandaunt, her grandfather’s younger sister. Her name was really Navomi, Navomi Ipe, but everybody called her Baby. She became Baby Kochamma when she was old enough to be an aunt.

Figure 2.2: Basic Image Steganography Model

2.2.2 Classifications of Image Steganography

In literature, various types of image steganographic methods have been proposed and most of them use a distinct approach of embedding. If we classify them according to model/approach based technique that can be further divided into different types depending on their implementation. Even though it is impossible to exactly classify all of them, but we divided them into general categories as shown in Figure 2.3. In Figure 2.3 (a), one way is to classify according to the embedding domain, where spatial and transform domains adopted by (Johnson & Jajodia, 1998) and briefly discussed in section 2.2.2.1 and 2.2.2.2. Furthermore, the both domain-based embedding methods target the same steganography objectives i.e. payload, visual quality, and security as highlighted in Figure 2.3 (a). Recently, adaptive embedding strategies are evolved in both spatial and frequency domains, where the underline embedding algorithms exploit the different statistical image characteristics to adapt or determine the size of secret data for embedding. For example, (Ioannidou, Halkidis, & Stephanides, 2012) employed the adaptive LSB substitution based on edge regions of the cover image, where the edge regions can accommodate extra secret bits instead of smooth regions. Furthermore, the comprehensive differences analyses of these domains are shown in Table 2.1.

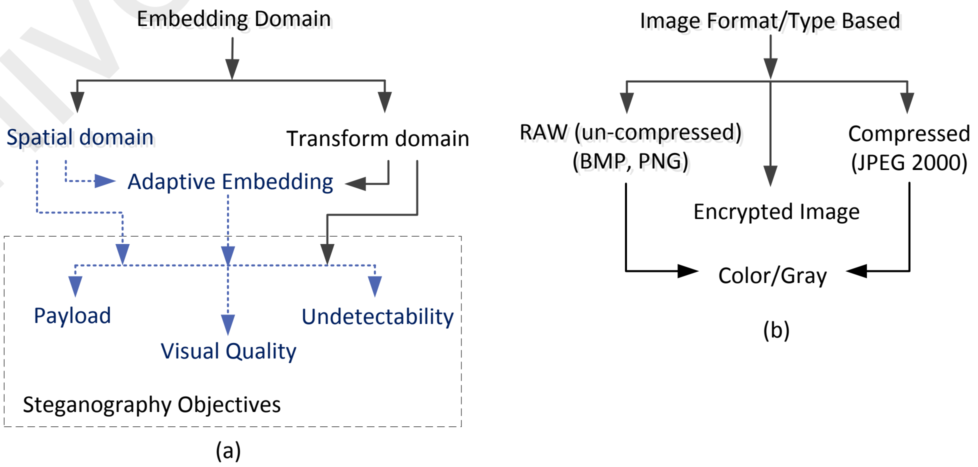


Figure 2.3: Classification of Steganography Techniques based on (a) Embedding Domains and (b) Image Format/Type

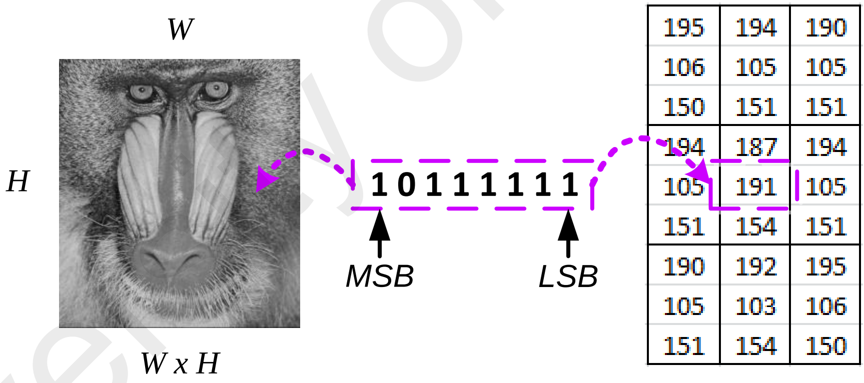
Furthermore, another classification can be based on distinctive steganography techniques that are specifically designed to target the image coded formats/types as shown in Figure 2.3 (b). For example, some steganography methods that only targets the uncompressed images, while some methods are designed for compressed and encrypted images. For further sub-classification, some methods can individually and specifically design for color and grayscale images as well. However, the focus of the thesis is only on grayscale spatial embedding domain based techniques.

Table 2.1: Comprehensive Comparison of Spatial and Transformed Domains with Adaptive Embedding

Characteristics	**Properties**	**Spatial Domain**	**Transform Domain**	**Adaptive Embedding**
System type	-	Simple	Complex	Depends on adaptive algorithm
Format dependency	-	Dependent	Independent	Independent
Pixel Manipulation	-	Direct	Indirect (e.g. in transformed coefficient)	Depends on inline technique
Computational complexity	-	Less computation time	High computational time	Algorithm-dependent
Embedding Capacity	Payload	High	Limited	Varied
Visual Quality	Imperceptibility	High	Less controllable	Highly controllable
Integrity of visual features	Sharpness, blurring, edges	Maintainable	Less maintainable	Maintainable
Robustness	Compression, Noise Cropping, Rotating etc.	Highly prone	Less prone	Depends on internal algorithm
Security	Geometric attacks	Vulnerable to geometric attacks	Resistant to geometric attacks	Hard to geometric attacks
Statistical detection attacks analysis	RS, Histogram	Easy to expose/detect	Hard to expose/ unsuccessful	Hard to expose/ unsuccessful
Non-Structural detection attacks analysis	Feature set, SPAM	Easily detectable	Easily detectable	Difficult/ Varied
Target	Capacity	High	Moderate	Moderate
	Visual quality	High	High	High
	Undetectability	Moderate	High	High

Generally, the structure of the grayscale image is as follows. The grayscale image f is modeled as a $W \times H$ matrix of integers known as pixels. Where each pixel being represented as an unsigned 8-bit byte. For any such image, one can identify 8 bit binary planes of each pixel with the i^{th} bit-plane of f as f_i of $W \times H$ binary image, which is defined for each pixel (x, y) in equation 2.1. For more clear representation of grayscale image with its characteristics are shown in Figure 2.4, where a pixel with the value of 191 is represented in $(1011111)_2$ binary form. Furthermore, the binary level of each pixel is classified as least significant bits (LSB) and most significant bits (MSB) model, where rightmost binary bits known as LSBs and leftmost bits considered as MSBs of an image pixel.

$$f_i(x, y) = i^{th}\ bit\ of\ f\ (x, y) \qquad (2.1)$$



195	194	190
106	105	105
150	151	151
194	187	194
105	191	105
151	154	151
190	192	195
105	103	106
151	154	150

Figure 2.4: Grayscale Image Pixels Representation

2.2.2.1 Spatial Domain

In spatial embedding domain, steganography techniques directly exploit the cover image pixels to conceal the secret information, where it modifies the pixel intensities with the secret bits. For example, a classical LSB embedding method that substitutes the secret data bits in the LSBs of each pixel because modification in LSBs of a pixel is visually less effective instead of MSBs modifications. Generally, the spatial domain embedding considered as favorite to applications that require high capacity, less computational complexity, and highly controllable imperceptibility as compared to transform embedding domain. The detailed characteristic of spatial domain embedding can be seen in Table 2.1. Furthermore, the various types of spatial domain embedding algorithms are discussed in section 2.3.

2.2.2.2 Transform Domain

The transform/frequency domain of an image usually refers to the representation of the image (or signal) in terms of waveforms, and a variety of such waveforms have been used to decompose/transform an image signal in terms of sub-bands of the frequencies of the waveforms that generate the given image. In 1822, Jean B. Fourier the French mathematician has shown that certain types of functions (i.e. image, audio data files) can be represented (i.e. decomposed/analyzed) by linear combination of the periodic trigonometric sinusoidal wave functions ($\mathrm{e.g.}\ \sin(x, y), \cos(x, y)$) of different frequencies (Gonzalez & Woods, 2007). The coefficients of the waveforms that a signal can be expressed in terms of their linear sum, is known as the frequency domain. Furthermore, the Fourier transform can be inverted without loss. In Figure 2.5 is an example of an image and its transformed domains using Discrete Fourier Transform (DFT), and Discrete Cosine Transform (DCT). In the case of DFT, the displayed image is the Fourier spectrum. Since the Fourier coefficients are complex numbers, and we cannot display the corresponding frequency domain. The DCT coefficients are real numbers and can be displayed.

Embedding in the frequency domain is performed on the coefficients of the transformed domain of the image. The three main types of transforms used for image-based steganography are Discrete Fourier Transform DFT (Bhattacharyya et al., 2009), Discrete Wavelet Transform DWT (P.-Y. Chen & Lin, 2006), and Discrete Cosine Transform DCT (Westfeld, 2001).

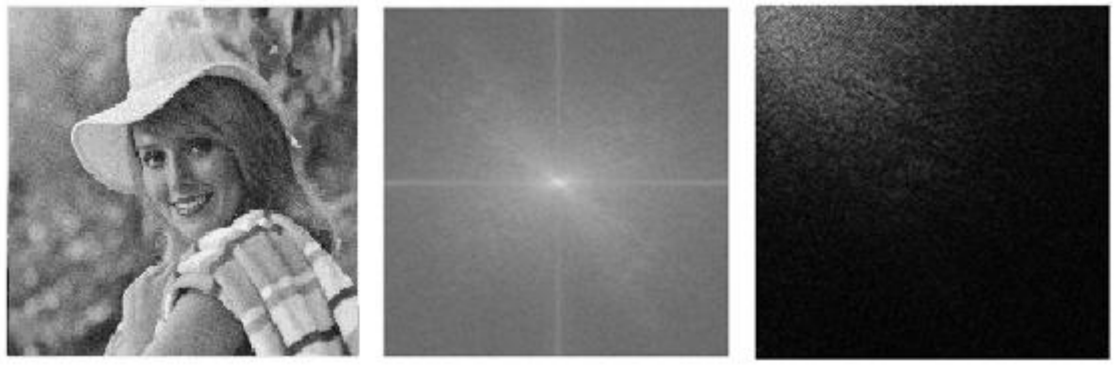


Figure 2.5: DFT and DCT Frequency Domain: (a) Original Image, (b) Spectrum of DFT and (c) a DCT Domain

Although, the focus of the thesis is to develop spatial domain based adaptive mannered steganography methods to achieve the optimal success of steganographic goals e.g. high embedding capacity with acceptable visual quality and security.

2.2.3 Image Steganography Objectives and Performance Evaluation Metrics

This section discusses the general image steganography objectives or performance evaluation criteria and furthermore exploits the most common respective measuring metrics or techniques. Currently, no standard test or measure is available in order to evaluate the effectiveness of steganography techniques. However, the most commonly used evaluation criteria for image steganography techniques are embedding capacity, visual quality, and security/undetectability of stego-image. As mentioned earlier, these performances evaluation criteria have trade-off especially in images based steganography techniques. For example, larger embedding capacity based stego-images are unable to maintain high visual quality, in contrast, high visual quality based stego-images suffers from low embedding rate. Therefore, to achieve the optimal ratio in above criteria may consider the ideal steganography methods. Furthermore, we present and discuss what are the most commonly used evaluation metrics in image-based steganography literature? How these employed for evaluation aspect in any steganography methods?

2.2.3.1 Embedding Capacity/Payload of Stego-Image

This defines the maximum length of secret binary string that can be embedded in the cover image. In the case of spatial domain image based steganography, the embedding capacity/payload may be stated in units of measurements such as the data embedding rate in terms bits per pixel (bpp), or the ratio of the secret message to number of cover pixels. For example, bpp = 1.0, this indicates that the number of embedded secret bits is equal to the number of cover pixels. In this thesis, the capacity is measured by using embedding ratio, i.e. if a cover image C is of size $W \times H$ width and height in pixels, and the length of the embedded secret is L bits, then the embedding capacity EC ratio is given by equation 2.2.

$$\text{EC (bpp)} = \frac{\text{L}}{W \times H} \tag{2.2}$$

Generally, the question arises that how much the embedding capacity is required to prove the ideal steganography technique? As discussed before, there is a trade-off between the embedding capacity and imperceptibility. Nevertheless, steganography techniques that embed messages for which L > $(W \times H)$ and introduce distortions to stego-images are considered as worthless systems. Conversely, if increasing the embedding capacity while maintaining the quality is considered a positive contribution in steganography systems. Additionally, improving the stego-image quality while maintaining the steganography capacity L > $(W \times H)$ is also considered a significant contribution (N.-I. Wu & Hwang, 2007).

2.2.3.2 Visual Quality of Stego-Image

In this section, another performance evaluation measuring parameter known as visual quality of stego-image is presented. The visual quality directly reflects the significance of an embedding algorithm because in embedding process it alters/modifies the original pixel intensities. The maximum differences between cover and stego-image pixels assumed the low visual quality and can be analyzed by steganalysis technique.

Table 2.2: Most Common Visual Quality Analysis Matrices

Metric	**Formulas**
Mean Square Error (MSE)	$\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{H} \times \mathbf{W}} \sum_{\mathbf{i=1}}^{\mathbf{H \times W}} (\mathbf{C_i} - \mathbf{S_i})^{\mathbf{2}}$ $\mathbf{C_i}$ = cover pixel value; $\mathbf{S_i}$ = stego-pixel value; **H** × **W**: represent the height and width of cover the image. **Lowest values considered as good.**
Root Mean Square Error (RMSE)	$\mathbf{RMSE} = \sqrt{\mathbf{MSE}}$ **Lowest values considered as good.**
Peak Signal to Noise Ratio (PSNR)	$\mathbf{PSNR} = \mathbf{10} \times \mathbf{log_{10}} \left(\frac{\mathbf{Max^2}}{\mathbf{MSE}} \right)$ **Max** = maximum pixel intensity value that is 255. **Highest values considered as good.**
Image Quality Index (Q Index) **(Z. Wang & Bovik, 2002)**	$\mathbf{Q} = \frac{\mathbf{4} \times (\acute{O}_{\mathbf{YZ}}) \times \mathbf{Y}^{''} \times \mathbf{Z}^{''}}{((\acute{O}_{\mathbf{Y}})^{\mathbf{2}} + (\acute{O}_{\mathbf{Z}})^{\mathbf{2}}) [(\mathbf{Y}^{''})^{\mathbf{2}} + (\mathbf{Z}^{''})^{\mathbf{2}}]}$ $\mathbf{Y}^{''} = \frac{\mathbf{1}}{\mathbf{N}} \sum_{\mathbf{j=1}}^{\mathbf{N}} \mathbf{Y_j}, \ \mathbf{Z}^{''} = \frac{\mathbf{1}}{\mathbf{N}} \sum_{\mathbf{j=1}}^{\mathbf{N}} \mathbf{Z_j}$ $(\acute{O}_{\mathbf{Y}})^{\mathbf{2}} = \frac{\mathbf{1}}{\mathbf{N-1}} \sum_{\mathbf{j=1}}^{\mathbf{N}} (\mathbf{Y_j} - \mathbf{Y}^{''})^{\mathbf{2}}, (\acute{O}_{\mathbf{Z}})^{\mathbf{2}} = \frac{\mathbf{1}}{\mathbf{N-1}} \sum_{\mathbf{j=1}}^{\mathbf{N}} (\mathbf{Z_j} - \mathbf{Z}^{''})^{\mathbf{2}}$ $\acute{O}_{\mathbf{YZ}} = \frac{\mathbf{1}}{\mathbf{N-1}} \sum_{\mathbf{j=1}}^{\mathbf{N}} (\mathbf{Y_j} - \mathbf{Y}^{''}) \times (\mathbf{Z_j} - \mathbf{Z}^{''})$ **Closest to 1 considered as good.**

Generally, the visual quality of a stego-images is measured in two ways: subjective and objective (Stoica, Vertan, & Fernandez-Maloigne, 2003). The human visual system is required to evaluate the subjective visual quality of stego-image, while the objective visual quality measures require some statistical or quantitative techniques. Practically, the subjective visual quality measuring is inefficient, because it consumes the maximum time in manual observation. However, in literature, the most common and widely used objective visual quality matrices are peak signal-to-noise ratio (PSNR), mean square error (MSE), root mean square error (RMSE) and universal quality index (Q). All these can quantitatively measure the differences in visual quality ratio between cover and stego-images. In addition, these measuring techniques may estimate or judge the visual modification levels, which are needed to decide whether the stego-image of respective steganography method is perceptually transparent or not. In Table 2.2, the aforementioned visual quality measures are briefly explained with respective formulas.

2.2.3.3 Security of Stego-Image

In this section, a performance evaluation criterion of stego-image security/ undetectability is addressed. We will present, what are the most commonly used steganalysis detection attacks from literature that are employed to expose the steganography techniques or secret data in stego-images?

Steganalysis is the counterpart of steganography, which aims to identify the presence of secret data in communication. That is why the security/undetectability of a stego-image plays a vital role in evaluation criteria of steganography, because if a stego-image is exposed by any steganalysis technique then the purpose of steganography becomes worthless. Generally, there are two types of attacks in information hiding, i.e. active and passive attacks. The active attacks destroy the secret data while the passive attacks determine the presence of secret data even can identify the size of secret data. Mostly, active attacks are performed in watermarking and authentication methods to evaluate the strength or security. Meanwhile, there are number of active attacks, e.g. blurring, sharpening, median filtering, rotation, noise adding or geometric variation on stego-images (Jiri Fridrich, 1999).

On the other side, the passive attacks aim to identify the suspected secret communication. Generally, cover images have neighboring correlation to pixels before employing the embedding process. As a result, stego-images are unable to maintain this neighboring correlation of pixels. Therefore, mostly steganalysis technique exploits these types of statistical or structural characteristics to identify the presence of secret data in stego-images. For example, in 1-bit LSB embedding process, the bit planes are switched to (0↔1, 244 ↔245 or 254↔255) therefore, regular and singular steganalysis by (Jessica Fridrich et al., 2001) exploit these characteristics to differentiate differences between cover and stego-images. There are three main categories of steganalysis that are defined and widely employed in literature.

(a) ***Structural Steganalysis***

This structural steganalysis detects the specific behavior of modification difference between cover and stego-images. While these type of steganalysis are efficient and rely on empirical pixel correlation model instead of global statistical method (Cogranne et al., 2014). The well-known regular and singular (RS) (Jessica Fridrich et al., 2001) technique is considered as a structural steganalysis tool for substitution based embedding.

In RS steganalysis, n adjacent pixels $(p_1, p_2, \dots, p_n)$ are selected as pixels group, where the discrimination function (DF) is presented as $DF = (p_1, p_2, \dots, p_n) = \sum_{i=0}^{n} |p_{i+1} - p_i|$. This DF computes the regularity of each pixels group as regular, singular and unusable groups with flipping masks i.e. $M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $-\mathrm{M} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$. The proportion or the percentage of the block against regular and singular groups are represented as $\mathrm{R_M}$, $\mathrm{S_M}$, $\mathrm{R_{-M}}$, and $\mathrm{S_{-M}}$. If these groups satisfies $\mathrm{R_M} \approx \mathrm{R_{-M}} > \mathrm{S_M} \approx \mathrm{S_{-M}}$, it indicates that there is no hidden data in respective image. Conversely, when an image has hidden data, the percentages of $\mathrm{R_{-M}}$ and $\mathrm{S_M}$ increases, and $\mathrm{R_M}$ and

S_{-M} percentages are decreases and considered as the respective image is detected by RS analysis. Figure 2.6 represents the basic RS analysis of 1-bit LSB based stego-image. This depicts as the embedding capacity is increased the Rm, R-m and similarly, Sm, S-m pixels group differences are increased. This stated that RS successfully detected the stego-image.

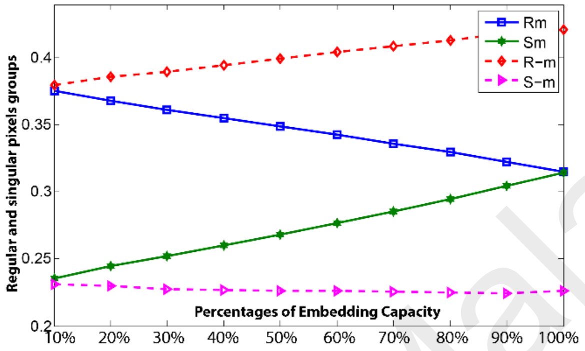


Figure 2.6: Basic RS analysis detection graph

Similarly, another powerful method is bit-plane analysis, which can detect the artifacts of stego-image directly. In visual attack (Westfeld & Pfitzmann, 1999), the corresponding bits in each pixel of cover and stego images is analyzed. In result, it construct a plane image by bit placement of cover and stego image in each pixel. Once the cover and stego-image bit-planes are drifted in term of visual differences, it indicates that the stego-image is unable to resist the bit-planes steganalysis. The visual bit-plane analysis of different methods are discussed in detail (section 4.1.3.3).

(b) ***Statistical Steganalysis***

This steganalysis process detects the statistical characteristics differences between cover and stego-images due to modification of statistical properties in stego-images. In literature, the most common statistical steganalysis are pixel difference histograms (T. Zhang & Ping, 2003) and histogram analysis (Choudhury, Das, & Baruah, 2015). This pixel difference histogram computes the number of occurrences between pixel pair with respect to particular difference value. In other words, the pixel difference histogram is computed by taking the differences of neighboring pixels with fall-off ranges between cover and stego-image. While the histogram that measures the number of occurrences/frequency of pixels with respect to particular pixel value. Generally, during the embedding process pixel values are changed, therefore the number of occurrences/frequency of a particular pixel value that becomes changed. This change can be used to detect the stego-image. Therefore, lesser the difference of histograms between cover and stego-image indicates the more resistance against stego-image detection.

(c) ***Universal Machine Learning based Steganalysis***

In literature, recently the interest of steganalysis is switched from specific steganalysis to universal machine learning based steganalysis. Where there is no need of prior knowledge of embedding algorithm for these types of steganalysis. These kinds of steganalysis can detect various types of embedding algorithms. For example, a modern steganalysis, known as Subtractive Pixel Adjacency Matrix (SPAM) detector proposed by (Pevny et al., 2010) is designed to break various steganography methods. This type of steganalysis model consists of two parts, first the feature extraction and pattern classification. Where the SPAM detector is employed to extract the features and for classification i.e. Support Vector Machine (SVM) or ensemble classifier by (Kodovsky, Fridrich, & Holub, 2012) used to classify the cover and stego-images. Generally, these machine learning based universal steganalysis techniques are computationally expensive and not suitable for real time steganalysis application, because this requires huge dataset of training and testing (Holub, Fridrich, & Denemark, 2014; Ker et al., 2013) process. However, these methods are more accurate to identify the stego-images.

2.3 Spatial Domain Image Steganography Techniques

In this section, we present and review the existing spatial domain image-based steganography techniques. There are number of spatial domain image steganography techniques that have been proposed even with their different variations based on embedding approaches/mechanisms. Therefore, it is evident that spatial domain based steganography is probably the most dominant domain in the literature. Majority of the existing steganography techniques are based on substitution and pixel differencing mechanisms, to some extent that are able to achieve the steganography objectives. However, there are some aspects that need to review to achieve the optimal steganography objectives. In the next paragraphs, we briefly highlight those aspects that influenced us to conduct this research.

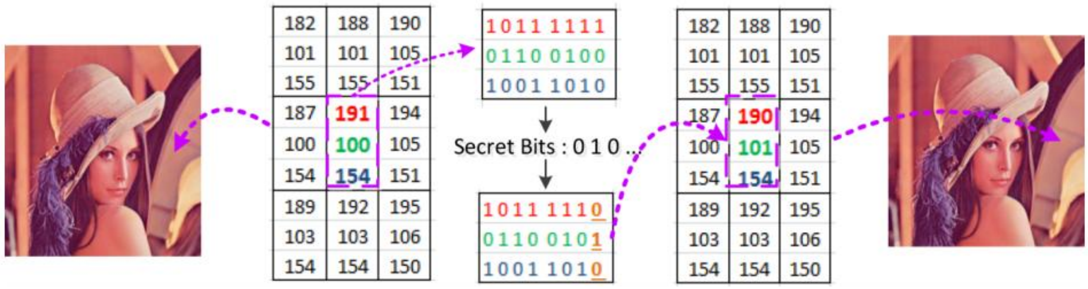
When the motive is to achieve a high visual quality in stego-images, mostly spatial domain steganography techniques are designed to embed the secret data in those places, where the distortion impact would be least on the stego-images. Therefore, lower bit planes as LSBs of a pixel are more suitable for embedding that generate the less distorted impact on stego-images. Various types of steganography techniques exists, which directly/indirectly substitute/modify the limited LSBs of pixels to achieve high visual quality of stego-images. However, the employing of limited LSBs means the lesser secret bits or limited embedding capacity can be achieved. Therefore, how can we (directly/indirectly) employ maximum LSBs while retaining the less distortion (as high visual quality) in stego-images to achieve high embedding capacity?

For security/undetectability aspect, it is indirectly interlinked to the visual quality of a stego-image. Generally, the efficient spatial domain image steganography methods are designed to embed the secret data in inconspicuous areas of stego-image or reduce the embedding distortion by lowering embedding capacity rate in stego-images, which indirectly resist the steganalysis detection attacks. How can we improve the embedding capacity rate without degrading the visual quality and the security/undetectability in a steganography technique?

In this section, we contemplate the well-known embedding techniques with its adaptive and hybrid steganographic mechanism that evolve in recent years to improve its payload, quality and security aspects. In Section 2.2.1 and 2.2.2, we will extensively review the various existing types of substitutions and pixel value differencing based methods. Meanwhile, in Section 2.2.3, we will also consider the other existing distinct embedding approaches that employed the substitution and pixel value differencing strategies in its embedding process. Furthermore, a comprehensive analysis highlights the merits and challenges of above approaches with quantitative manners presented in the tabular form in Table 2.3. We will also illustrate the chronological orders of existing techniques with their efficiencies in recent years (Figure 2.11).

2.3.1 Substitution-based Steganography Methods

Substitution-based steganography methods replace the redundant data of the cover image with the required secret data. The strengths of these methods are the simplicity of implementation and the high embedding capacity relative to other types of embedding techniques. In the literature, most of the existing substitution-based steganography are actually inspired by the least significant bit (LSB) (Chan & Cheng, 2004) method, that employ the different variations of LSB's or bit-planes of pixels for concealing the secret data. LSB technique is one of the fundamental and conventional method that is capable of hiding larger secret data in a cover image without noticeable visual distortions (B. Li, He, Huang, & Shi, 2011). Generally, LSB-based substitution works by replacing the LSBs of (randomly) selected pixels in the cover image with secret data bits. The selection of pixels or the order of embedding may be determined by a stego-key (pre-defined protocol) between sender and receiver. The practical implementation of LSB substitution mechanism is shown in Figure 2.7.



182	188	190
101	101	105
155	155	151
187	191	194
100	100	105
154	154	151
189	192	195
103	103	106
154	154	150

1011 1111
0110 0100
1001 1010

Secret Bits : 0 1 0 ..

1011 1110
0110 0101
1001 1010

182	188	190
101	101	105
155	155	151
187	190	194
100	101	105
154	154	151
189	192	195
103	103	106
154	154	150

Figure 2.7: Basic LSB Embedding Process

Generally, steganography methods are designed based on some motives/strategies i.e. optimization of secret data size, exploiting the noisy area of cover image for embedding, reduce the number of modified bit-plane, etc. However, all the motives/strategies are indirectly targeting the improvement in steganography objectives such as embedding capacity, quality and security. In next few paragraphs, we review the recent LSB-based techniques based on different motives/strategies to achieve the above steganography goals.

Many attempts have been done for increasing the visual quality, indirectly enhances the security of LSB-based methods. Recently, to improve the visual quality and security against histogram attacks, (Sarreshtedari & Akhaee, 2014) proposed a ±1 based approach with the 1 bpp embedding capacity. It reduces the probability of change per pixels as 1/3 pixel modification. Due to less modification of stego-pixels, it enhances the imperceptibility and also provides the resistance against (Ker, 2005) steganalysis detection attacks. However, the embedding rate of 1 bpp is not suitable for larger embedding payload demanding applications. Another well-known approach LSB+ to enhanced the visual quality and security of stego-image, this intentionally embeds some extra bits to avoid the histogram steganalysis attack, but these extra bits embedding is traced by second order statistics (co-occurrence matrices) analysis. In (Qazanfari & Safabakhsh, 2014), authors improved the existing LSB+ method by introducing to identify the sensitive pixels and avoid them from extra bit embedding using key lock method. This LSB++ method decreases the amount of changes made to the perceptual and statistical attributes of the cover image. It retains the avoidance of statistical attacks while preserving the histogram and co-occurrence metrics. This technique also enhances the visual quality measured by peak signal to noise ratio (PSNR) while embedding capacity is still limited to 1 bpp. Similarly, (Tavares & Junior, 2016) introduced the LSB Word-Hunt (LSB WH) method, which is inspired from the world-hunt puzzle game. The motivation of the approach is also to reduce the modification per pixel value which indirectly increases the visual quality of stego-image. The LSB WH approach only resists the statistical chi-square detection attacks while this method is only suitable for low embedding capacity based applications.

To achieve the larger embedding payload in LSB-based steganography methods, generally these methods exploit more than 1 bits-planes of pixel or utilize multiple LSBs for embedding process based on some strategy, i.e. image edges, textures, or the brightness can be used to estimate the number of LSBs for embedding process like (H. Yang et al., 2009). Similarly, in (H.-W. Tseng & Leng, 2014) approach it employs the edge characteristics of the cover image, which further incorporates to decide the number of LSB's used for embedding. Another texture region based adaptive LSB method is introduced by (Nguyen, Arch-int, & Arch-int, 2015) known as multiple block data-hiding (MPBDH). This exploits more than one-bit planes with adaptive complexity threshold to select the complex regions of a cover image for embedding purpose. The embedding capacity rate is 1.6 bpp and security performance is improved with respect to existing pixel/block-based adaptive LSB methods. Meanwhile, some methods employ the other strategies i.e. optimized LSB substitution using cat swarm strategy (Z.-H. Wang, Chang, & Li, 2012), LSB substitution with interpolation image (Jung & Yoo, 2015b), however these methods are unable to maintain the acceptable visual quality. Recently, a novel LSB-based scheme introduced using modulo three strategy in (Xu et al., 2016). The two ternary numbers in each pixel can be embedded, which generally modify the two LSBs of a pixel that can cause the overflow/underflow problems. Therefore, a pre-processing of ±1 is applied on pixels before embedding process. This method proves the larger embedding capacity +3 bpp while retaining the acceptable visual quality (+37 dB PSNR value). However, this technique is unable to resists the modern steganalysis detection attacks even at 0.25 bpp of embedding rate.

With respect to security or undetectability against modern steganalysis in LSB-based method, a highly undetectable stego (HUGO) embedding method (Pevný, Filler, & Bas, 2010) was proposed based on LSB matching technique. It consists of a high dimensional image model to calculate the distortion corresponding to a modification of each pixel by ±1. The payload is limited to 1 bpp, but can resist the modern steganalysis detection attacks (Pevny et al., 2010). Another method is proposed by (Yuan, 2014) that is based on multi-cover adaptive steganography. The secret data embedding is done into LSBs of pixels. Furthermore, this can resist the modern steganalysis detection attacks such as SPAM features based steganalysis (Pevny et al., 2010; H. Zhang, Ping, Xu, & Wang, 2014). The aforementioned methods retain the maximum ≈ 1 bpp embedding capacity, while require the high computation for embedding process. However, these techniques are not suitable to the high capacity based application, and even not ideal for real-time application. In the next section, pixel value differencing strategies that concern to enhance the visual quality while retaining the larger embedding capacity are reviewed.

2.3.2 Pixels Value Differencing based Steganography Methods

In this sub-section, we will review the recent pixel value differencing based steganography techniques with respect to embedding capacity, visual quality and security. Pixel value difference (PVD) technique is proposed by (D.-C. Wu & Tsai,

2003) and considered as another well-known and majorly employed technique in spatial domain image steganography system. The basic PVD embedding process is illustrated in Figure 2.8.

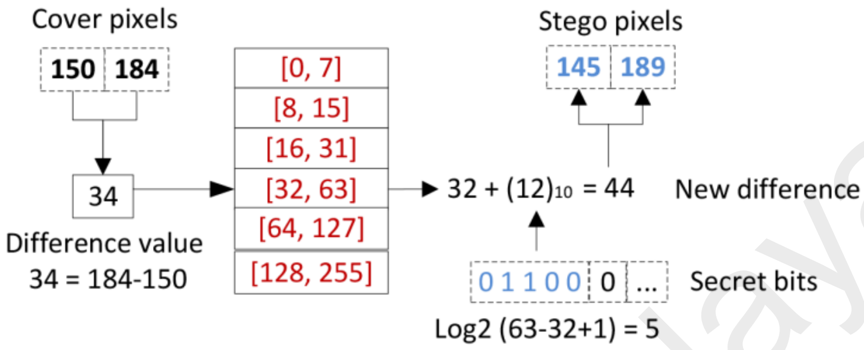


Figure 2.8: General Pixel Value Difference Embedding Technique

The notion of PVD is to readjust the differences between cover pixels to accommodate the secret data. The difference value between two neighboring pixels is used to decide how many secret bits should be embedded? First, a cover image is partitioned into two non-overlapped consecutive pixels block in a zig-zag direction. The difference value between two pixels is calculated to decide the secret embedding bits, where difference values are grouped into a number of ranges. Finally, the difference is modified with the new difference value along the secret data. The number of embedding secret data depends on the texture area of an image that actually controlled by range levels of the table. The larger the difference (higher the texture), the more secret bits can be embedded into pixel pair. Generally, PVD method provides the reasonable embedding capacity while achieves the higher visual imperceptibility (PSNR +40 dB) as compared to LSB-based substitution method. However, the major issues regarding PVD method are the lower embedding capacity and security. Generally, image contains more smooth area instead of high texture area, so limited secret data bits are embedded in the small value ranges, indirectly inefficient/lower embedding capacity gained. Similarly, the PVD-based stego-image histogram generates the remarkable steps that are able to reveal the existence of a secret message. In addition, the falling-off-boundary procedure is also one of the significant problems as well.

In literature, various PVD-based techniques are presented to resolve the PVD limitations and enhancing the general steganographic objectives. The most common approaches are Tri-way PVD (Chang, Chang, Huang, & Tu, 2008), Multi-Pixel Differencing (C.-H. Yang, Wang, et al., 2010), Modulus Function (MF) (F. Pan et al., 2011) and block based PVD (C.-H. Yang, Weng, Tso, & Wang, 2011) that tried to tackle the above issues as well enhancing the embedding capacity but still found the tradeoff in steganography objectives.

To improve the embedding capacity in PVD-based methods, Tri-way PVD (Chang et al., 2008) technique employ the 2x2 pixel block in three pairs of pixels to embed the secret data, where it improves the embedding capacity while reduces the visual quality of stego-image (-4 dB PNSR). However, the improvement of embedding capacity enables the Tri-way PVD method to employ in different practical embedding approaches. For example, (Lee et al., 2012) presents the secret image communication steganography approach with the combination of compression and Tri-way PVD embedding technique. First secret image (data) is compressed by JPEG2000 at high compression ratio and further Tri-way PVD is employed for actual embedding process. The visual quality of secret image degraded due to highly compressed ratio, where a residual value coding is proposed to reduce the visual distortion in the recovered secret image. The proposed method provides the high secrecy while avoiding the dual statistical detection attacks. Similarly, another usage of Tri-way PVD, in (Hernández-Servin, Marcial-Romero, Jiménez, & Montes-Venegas, 2015) presents a modified version of Tri-way PVD embedding to resolve the extra need of location map for overflow/underflow PVD problem. This approach employs the two sub-embedding techniques, Tri-way PVD and reversible steganography technique. The regular secret data embedding are embedded by Tri-way PVD, while reversible embedding technique is used for location map insertion. Recently (Grajeda-Marín, Montes-Venegas, Marcial-Romero, Hernández-Servín, & De Ita, 2016) presents a Tri-way PVD-based approach, to resolve the overflow and underflow problem of PVD while improving the capacity as well. It computes the optimal pixel values for each embedding block. In results, it resolves the above issues and improves the embedding payload, but the visual quality becomes degraded (-2 dB PSNR) even against the conventional PVD method.

In literature, there is another strategy to enhance the embedding payload of pixel differencing methods known as hybrid PVD, where the researchers combines the PVD approach directly or indirectly with other existing steganography methods. For example, Jung et al. and Wu et al. proposed PVD+LSB hybrid steganography techniques (Jung, 2010; H-C Wu et al., 2005). In result, these methods improve the embedding capacity while retaining acceptable visual quality of stego-images. Similarly, another hybrid technique, where an adaptive PVD method is introduced with modulus function to resolve the fall-off-boundary conditions (Mandal & Das, 2012). However, it is unable to improve the embedding capacity while retains the imperceptibility as compared to original PVD approach. In (M Khodaei & Faez, 2012) approach, this utilizes the PVD with adaptive LSB substitution and optimal pixel adjustment process. As a result, this method achieves the larger embedding payload while maintaining the acceptable PSNR. However, it is unable to maintain the histogram and modern steganalysis detection attacks. Another hybrid PVD with exploiting modification directions (EMD) steganographic method is proposed to improve payload and imperceptibility by (S.-Y. Shen & Huang, 2015). First, a cover image is mapped into a 1D pixels array by Hilbert filling curve instead of conventional zig-zag ordering. Hilbert filling order shows more locality preserving property against raster scan or zig-zag scan orders. It could resolve the overflow/underflow issues and minimize the embedding distortion. However, the embedding payload is still considered as limited. Similarly, (S. Shen, Huang, & Tian, 2015) presents another PVD hybrid scheme with the combination of PVD and modulus function to improve hidden capacity. Meanwhile, it exploits the correlation of the R, G and B planes of the color image. The number of secret bits is determined by the difference of corresponding G planes pixels. Furthermore, various adjustment processes are applied to overcome the overflow and underflow problems. The proposed method is secured against RS diagram and histogram analysis while provides an acceptable visual quality. However, the improvement of embedding capacity is not sufficient for larger capacity demanding steganography applications. Another combination of PVD with LSB is presented in (Swain, 2016) to improve the embedding capacity. First, it inserted the k-bits secret data in upper-left pixel from 2x2 pixels block. Next, the PVD embedding process is applied to the upper-left based pixel and other remaining pixels in horizontal and vertical edge directions. Recently, to obtain the larger embedding payload, (Masoumeh Khodaei, Sadeghi Bigham, & Faez, 2016) introduce another PVD with LSB approach. It divides the cover image into two pixels blocks and estimates the difference between these two pixels. The numbers of secret bits are estimated based on difference value and the embedding process done by adaptive LSB scheme. However, this method is capable to maintain the highest ratio in capacity and visual quality, but the core embedding process depends on adaptive LSB substitution. Furthermore, this method did not reported any resistant against steganalysis detection attacks.

To enhance the visual quality, a multi-way PVD with the combination of Tri-way PVD using mode selection process is presented in (Huang, 2015), while this combination improves the visual quality with limited embedding capacity. Furthermore, two adaptive PVD-based steganographic solutions are proposed by (Swain, 2015) that utilizes the vertical and horizontal edges for secret data embedding. The first approach used the 2x2 pixels blocks and the second one is applied on 3x3 pixels blocks. Both methods are targeted for larger capacity and better visual quality of stego-images. Similarly, in (Balasubramanian et al., 2014), an octonary pixel pairing scheme proposed to handle the visual distortion and low payload. This method is based on the principle that edge areas are more tolerable for larger modification than smooth areas, and hence can hold more secret data. So the edge areas are identified first in the region selection phase. Subsequently, the number of bits that can be embedded inside each pixel pair is determined by referring the range table. If the regions are sufficiently large for hiding the given secret message, then secret data is embedded into the selected regions. Otherwise, the smooth regions are utilized for embedding after using all the edge regions. The data hiding is performed as per the octonary PVD scheme. Finally, pixel readjustment is applied to improve the perceptual quality and the statistical undetectability. The next section discusses the other distinctive embedding strategies/techniques found in literature to achieve the general steganography goals.

2.3.3 Other Approaches of Spatial Domain Steganography

This section exploits the other existing distinctive spatial domain image steganography techniques that are directly or indirectly employ substitution and pixel value differencing methods. As mentioned earlier, it is impossible to incorporate and discuss all existing image based steganography techniques due to the scope of thesis. We will cover the most commonly employed steganography approaches that are based on some strategies and specific to algorithm/implementation. However, the motive is to review the other existing approaches that are evolved to improve the embedding capacity, visual quality and maintain the resistance against steganalysis detection attacks.

(a) *Edge Adaptive Methods*

One of the prominent embedding strategies in the spatial domain steganography is an edge adaptive embedding. Generally, the edge based embedding techniques are inspired from Human Vision System (HVS) principle, where the change in the smooth regions becomes more prominent than noisy regions. Similarly, an image is based on different textures or regions i.e. smooth regions, edgy or noisy regions. Therefore, direct/constant modifications in all regions of an image yield a visual distortion in smooth region as compared to edge regions. Thus, edge adaptive embedding schemes are evolved to maintain the minimum visual distortion. Similarly, these embedding methods are more popular for providing high imperceptibility. To identify the edge regions of an image, Figure 2.9 shows the Lena image with respective canny edge detector based image, where the white lines indicate the most prominent edge regions of the Lena image.

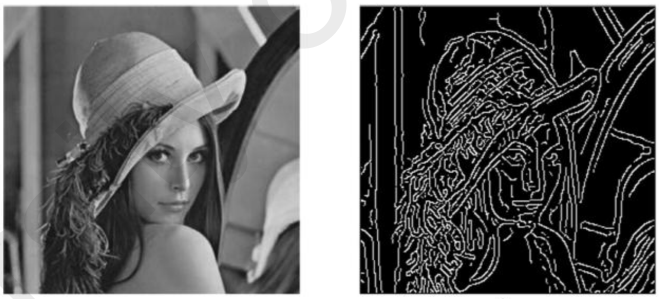


Figure 2.9: Lena Image and Lena’s Canny Edge based Image (Al-Dmour & Al-Ani, 2016)

In (Luo, Huang, & Huang, 2010) proposes an edge adaptive steganography by employing the LSB-MR technique for secret data embedding. In this method, complex texture areas are used for larger payload, while the smooth/light edge textures regions are employed for limited embedding payload. It maintains the high imperceptibility and security of stego-images, however, suffer from limited payload. Similarly, a simple and effective embedding technique based on hybrid edge detection (fuzzy edge and canny edge detectors) is proposed in (W.-J. Chen, Chang, & Le, 2010). However, the underline embedding is employed by LSB substitution. In result, it increases the visual quality (PSNR) and security against statistical steganalysis detection attacks. However, there is an overhead of unwanted (n−1) bits of modifications in each block to maintain the secret data consistency. Furthermore, another hybrid (fuzzy and sobel) edge detector based adaptive LSB embedding technique for color images is presented in (Ioannidou et al., 2012). The sharp regions of an image are employed by multiple LSBs based substitution embedding technique. In result, it increases the embedding capacity, however, having overhead of extra information logging. This extra logging is required to recover the secret data at decoding phase. Unlike (W.-J. Chen et al., 2010), this method uses the sobel edge detector instead of canny edge detector to increase the visual quality as PSNR. The scheme also suffers from maintaining of two separate additional files, i.e. height, width, and channel modified bits. Meanwhile, this scheme is not evaluated by any steganalysis technique to verify its security level. Another edge based adaptive steganography technique for color images is presented by (Grover & Mohapatra, 2013). Where it resolves the issues of (Ioannidou et al., 2012) technique, and enhances the embedding capacity rate. In this scheme, for efficient embedding purpose, secret data is divided into two different blocks, i.e. edge based and non-edge based blocks, meanwhile, this scheme also enhances the security of stego-images as well.

Similarly, another edge adaptive technique is presented by (Roy, Sarkar, & Changder, 2013) that combines the matrix encoding with LSBM embedding method. Furthermore, a cat chaotic mapping is employed to distort the secret data for improving secrecy, where the secret data is restorable only by supplying the correct key. This cat chaotic mapping provides the high fidelity and imperceptibility, even performs better than LSB + PVD-based techniques. However, the embedding capacity rate is still low.

Furthermore, another edge based embedding technique for color images is proposed in (Modi, Islam, & Gupta, 2013), where it utilizes the 2-bit LSBM for embedding process. The canny edge detection is applied in one of the selected R, G, or B channel. Meanwhile, the rest of two channels corresponding to the edge pixels are used for actual secret data embedding process. Embedding payload size is roughly 0.083 bpp (limited) for color edge pixels, while maintains the high visual quality of stego-images. A semi-reversible edge based embedding technique is proposed by (Jung & Yoo, 2014a), where the image is interpolated and divided into two regions i.e. edge and non-edge. In this scheme, a threshold value determines the number of secret bits for edge pixels of an image. In contrast, for non-edge based pixels, the difference between two non-overlapped consecutive pixels is utilized to estimate the number of secret bits for the embedding process. Similarly, another type of edge based secret image embedding technique is proposed by (S. Sun, 2016), where it employs the canny edge detector and Huffman encoding process to improve the secrecy and visual quality of the proposed scheme. In this method, the edge pixels are determined by the canny edge detector, where the only identified edge pixels are employed for embedding process. This scheme requires an extensive computation due to encoding phase with respect to other existing spatial domain methods. Recently, another technique is proposed to improve the visual quality and security by integrating the edge detection and XOR/LSB coding method (Al-Dmour & Al-Ani, 2016). This scheme first employs the sharpest regions for embedding process, next it gradually moves to the less sharp regions. It maintains the edge consistency in both cover and stego-images even before and after embedding process. Thus, this edge consistency resists the various textural feature based steganalysis detection attacks.

(b) ***Exploiting Modification Direction (EMD) Methods***

In this sub-section, we discuss the EMD scheme and its recent improvements with respect to singular and hybrid steganography approach. Exploiting modification direction (EMD) is a well-known embedding technique that maintains the high fidelity of stego-images (X. Zhang & Wang, 2006). Generally, in EMD embedding process, the secret digit is transformed by (*2n + 1*)-ary system, where *n* are the number of cover pixels. In other words, the EMD utilizes the specific based to determine the local variation of pixel intensity in the image. Therefore, pixels in high texture areas are able to embed more secret data. As a result, the EMD can achieve good visual quality as compared to LSB and PVD-based methods. Conversely, maximum embedding capacity of EMD method is up to 1.16 bpp for number of (n = 2) two pixels. However, its embedding capacity rate drastically decreases when the numbers of selected pixels are increases. In literature, various EMD based methods are proposed to improve the embedding capacity, i.e. (Kieu & Chang, 2011; Kuo, Kuo, & Huang, 2013; Wen-Chung & Ming-Chih, 2013), and can also achieve the general steganography objectives.

To improve the embedding capacity and imperceptibility of the EMD method, (H.-M. Sun, Weng, Lee, & Yang, 2011) come up with the proposing of two EMD based embedding techniques called HoEMD and AdEMD. Where, in the HoEMD approach, the concept is to exploit the pixels direction, where the pixels with larger variations have larger directions and may have larger embedding payload. In the other proposed AdEMD scheme, the concept is based on if the pixels belong to edge regions may compensate more secret data. In result, proposed methods achieve the high embedding capacity rate, while faces some overflow problems. A fully exploiting modification direction (FEMD) technique is presented by (Kieu & Chang, 2011). The FEMD technique improves the embedding capacity from 1 bpp to 4.5 bpp, together with acceptable visual quality against (X. Zhang & Wang, 2006) technique. During embedding process, it requires an extra search matrix, which is an overhead of this method. In addition, overflow problems of EMD technique are also inherited in proposed FEMD method. However, in (Wen-Chung & Ming-Chih, 2013) technique, it resolves the above overflow problems and while maintaining the similar embedding capacity. The secret data are embedded directly by formula operations (or without using a lookup matrix) known as formula fully exploiting modification directions (FFEMD) steganography. Similarly, in another EMD based technique, a generalized exploiting modification direction (GEMD) is presented in (Kuo et al., 2013). The main contribution as the (*n+1*)-ary binary bits can be embedded into *n* adjacent pixels directly. From experimental results, this scheme is able to maintain the embedding payload at (*1+1/n*) with adjustable pixels group. In simple words, the GEMD technique is not able to hide more than two secret bits in each pixel. However, it suffers from excessive pixel modification issue, because all pixels of the group are modified during GEMD embedding process. To tackle the above number of pixels modification problem, a Modified Signed-Digit (MSD) technique is proposed by (Kuo, Wang, & Hou, 2016). Where, it only modifies the *n/2* number of pixels in a group with the maximum value range of ±*1*. This scheme maintains the embedding rate as 1 bpp, which is independent of increasing the *n* pixels in a group. The MSD scheme is able to resists the RS steganalysis (Jessica Fridrich et al., 2001) and retains acceptable visual quality of stego-images.

Recently, another method is proposed to improve the embedding capacity in (Kuo, Kuo, Wang, & Wuu, 2016) technique. This scheme employs a multi-bit encoding function, which can embed up to (*k+1/n*) on average of each pixel, where *k* is determined by the number of embedded bits per pixel. It reduces the overhead of secret data conversion and also provides the flexibility of adjacent pixels relation. Furthermore, this MBEE approach maintains the security against RS and bit plane detection analysis. However, this scheme founds the tradeoffs between high capacity and visual quality, because higher embedding capacity reflects in result of lower visual quality of stego-images. Generally, most of the EMD based methods are decided the *n*-base notation system before actual embedding procedure. Therefore, it can be predictable, where this *n*-base notation system should be adaptive i.e. (Kuo, Kuo, et al., 2016).

Another type of hybrid embedding based strategy, a hybrid approach of EMD with LSB and modification of prediction errors (MPE) is presented in (K. Wu, Liao, Lin, & Chen, 2015). Where it improves the embedding capacity, and retains the acceptable visual quality. However, it suffers from low security, because it is unable to resist the histogram and RS steganalysis detection attacks.

(c) ***Pixel/Block Indicator based Methods***

Another strategy of the spatial domain is the pixel/block indicator based steganography. Where, the pixel/block is employed as an indicator for underline embedding technique. An RGB based color image consists of 3 bytes including red, green and blue intensities. Where one of the RGB channels is used as an indicator and the rest are considered as data channels. One of the earlier pixel indicator-based scheme is introduced by (Gutub, 2010). This embeds the secret data by LSB substitution in one or both of the data channels in a predefined cyclic manner. The experimental results of this scheme are effective, in term of embedding capacity and imperceptibility. Meanwhile, it also avoids the key exchange overhead for data indicator signaling. However, embedding capacity is completely dependent on a cover image and its indicator bits. In addition, it hides the fixed number of bits in each pixel, whereas embedding capacity directly affects/degrades the visual quality of the stego-image. Similarly, two embedding techniques are introduced by (Tiwari & Shandilya, 2010).

First, it improves the (Gutub, 2010) method by changing the indicator channel for every subsequent pixel to improve the security factor. Second, the random number generator is employed to estimate the number of secret bits that are embedded by LSB scheme, where up to 4 LSBs can be embedded into the data channel.

A block based RGB indicator steganography technique is presented by (Swain & Lenka, 2012). It divides the image and secret data into each 8 blocks, where a user defined key decides the one to one image and secret block mapping. In embedding process, one channel is considered as an indicator and rests are the data channels. The secret data are embedded by LSB, where the motive is to maximize the image and secret data matching portion, which indirectly reduces the visual distortion in stego-image.

Another indicator based steganography method is proposed in (Mahimah & Kurinji, 2013) by employing a zigzag mannered LSB embedding. It utilizes two different indicators that are based on zigzag traversing order. In result, the visual quality and security of secret data are improved. In (Thanikaiselvan, Subashanthini, & Amirtharajan, 2014) technique, first a cover image is scrambled and further employed by PVD and adaptive LSB embedding technique according to the blue pixel indicator. Where, red and green planes are considered as data channels. The proposed method improves the payload and security by scrambling the red and green planes. However, the visual quality is dependent on embedding capacity. Recently, another color channel indication based steganography technique is presented by (Das & Kar, 2015). In this method, the hiding sequence is controlled by an indicator pattern table, which is further indexed by the secret data bits. During embedding phase, indicator and other metadata are embedded inside the cover image as a header that is further used in the blindly secret data recovery phase. In this scheme, encryption of secret data and RC4 cipher of the header increases another layer of security also the complexity as well.

(d) ***Multi-Base Notation System (MBNS) Methods***

Another spatial domain embedding method based on multiple base notational systems (MBNS) that is introduced to re-express/transform the secret data into the notational system before embedding process. In MBNS based techniques, secret data converted into symbols and re-expressed in the multiple-base notational system, i.e. binary, decimal, and octonary system. Further, these symbols are embedded into pixels intensities. Generally, the larger notational base symbol indicates the larger embedding rate.

Many steganography techniques have been proposed to improve the embedding capacity and imperceptibility in MBNS based technique. M. Afrakhteh et al. presents adaptive more surrounding pixels using (A-MSPU) MBNS technique (Afrakhteh & Ibrahim, 2010) with the motive to enhance the visual quality. Similarly, an adaptive steganographic method based on varying-radix numeral system (VRNS) is presented (Geetha, Kabilan, Chockalingam, & Kamaraj, 2011). The method decomposes the secret data into numerals that have variable data carrying capacity. This decomposition depends on the cover pixels tolerance to manage maximum adulteration for larger secret data. This scheme improves the visual quality, embedding capacity and also retains the security against RS (Jessica Fridrich et al., 2001) steganalysis detection attack. However, the embedding payload is still limited to other radix based techniques. Therefore, (Tang, Song, Chen, & Hu, 2015) improves the (Geetha et al., 2011) VRNS method by introducing an information hiding using adaptation and radix (AIHR) algorithm. However, from the experimental results, this method has larger payload than existing VRNS systems but also has some ambiguity in proposed flow e.g. how the sender and receiver will be synchronized with the selection of bases? Similarly, in AIHR extraction process also suffers from recovering the actual secret data due to *M* parameters.

Recently, a general multiple-base (GMB) secret data embedding technique is proposed by (W.-S. Chen, Liao, Lin, & Wang, 2016). Secret data bits are converted to M-ary secret digits for pixel-cluster (i.e. n pixels). The M is automatically determined by the input function of the end user. It provides multi-purpose embedding styles. In result high embedding and high quality of stego-image can be achieved. Furthermore, this method is able to accurately predict the overall capacity and visual quality by mathematical expression without embedding the real secret data inside images. At lower or 1.0 bpp, GMB method can resist the non-structural SPAM feature based steganalysis and also has resistance against statistical RS steganalysis (Jessica Fridrich et al., 2001). The complexity of the proposed scheme is quite high. However, the performance of this scheme shows the one of the best in existing EMD based techniques.

(e) ***Mapping based Methods***

In the spatial domain, one way of embedding using mapping of secret data with the cover image data. There are numerous methods available i.e. pixel, block, bit-plane mapping etc. Another type of pixels to the alphabetic letter mapping based technique is presented in (Al-Husainy, 2009). English alphabets plus some special characters are mapped to the pixel values with the help of mapping table. Furthermore, these matching patterns are required during embedding and extraction phases. However, this scheme has low computation complexity because there are as such no overhead for texture computation etc. A novel approach based on LSB using X-box mapping is presented (Nag, Ghosh, Biswas, Sarkar, & Sarkar, 2012), where unique pattern of different X-boxes are employed for embedding process. Four unique X-boxes with sixteen different values (represented by 4-bits) are used and further each value is mapped to the four LSBs of the cover image. The security of the proposed method is dependent on mapping rules. However, the visual quality is degrades due to fixed 4-bit LSB substitution.

Another type of embedding technique known as image realization steganography that is presented by (Roy & Changder, 2014). This employs the simple cover-to-secret mapping strategy, where secret image Longest Common Subsequence (LCS) is directly mapped to the cover image. However, it requires high computations due to LCS mapping nature. In addition, the maintenance of auxiliary information is also an overhead of this technique. In literature, there is another way of mapping known as direct bit-plane mapping (i.e. binary, Fibonacci, Prime, Natural, Lucas, and Catalan-Fibonacci) based techniques. Recently, a bit plane mapping method is proposed to improve the visual quality and security (Alan A Abdulla, Harin Sellahewa, & Sabah A Jassim, 2014). It consists of two phases. First, it reduces the secret data size by proposing a secret image size reduction (SISR) algorithm. Second, the compressed data are embedded through Fibonacci representation in pixel intensities to reduce the embedding distortion of the stego-pixels. Therefore, the payload and good imperceptibility attains by using bit-plane(s) mapping instead of bit-plane(s) replacement in the embedding process. Similarly, another virtual bit plane mapping technique is presented in (Alan Anwar Abdulla, Harin Sellahewa, & Sabah A Jassim, 2014). This employs the specific representation to decompose the pixel values into 16 virtual bit planes for embedding process. However, this improves the visual quality and embedding payload against existing pixel decomposition based bit plane mapping techniques.

(f) ***Pixel Pair Matching (PPM) Methods***

Another promising spatial domain steganography strategy is based on pixel pair matching (PPM). Usually, these embedding methods employ the pixel pair $(p_{i,1}, p_{i,2})$ as a reference coordinate to search another coordinate $(p'_{i,1}, p'_{i,2})$ within a predefined neighborhood set of $\phi\ (p_{i,1}, p_{i,2})$ to satisfy $f(p'_{i,1}, p'_{i,2}) = SB$. Where f denoted an extraction function and SB is the secret digit in B-ary notational system. Data embedding scheme is done by replacing $(p_{i,1}, p_{i,2})$ with $\left(p'_{i,1}, p'_{i,2}\right)$ as shown in Figure 2.10.

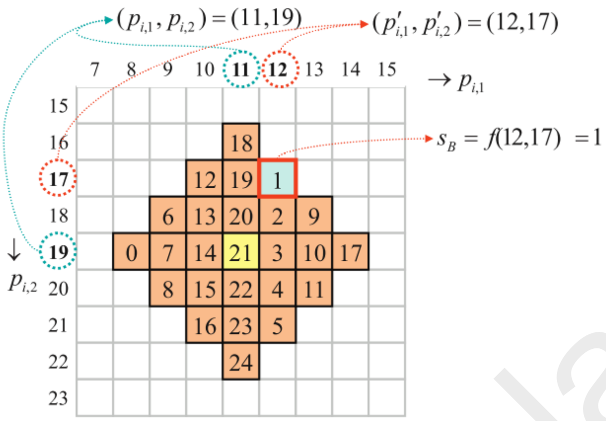


Figure 2.10: The Neighborhood Set ϕ (11,19) (Hong, Chen, & Luo, 2012)

An adaptive pixel pair matching (APPM) method is proposed in (Hong & Chen, 2012), where the two pixels are scanned as an embedding unit. In this scheme, the special sequence is designed as a neighborhood set to embed the secret message digits. Similarly, a patch reference table (PRT) based embedding technique is proposed by (Hong, 2013), where it adopts a single reference table (RT). Further, the PVD concept is utilized with PRT method to improve embedding capacity and visual quality. In this method, a special embedding sequence is designed and the number of secret bits are embedded and estimated by the pixel-value difference. It retains the security against histogram steganalysis, while has limited resistance against SPAM based steganalysis (@ 0.5 bpp).

Another pixel pair matching (PPM) with PVD method is proposed by (J. Chen, 2014). In this method, secret data are embedded adaptively into a pixel pair using two reference tables. Based on the pixel value differences, variable number of secret bits are embedded in the image. This method reduces the falling-off-the problem and provides a larger embedding payload with the acceptable visual quality. In addition, proposed method is able to maintain the shape of pixel difference histogram and also has resistance against chi-square steganalysis.

(g) *Gray Level Modification (GLM) Methods*

Gray level modification (GLM) is also considered as another strategy of spatial domain steganography. These types of embedding methods map the secret data by modifying the gray level of pixels (not hide or embed). Generally, GLM base methods are considered as simple to implement and having minimum computational complexity. However, these methods are unable to resist steganalysis detection attacks.

Recently, a RGB image based gray level modification (GLM) and multi-level encryption (MLE) method is presented in (Muhammad et al., 2015). This approach encrypts the secret data using MLE algorithm before mapping to GLM. The experimental results depict that the proposed method has less complexity than other standard encrypted steganographic methods. Furthermore, this improves the visual quality although it suffered from statistical steganalysis detection attacks.

(h) *Prediction Error based Methods*

The prediction based spatial domain embedding techniques also gained a lot of attention in recent years. Generally, the direct altering of pixel values for embedding leads to distortion of visual quality and it causes the lower embedding capacity if the good visual quality is also the motive of the proposed scheme. Therefore, predictive coding technique is proposed to resolve the above problems. Generally, in these techniques, the pixel intensities are predicted through predictor instead of direct modifications. The predicted error values are modified to compensate for secret data. In literature, various predictions based reversible embedding techniques are proposed to improve existing ones.

In (Yu, Chang, & Hu, 2005), a prediction error based image steganographic method is proposed to modify the predictive errors. Due to the use of uniform quantization embedding rule, the prediction errors distribution during the embedding process propagates the visual artifacts that are led to steganalysis. Similarly, a modification of prediction error (MPE) technique is presented in (Hong, Chen, & Shiu, 2009), whereas it modifies the histogram of prediction errors to find the vacant position for secret data embedding. The overall visual quality of MPE method guaranteed to above 48 dB PSNR, while embedding capacity is also improved by well-known classic Ni et al. method. Another proposed predictive coding based reversible embedding technique in (Hsien-Chu Wu, Wang, Tsai, & Wang, 2010), this method employs the secret data into compress codes which are utilized during the lossless image compression coding. At the predictive coding stage, the proposed method embeds the secret data into error values by referring to a hiding tree. In reverse, secret data can be recovered by referring to the hiding tree at entropy coding stage. This method provides the largest up to 0.0992 bpp embedding capacity with respect to lossless steganography techniques.

Recently, (K. Wu et al., 2015) employ the MPE technique with other steganographic LSB and EMD methods to enhance the high capacity based steganography solution. Similarly, To obtain the higher rate of embedding capacity, a multiple predictor based data embedding approach is presented (Jafar, Darabkh, Al-Zubi, & Al Na'mneh, 2015). This multiple predictor's mechanisms are basically the extension of MPE approach to embed the secret data without adding any predictor overhead. During embedding process, the selection of accurate predictor depends on the history of the predictor. The proposed method shows the improvement in embedding payload and visual quality, while security is still questionable.

(i) ***Histogram based Methods***

Histogram based data hiding is another commonly used steganographic technique. The histogram shifting is considered the most efficient histogram based embedding schemes. It has the following phases, first, it finds the peak and zero points in a cover image, whereas the bins are shifted with one level between the zero and peak points for emptying peak points. In the second phase, the secret bits are concealed by predefined adjustments in new peak point and the empty point.

In (P. Tsai, Hu, & Yeh, 2009) embedding scheme, a cover image is divided into 5x5 non-overlapped image blocks. In each block, the center pixel is treated as a base pixel for linear prediction process, whereas the other (remaining) pixels in the block are processed by linear prediction to generate the residual values. The histogram of residual is employed by histogram shifting to store secret data, whereas, multiple pairs of peak and zero points are used the histogram shifting to increase the embedding payload. Furthermore, another novel (X. Li, Zhang, Gui, & Yang, 2013) technique is presented based two-dimensional difference histogram modification and difference pair mapping. In this method, a pixel pair selection strategy enhances the performance of reversible embedding. The pixel pair selection strategy is able to accurately locate the targeted pixels in smooth regions. Therefore, this strategy performs much better on smooth images than the heavily texture based images.

A novel hybrid steganographic method is presented based on histogram shifting with difference expansion and interpolation technique (Lu, Chang, & Huang, 2014). In this scheme, the secret data are embedded in two ways i.e. concealable pixels and difference of interpolated pixels. Therefore, the proposed method gains a high payload against existing compared methods. Similarly, another reversible embedding (Z. Pan, Hu, Ma, & Wang, 2015) technique is presented based on histogram shifting, where the neighboring points of the peak point are used to embed secret data using histogram shifting, while the peak point remains unchanged. The concept of localization is introduced to generate more peak points, where the neighboring points are embedded by more secret data. In fact, the localization equally redistributes the greater histogram changes into small changes and keeps the similar histogram to cover image. It improves the embedding capacity by exploiting the localization with multilayer embedding.

Recently, reversible data embedding technique with histogram shifting for medical images is presented (N.-K. Chen, Su, Shih, & Chen, 2016). Generally, reversible embedding techniques require an extra data as a location map for reconstruction of cover images. To reduce the size of the location map, the proposed method keeps the information record in just two bits of each block, ultimately it significantly reduces the size of the location map table, while achieving an efficient data embedding by histogram shifting.

(j) ***Machine Learning/Modern Steganography Methods***

In spatial domain embedding methods, the optimization techniques are employed to improve the success of embedding algorithms. Where an embedding method by Tseng et al. is presented based on OPAP and genetic algorithm (GA) (L.-Y. Tseng, Chan, Ho, & Chu, 2008). This improves compatibility of cover and stego-images by altering the secret bits. Similarly, GA-based technique is applied as setting parameters of the objective mapping function (high imperceptibility), where it obtains the best condition in the distribution of pixels by employing LSB substitution (Masoumeh Khodaei & Faez, 2010). Another spatial domain GA-based reversible data embedding method is presented with tunable visual quality (Kanan & Nazeri, 2014). This method models the hiding process as a search and optimization problem. As a result, embedding payload and visual quality are enhanced. However, the computational complexity is quite high, while the security analysis is still questionable. To obtain a larger embedding payload, recently a steganography method based on adaptive neural networks (ANN) with modified particle swarm optimization (PSO) is proposed (El-Emam, 2015). This scheme achieves the good imperceptibility while maintaining the high security with larger embedding payload as proved in its experimental results. Another method, a three-phase intelligent technique for color images is presented with the motive of improving imperceptibility and embedding payload (El-Emam & Al-Diabat, 2015). The first phase of a learning system (LS) is applied before embedding steps, while the other phases are applied after embedding process. The ANN and adaptive GA are applied to estimate the number of embedded secret bits inside the pixels. The results show that the proposed algorithm is able to embed larger payload up to 12 bpp with having tradeoffs in visual quality. Recently, chaotic map based technique is proposed to improve the data hiding technique using GA (Doğan, 2016). In this method, the GA fitness function is selected based on PSNR. Further, the various sizes of secret data are employed into the cover image using random functions and chaotic maps. Meanwhile, the randomness of genetic algorithm is performed by using different chaotic maps, i.e. gauss, logistic, tent. Finally, chaotic maps are considered the fastest than random function for steganographic technique. These aforementioned techniques stand in the category of high computationally expensive methods due to optimization based methods i.e. GA.

In the next section, comprehensive performance comparisons of spatial domain image steganography techniques in recent 5 years are presented in tabular form (Table 2.3). Where, we tried to highlight their strengths and expected challenges with respect to each proposed technique. In addition, the quantitative evaluation metrics are directly taken from the respective papers, i.e. embedding capacity, visual quality and security. Meanwhile, Figure 2.11 depicts the chronological orders of steganography methods of its efficiencies in recent 5 years.

Table 2.3: Performance of Recent Spatial Domain Steganography Techniques

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(Sarreshtedari & Akhaee, 2014)	LSB-based	±1 LSB	- High imperceptibility - Simple implementation - Reduced probability of change per pixel	- Lower capacity compared to existing LSB-based methods - Secret key dependency	1 bpp (gray)	52.90 dB	HCF-COM (normal, calibrated, adjacency)
(Qazanfari & Safabakhsh, 2014)	LSB-based	GLSB++	- Improved visual quality - Reduced extra bit embedding in existing LSB++ technique - Secure against Histogram analysis	- High complexity for new cover to compute lock key - Encryption key dependency - No robustness	≈ 0.8 bpp (gray)	> 50 dB	Preserve the Histogram, Chi-Square
(Yuan, 2014)	LSB-based	Adaptive ±1 operation LSB	- Utilize multiple covers with location sensitive secret embedding in 2 LSB planes - Stego-key less - Low modification per pixel - Time efficiency	- Overhead of multiple cover images for the steganographic process - Limited embedding capacity even employing multiple covers	NA	≈ 50 dB	SPAM 2nd order with SVM
(Xu et al., 2016)	LSB-based	Modulo-three	- Improved embedding capacity - Maintain the acceptable visual quality - Employ ternary secret data for embedding	- Not reported security against statistical steganalysis. - Proposed method exposed @ 0.25 bpp by SPAM feature based analysis.	3.16 bpp (gray)	≈ 37 dB	SPAM 2nd order with SVM
(Muhammad, Ahmad, Rehman, Jan, & Sajjad, 2016)	LSB-based	ALSB-MLEA	- Multi-level encryption applied on stego-key as well as secret data - Channel indicator based embedding for secrecy - Keeps balance between security and imperceptibility - Light-weight than encryption	- Limited embedding capacity	≈ 1 bpp	> 45 dB	Histogram, Robustness against salt & pepper noise

Table 2.3, continued.

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(Tavares & Junior, 2016)	LSB-based	LSB-WH	- Based on Word hunt puzzle approach - Reduced modification of per pixel value - High imperceptibility	- Note reported any modern steganalysis	NA	NA	Chi-Square
(Nguyen et al., 2015)	LSB-based	MPBDH	- Block based multi-bit plane adaptive LSB embedding - Efficient texture complexity levels are computed by an adaptive threshold - Maximum utilization of all texture regions - Reduce visual attacks	- RSA and AES key maintenance dependency for encryption - Limited embedding capacity	≈ 1.5 bpp (gray)	≈ 46 dB	SPAM with Ensemble Out of Bag (OOB) @ low bpp
(Lee et al., 2012)	PVD-based	PVD-TPVD	- Secret image communication - Can embed larger secret image against the cover image - TPVD utilized for embedding - JPEG2000 compression applied on the secret image to reduce size	- High complexity - Lack of other statistical steganalysis evolution	1.64 bpp (gray)	≈ 40 dB	RS analysis
(Balasubramanian et al., 2014)	PVD-based	Octonary PVD	- Exploited the all eight directions for higher embedding capacity - Adaptively region based embedding - Readjustment phase maintains regions after embedding to fully recovery of secret data - Resistance against various specific and universal statistical steganalysis	- Not reported any modern steganalysis evaluation.	≈ 3.6 bpp (gray)	≈ 40.20 dB	RS analysis, HCF-COM, LSB matching, PVD analysis

Table 2.3, continued

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(S. Shen et al., 2015)	PVD-based	MF-PVD	- A simple implementation for reversible embedding - Utilized the correlation of R G B channels - Resolve the underflow /overflow problem	- PSNR is marginal acceptable. - Not reported any modern steganalysis detection attacks	≈ 1.03 bpp (color)	≈ 36dB	RS analysis, Pixel Difference Histogram
(Hernández-Servin et al., 2015)	PVD-based	PVD-TPVD	- Eliminate the location map of overflow/underflow (TPVD) - Replace the range table with simple linear function - Resolve boundary problem	- Not discussed any robustness - Not reported any security against steganalysis	≈ 1.55 bpp	≈ 36.25 dB	NA
(Swain, 2015)	PVD-based	Ad-PVD	- Application based adaptive solutions - Efficient horizontal and vertical edge directions are considered for embedding	- Note reported modern analysis - Lower embedding capacity compared to existing PVD based method.	≈ 1.74 bpp (color)	≈ 46.65 dB	RS analysis, Pixel Difference Histogram
(Grajeda-Marín et al., 2016)	PVD-based	TPVD	- Skip overflow/underflow problems - Improved visual quality in TPVD-PVD - 100% utilization of pixels for embedding	- Embedding capacity is limited to existing methods - Not reported any security against steganalysis	≈ 2.41 bpp (gray)	≈ 38.33 dB	NA
(Kieu & Chang, 2011)	EMD-based	FEMD	- Massively enhanced capacity - Adaptive payload solution - Exploited eight directions for EMD - Embedding with minimal distortion	- Not handled any overflow condition - Not reported security against steganalysis	1 to 4.5 bpp (gray)	≈ 52 to 31 dB	NA

Table 2.3, continued

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(H.-M. Sun et al., 2011)	EMD-based	Ad-EMD, HoEMD	- Improved capacity - Adaptive texture based embedding - Resolve the overflow/ underflow problem	- Limited steganalysis evaluation	2.5 to 3.5 bpp (color)	≈ 43 to 34 dB	Chi-Square
(Kuo et al., 2013)	EMD-based	GEMD	- Resolve the extraction function fixed weighting with dynamic modulus table - Extraction function: lookup & formal form	- Only two pixels limited relationship in embedding - All pixels modifications occurs - Note reported resistance against steganalysis	1.5 bpp	≈ 50.17 dB	NA
(Kuo, Wang, et al., 2016)	EMD-based	MSD	- Reduce the pixel modification ratio (n/2) - Only ± 1 ranges variations - Maintain the bpp with increasing of n pixel	- Limited embedding capacity	1 bpp	> 52 dB	RS analysis, Bit plane attacks
(Kuo, Kuo, et al., 2016)	EMD-based	MBEF	- Improved embedding capacity - Flexible adjacent pixel relation up to *n* - Adaptive embedding - Not required any secret data conversion - Handled the overflow/ underflow problem	- Lower visual quality against EMD approach i.e. *n=2* - Higher embedding capacity reduces the visual quality	3.25 bpp	≈ 37.24 dB	RS analysis, Bit plane attacks
(Geetha et al., 2011)	MBNS-based	VRNS	- Renowned numerical model - Good visual quality as embedding required minimal visual distortion	- Not reported security against modern steganalysis - Limited embedding capacity with recent methods	≈ 1 bpp	≈ 41 dB	RS analysis

Table 2.3, continued

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(W.-S. Chen et al., 2016)	MBNS-based	GMB	- Adaptive capacity based solution - Predict the embedding capacity w.r.t to visual quality by mathematical expression - Content adaptive multi-base embedding - Increase security by coefficient mapping	- High complexity - Greater than > 1 bpp, SPAM analysis can be successful	≈ 1.46 to 3.8 bpp	≈ 50 to 35 dB	RS analysis, Histogram, SPAM analysis
(Muhammad et al., 2015)	GLM-based	GLM-MLE	- High imperceptibility - Low computation cost by skipping the conventional encryption of the secret message - Multiple levels of security - Robustness against salt & pepper	- Limited embedding payload - Not reported steganalysis evaluation	8 KB	≈ 57 dB @ 8 KB	NA
(Hong, 2013)	PPM-based	APPM	- Adaptive to visual quality vs payload - Special embedding sequences incorporated - Maintain the statistical image features	- Reference tables overhead	1 to 4 bpp	≈ 52 to 35 dB	RS analysis, Histogram, SPAM analysis
(J. Chen, 2014)	PPM-based	PPM-PVD	- Random embedding characteristics - Reduce falling-off-problem of PVD - Complex embedding order to enhance security	- Reference tables overhead - Not reported resistance against modern steganalysis	≈ 1.3 to 2.53 bpp	≈ 50 to 42 dB	Histogram, Chi-Square
(Z. Pan et al., 2015)	Histogram-based	RDH-HS-ME	- Adaptive approach - Localization keeps the histogram intact - Improved capacity with less distortion	- Limited security evaluation - Low embedding capacity	< 1 bpp	≈ 30-50 dB	Histogram
(N.-K. Chen et al., 2016)	Histogram-based	RDH-HS	- Reduce the location map size - Avoid underflow/overflow problem - Efficient while transmission	- No robustness or security discussed	NA	NA	NA

Table 2.3, continued

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(Ioannidou et al., 2012)	Edge-based	Hybrid-Edge-ALSB	- Efficient texture evaluation by the hybrid edge detector - Gradually embedding by sensing the edge regions - High imperceptibility and capacity	- Extra logging information required in decoding phase - Not reported any steganalysis evaluated	1.88 bpp	≈ 44 dB	NA
(H.-W. Tseng & Leng, 2014)	Edge-based	ALSB	- Efficient edge detection by the hybrid fuzzy edge detector - Adaptive LSB embedding based on block-based edge/texture computation while retaining minimum distortion by MSE	- Not evaluated by steganalysis - Low embedding rate against recent methods	≈ 2.41 bpp	≈ 38.18 dB	NA
(Jung & Yoo, 2014a)	Edge-based	Edge-Interpolation	- Hybrid approach with interpolation - Improved embedding capacity	- Resolution conflict due to interpolation, attraction for the attacker - No steganalysis evaluation	≈ 399,115 bits (256x256)	> 35dB	NA
(Al-Dmour & Al-Ani, 2016)	Edge-based	E-XoR coding	- Can be employed in both spatial and transform domain - Edge adaptive embedding - Simple implementation	- Non-adaptive thresholding overhead	> 1 bpp	> 40 dB	Histogram, Li110D with SVM
(S. Sun, 2016)	Edge-based	Canny-Huffman	- Improved visual quality and capacity - 2k correction maintains visual quality - Secret image data transform by Huffman encoding to achieve compression and security	- Limited embedding capacity - Encoding complexity - Not reported resist against modern steganalysis, RS analysis	< 1 bpp	≈ 60 dB	Histogram

Table 2.3, continued.

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(Roy & Changder, 2014)	Mapping-based	LCS	- Limited modification in the cover image - Embedding capacity can be higher than cover image - String based mapping	- Computationally expensive - Auxiliary and realization information maintenance	NA	NA	NA
(Alan A Abdulla et al., 2014)	Mapping-based	Fibonacci 3bit-plane mapping	- Reduce secret data size up to 66% by SISR compression - Fibonacci embedding reduces the visual distortion effects	- Compression overhead - Not reported security against modern steganalysis - Eventually low payload	465301 compressed bits	> 50 dB	RS and WS analysis
(Swain & Lenka, 2012)	Pixel/ Block indicator-based	BI	- Block based channel indicator - Simple to implement - Use adaptive channel selection	- Encryption overhead - Indicator information handling	240632 compressed bits	> 42.75 dB	NA
(Mahimah & Kurinji, 2013)	Pixel/ Block indicator-based	PI-zigzag	- Use the Zigzag direction of embedding - Multi-mode of indicators - Adaptive channel embedding	- Not reported security against statistical analysis i.e. RS analysis is compulsory due to LSB - Limited embedding capacity	< 1 bpp	> 50 dB	NA
(Kanan & Nazeri, 2014)	AI based	GA	- Adaptive embedding - Tunable visual quality of stego-image - Lossless secret embedding	- Computationally expensive - Lack of steganalysis evaluation	0.5 to 3.95 bpp	≈ 34-55 dB	NA
(El-Emam, 2015)	AI-based	ANN-MPSO	- Proposed a comprehensive method - 5 layers of security - Improved capacity and visual quality.	- Highly complex	Up to 12 bits/pixel (color)	> 55 dB	WFlogSv, WAM, OOB

Table 2.3, continued.

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(El-Emam & Al-Diabat, 2015)	AI-based	ANN-PSO-GA	- Hybrid utilization of ANN with GA - 7 layers of security - Reduce the number of iterations - Efficient in training time	- Extensive computations	Up to 12 bits/pixel (color)	> 50 dB	Pixel difference histogram, OOB
(Doğan, 2016)	AI-based	ANN-GA GA-Chaotic	- Chaotic map improved GA-based hiding - Chaotic map results faster than random function	- NA	NA	> 52 dB	NA
(Jung, 2010)	Hybrid	PVD-ALSB	- Simple implementation - Efficient region utilization for LSB and PVD embedding	- Lack of steganalysis evaluation - Low visual quality	3 bpp (gray)	≈ 36.28 dB	NA
(Liao, Wen, & Zhang, 2011)	Hybrid	OPAP-FPVD	- Simple implementation - Adaptive LSB embedding based on lower (smooth) and higher (edge) levels - Four pixels difference employing	- Not reported any security against any steganalysis	≈ 3.15 bpp (gray)	≈ 39.11 dB	NA
(M Khodaei & Faez, 2012)	Hybrid	ALSB-PVD-OPAP	- Improved embedding payload - Efficient utilization of PVD with ALSB	- Steganalyzed at higher embedding rate by modern analysis	> 3.04 bpp (gray) T=1,k=3	≈ 38 dB	RS analysis, SPAM feature analysis
(Y.-Y. Tsai et al., 2014)	Hybrid	LSB-PVD	- Adopted dynamic block division for adjustable embedding rate - Fully utilized image boundary regions - Resolve the overflow problem	- Not reported security against any statistical or non-statistical steganalysis	≈ 3.08 bpp (gray)	≈ 35.64 dB	NA
(Lu et al., 2014)	Hybrid	RDH-DE-IN-HS	- Hybrid with interpolation - No peak point searching - No compression overhead	- Limited visual quality - Limited embedding capacity	< 1 bpp	≈ 33 dB	Histogram

Table 2.3, continued.

Reference	Approach	Algorithm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
(S.-Y. Shen & Huang, 2015)	Hybrid	IEMD-PVD	- Efficiently estimate the base digit by PVD for EMD embedding - Exploit the Hilbert curve traversing for locality preserving and minimal distortion - Resolve the overflow/ underflow problem	- Limited payload as compared to other EMD based methods - Not reported security against modern analysis	1.53 bpp	≈ 42.46 dB	RS analysis, Pixel Difference Histogram
(K. Wu et al., 2015)	Hybrid	MPE-LSB-EMD	- Hybrid embedding of irreversible & reversible methods - Balanced steganographic solution; payload vs visual quality - Application adaptive solution	- Extensive PSNR measuring on every bit of embedding becomes computationally complex - Not reported security against any statistical or non-statistical steganalysis	> 1 bpp	> 35dB	NA
(Das & Kar, 2015)	Hybrid	PI-LSB-PVD	- Color channel based indicator - Hiding sequence controlled by pattern table indexed by secret data - Stego-image itself retained the auxiliary information	- Encryption header is another data overhead - Lack of evaluation of security against structural steganalysis	2.4 bits per channel (color)	> 39 dB	Histogram analysis
(Swain, 2016)	Hybrid	Directional-PVD-ALSB	- Three directional PVD block based embedding - Adaptive solutions for higher visual quality and higher capacity with good quality - Integration of ALSB with PVD	- Step effects as histogram analysis - Not reported security against modern analysis	≈ 3.03 to 3.17 bpp (color)	≈ 40.44 to 39.29 dB	RS analysis

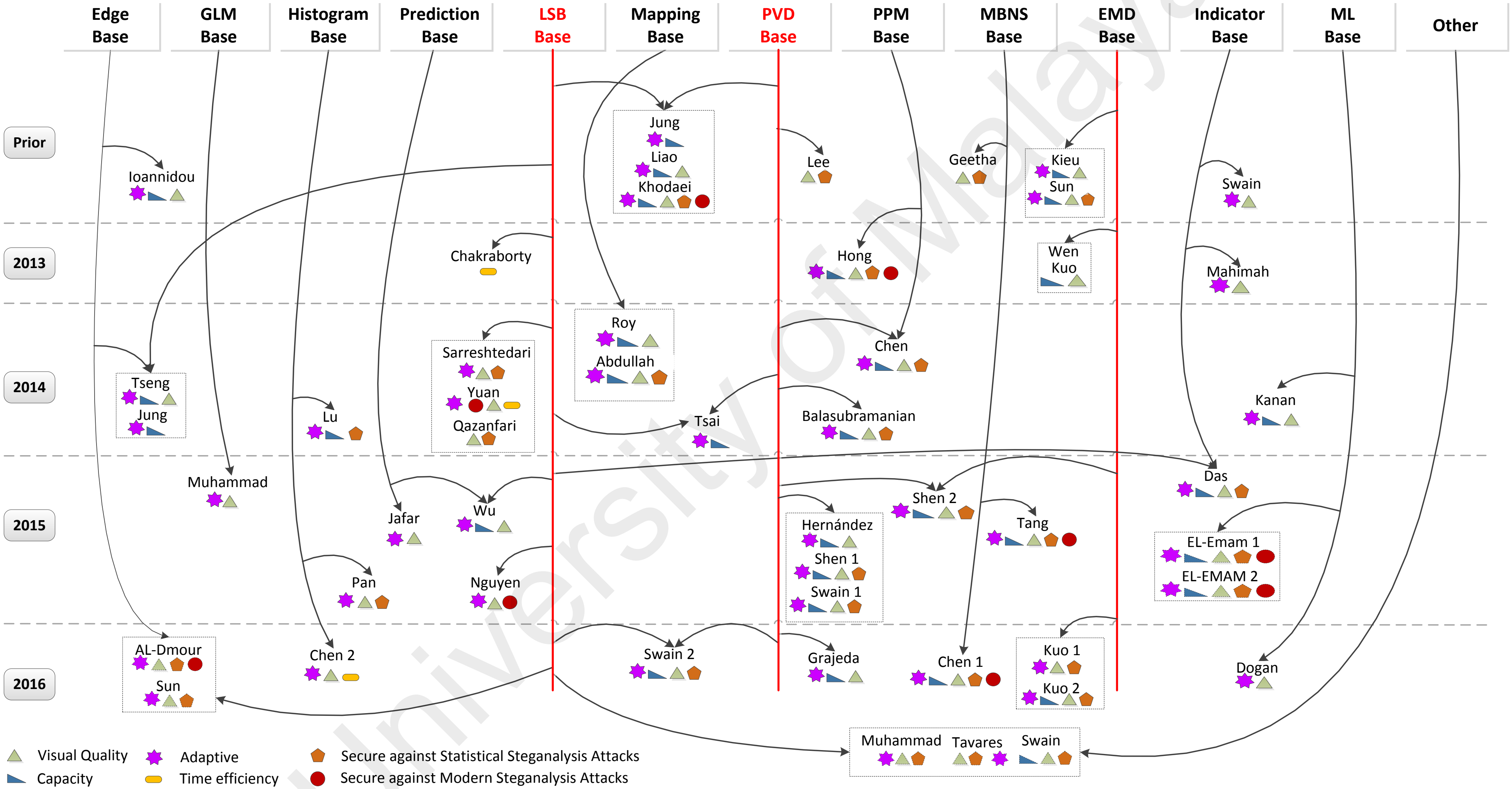


Figure 2.11: Chronological Orders of Spatial Domain Steganography Techniques with its Efficiencies

2.4 An Overview of Common Issues

In this section, we highlighted some observed issues in existing image based steganography techniques. The discussion over these issues leads us to our research problem.

2.4.1 High Capacity based LSB Substitution Issues

As we observed from Section 2.3.1, the aforementioned LSB based techniques are considered a simple way of information hiding and are flexible to integrate with other approaches based on various strategies (Section 2.3.3). In these methods, the main issue is the direct relation between embedding capacity and visual quality of stego-image. For example, most of the LSB based substitution methods that are designed to achieve the high rate of embedding capacity, where, it directly and indirectly modifies the multi-bit planes of pixels to accommodate the maximum secret data based on various adaptive embedding strategies. However, the resultant modification differences between cover and stego-pixels reduce the visual quality (PSNR) and increase the risk of steganalysis detection attacks. Conversely, the techniques mentioned earlier are specifically designed to enhance the visual quality by reducing the modification changes and differences in LSBs of the pixels. However, that approaches have limited embedding capacity of around ≈1 bpp. From the above tradeoffs in capacity vs. visual quality, it concludes that, *there is an inability to generate the closest/similar stego-pixels to its respective cover-pixels in high capacity based substitution methods, which indirectly decreases the visual quality and security against steganalysis detection attacks*. Therefore, in this thesis, the focus is on the high embedding capacity based substitution technique, which improves the visual quality and security.

2.4.2 High Imperceptibility based Pixel Value Differencing Issues

From Section 2.3.2, we can observe all the PVD based methods that employ different directions, multiple pixels pairing and even combining the PVD approaches with other steganography techniques to increase the embedding payload, quality, and security. Meanwhile, it also resolves internal PVD method issues, i.e. underflow/overflow, histogram steps against detection etc. As noticed, the core PVD based methods can only achieved a certain level of embedding capacity with ensuring of high visual quality. Therefore, the majority of PVD methods are integrated with other steganography approaches to achieve larger embedding payload while some of them are still suffering from lower visual quality (PSNR) because of its employed strategies. As observed that PVD based methods still have the tradeoffs in steganography objectives.

Furthermore, it was noticeable that all the aforementioned PVD based methods employed the identical pixels *difference adjustment process*, where this process accommodates the novel differences between selected pixels. To the best of our knowledge, this pixels *difference adjustment process* is still underutilized and is considered as an *inefficient* usage of difference adjustment between selected pixels. However, this inefficient difference adjustment process results in a limited embedding capacity in all the PVD (even hybrid) based techniques. Therefore, *the pixel differencing techniques are unable to simultaneously accommodate the extra secret data bits during pixel difference adjustment process*.

2.4.3 General Observations based on all Existing Steganography Methods

Table 2.3 presented a comprehensive analysis of spatial domain image steganography techniques. It highlights the strengths and limitations of the techniques with quantitative statistics. For better understanding, Figure 2.11 illustrates chronological orders chart of recent 5 years based steganography techniques with achieved statistics.

As concluded, we observed that the recent steganography techniques derive other embedding techniques to strengthen its efficiency in term of steganography objectives, i.e. capacity, visual quality, and security. Meanwhile, most of the steganographic methods are evolved as an adaptive hybrid embedding techniques to achieve better results. Furthermore, most of the recent steganography techniques have tradeoffs in general steganography objectives. However, the strengths of hybrid steganography cannot be neglected in term of its security and capacity concern. Meanwhile, *we observed that a powerful singular steganography technique definitely gained positive impact when it is employed as a hybrid technique*. Therefore, in this thesis, we employed the proposed steganography techniques in hybrid embedding manners and also gained the overall steganography objectives.

2.5 An Overview of Proposed Techniques

The concern of this study is to enhance the visual quality and embedding capacity using novel substitution and pixel differencing techniques. In addition, this study employs the above-proposed solutions into hybrid manners to enhance the steganography objectives statistics. Our main objective is to design a novel substitution based image steganography technique that has the advantage of larger embedding capacity, improved imperceptibility, and enhanced security against structural and statistical steganalysis. Therefore, in order to achieve larger embedding capacity, we proposed a novel right most digit replacement technique that provided up to 3 bpp secret data embedding rate (in Chapter 4). For improving visual quality, the proposed technique introduces an efficient closest selection process that increases the similarity between cover and stego-pixels (+39 PSNR). Furthermore, the process of substitution of digits instead of bits in pixels also reduces the risk of statistical steganalysis (RS analysis). In Chapter 5, we have presented another steganography technique, which aims to enhance the embedding capacity in existing PVD based methods without losing the visual quality and security. Therefore, the proposed technique efficiently exploits the pixel difference adjustment strategy with the correlation of secret data bits. As a result, it improved the embedding capacity in all type of PVD based methods. Furthermore, we exploit the above two embedding techniques in hybrid mannered steganography (in Chapter 4 and 5). We also demonstrated the hybrid versions of proposed techniques produce the stego-images with the highest ratio in all matrices i.e. bpp, PSNR, and undetectability.

Another major concern of this thesis is to achieve the highest ratio in embedding capacity and visual quality in both substitution and pixel differencing based steganography mechanisms while retaining the security aspect as well. As observed, the substitution and pixel differencing based embedding approaches are widely employed in both singular and hybrid manners. Therefore, the progressive improvement in these (substitution and pixel differencing) methods indirectly improves the performance of its hybrid approaches as well.

2.6 Chapter Summary

In this chapter, the basics of image steganography were discussed in term of its model component and different classification. Furthermore, the spatial domain image steganography techniques have been reviewed. The spatial domain methods included: substitution, pixel value differencing and other distinct approaches that may incorporate the LSB and PVD based methods to improve its steganographic objectives. A comparative summary of recent existing image steganography techniques was also presented by highlighting the embedding capacity, visual quality, and security of each technique. Furthermore, common issues in improving the steganography objectives were highlighted, mainly in substitution and pixel differencing based steganography techniques. Finally, we presented overview of the proposed methods adopted in this thesis and discussed the main planned contribution to achieve optimal steganography objectives in substitution and pixel differencing based methods.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter discussed the proposed methodology, for the development of novel steganography solutions based on substitution, pixel differencing and its hybrid techniques for digital images.

3.1 Introduction

In the previous Chapter 2, the various methods developed critically reviewed in spatial domain steganography for digital images. Generally, an ideal image steganography must pose the highest ratio in all steganography objectives (e.g. high capacity, high visual quality, and high security). However, noted from the literature review that it is difficult to achieve the highest ratio in all steganography objectives due to the tradeoffs in objectives. Therefore, most of the steganography techniques improved some steganography objectives while retained the other ones. From this aspect, next few paragraphs will give the exact direction of proposed research.

It is noted from the output of literature review that many substitutions based techniques are able to achieve the high embedding capacity, but it reduce the visual quality and security of stego-images due to the increase of cover and stego-pixels differences ratio (Section 2.4.1). Thus, the novel substitution based steganography method becomes essential. However, this study will help to improve the visual quality and security while retaining the high embedding capacity in substitution based steganography technique.

We also observed that pixel-differencing techniques are able to achieve the highest ratio of visual quality in stego-images. However, it suffered from the lower embedding capacity rate due to its internal limited pixel adjustment procedures (Section 2.4.2). Therefore, the pixel differencing technique is also essential with respect to high embedding capacity rate. However, this study will also help to improve the embedding capacity while retaining the similar visual quality and security of all pixel differencing based techniques.

Furthermore, we noticed from the recent literature review that most of the steganography methods evolved as hybrid adaptive embedding techniques using substitution and pixel differencing methods to provide better results. However, most of the hybrid methods are unable to maintain the balance among capacity, visual quality and security. Thus, the novel hybrid adaptive steganography methods that retain the highest ratios in above steganography objectives become important. Therefore, this study will help to obtain substitution and pixel differencing based hybrid steganography methods to keep the optimal balance among steganography objectives. In the next section, we present the system requirements.

3.2 System Requirement

The proposed system for all steganography algorithms for digital images developed using Matlab programming version R2013b on Intel (R) Core(TM) i7 computer having @ 3.40 GHz processor speed, 64-bit operating system, and 8GB RAM.

3.3 Research Methodology

The proposed methodology that used in this research showed in Figure 3.1. The methodology consists of three major phases, Phase I: a literature review, Phase II: design and development of proposed techniques and Phase III: performance evaluation.

3.3.1 Phase I: Literature Review

In the first phase of the proposed methodology, we conducted the literature review in (Chapter 2) of the existing spatial domain image based steganography techniques. This phase identified the strengths and limitations of existing techniques and highlighted the issues. Therefore, based on the identified issues, the second phase of the research methodology is to design and implement the novel steganography solutions.

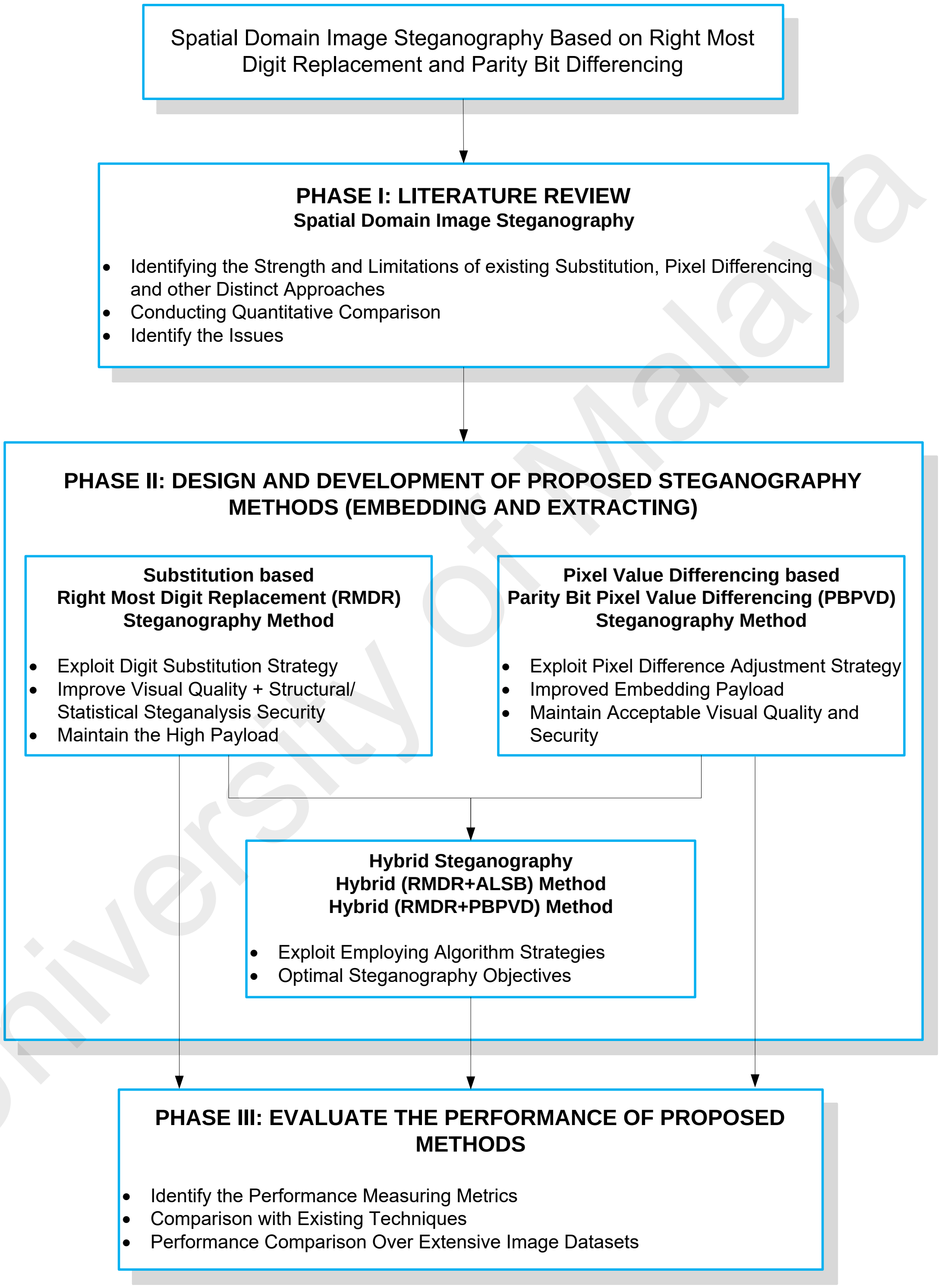

Spatial Domain Image Steganography Based on Right Most Digit Replacement and Parity Bit Differencing
PHASE I: LITERATURE REVIEW
Spatial Domain Image Steganography
• Identifying the Strength and Limitations of existing Substitution, Pixel Differencing and other Distinct Approaches
• Conducting Quantitative Comparison
• Identify the Issues
PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHODS (EMBEDDING AND EXTRACTING)
Substitution based Right Most Digit Replacement (RMDR) Steganography Method
• Exploit Digit Substitution Strategy
• Improve Visual Quality + Structural/ Statistical Steganalysis Security
• Maintain the High Payload
Pixel Value Differencing based Parity Bit Pixel Value Differencing (PBPVD) Steganography Method
• Exploit Pixel Difference Adjustment Strategy
• Improved Embedding Payload
• Maintain Acceptable Visual Quality and Security
Hybrid Steganography
Hybrid (RMDR+ALSB) Method
Hybrid (RMDR+PBPVD) Method
• Exploit Employing Algorithm Strategies
• Optimal Steganography Objectives
PHASE III: EVALUATE THE PERFORMANCE OF PROPOSED METHODS
• Identify the Performance Measuring Metrics
• Comparison with Existing Techniques
• Performance Comparison Over Extensive Image Datasets

Figure 3.1: Research Methodology

3.3.2 Phase II: Design and Development of Proposed Steganography Methods

The second phase of this research methodology is to design and implement the proposed steganography techniques with respect to identified issues in the literature review section. This phase II of research methodology categorized the proposed steganography solutions into substitution, pixel differencing and its hybrid strategy based approaches. In this thesis, we designed four steganography techniques, two singular (substitution and pixel differencing based) and two of its hybrid (substitution + pixel differencing based) approaches as shown in phase II of the research methodology Figure 3.1. Furthermore, each proposed steganography method requires the embedding and extracting sub-phases for the design and development process of phase II. Therefore, the detail of these embedding and extracting sub-phases of novel steganography techniques are as follows.

3.3.2.1 Embedding Phase of Steganography Method

In this section, we present the embedding methodology of proposed steganography techniques under the phase II in Figure 3.1. This consists of input, pre-processing, embedding algorithm and output stages as showed in Figure 3.2. The detail discussed below.

The input image and secret data are required to proceed the embedding process as showed in Figure 3.2. The input image known as cover/carrier image that is used to conceal the secret data. This research studies the raw/uncompressed grayscale images for proposed embedding techniques. In addition, various types of texture-based images are employed for testing and evaluating the proposed algorithms.

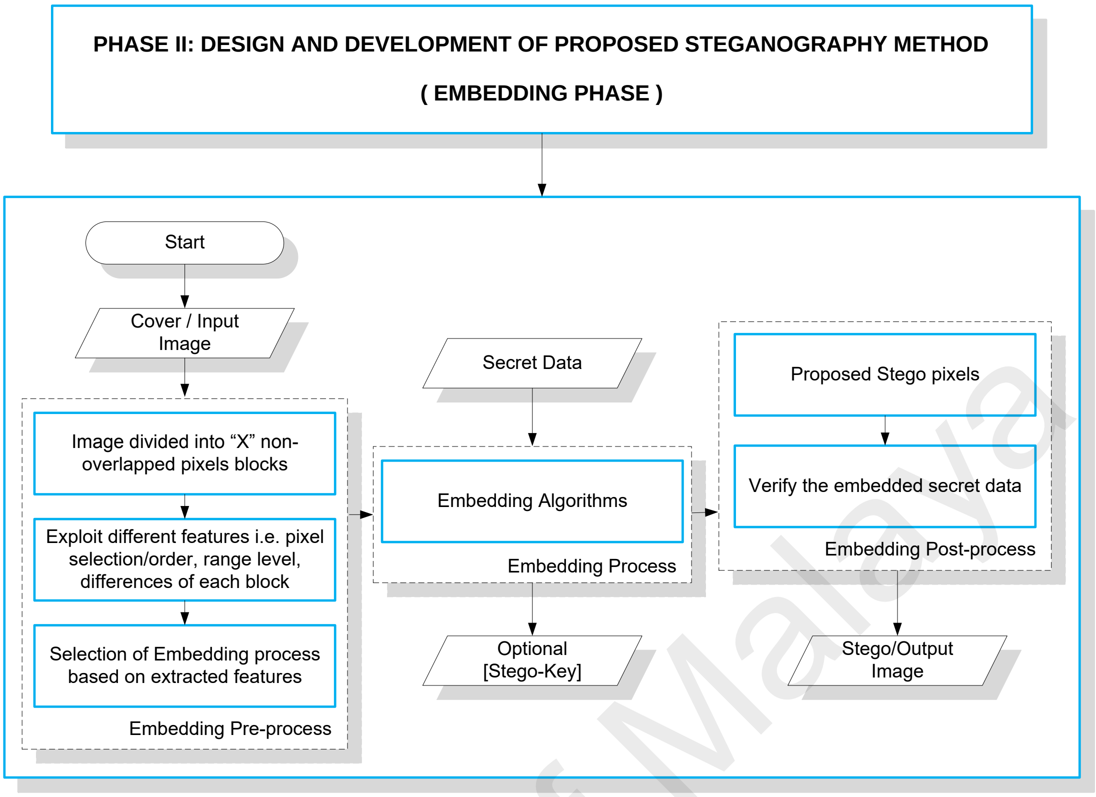

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EMBEDDING PHASE)
Start
Cover / Input Image
Image divided into "X" non-overlapped pixels blocks
Exploit different features i.e. pixel selection/order, range level, differences of each block
Selection of Embedding process based on extracted features
Embedding Pre-process
Secret Data
Embedding Algorithms
Embedding Process
Optional [Stego-Key]
Proposed Stego pixels
Verify the embedded secret data
Embedding Post-process
Stego/Output Image

Figure 3.2: Steganography Embedding Phase in Research Methodology

(a) ***Embedding Pre-Processing***

After selecting the input/cover image (as showed in Figure 3.2), the next stage of this methodology is to pre-process the image in order to apply the proposed steganography algorithms. This pre-process stage divides the image into '*X*' number of non-overlapped pixels blocks to compute the various features, e.g. identification of high and low texture areas, correlation of neighboring pixels, pixel range levels, and pixels differences, etc. These above features considered as the essential part of our proposed algorithms. For example, identification of image regions i.e. high and low textures has its own significance with respect to concealment of a secret data size. Generally, a human eye has more ability to perceive the changes in the smooth regions instead of high texture based regions. For better understanding, we present the basic pre-processing phase in graphical representation see Figure 3.3, where it identifies the edge and smooth texture areas of 'Lena' image. This identification is based on the simple threshold value (i.e. 32

between two pixels). The higher texture region of 'Lena' image is highlighted with the green blocks and rest of image area is depicted more relevant to smooth regions. The embedding processes of proposed methods differently treat/handle these both regions. Because the higher texture regions have more ability to modify pixels without noticeable effects, indirectly conceal more secret data instead of smooth regions.

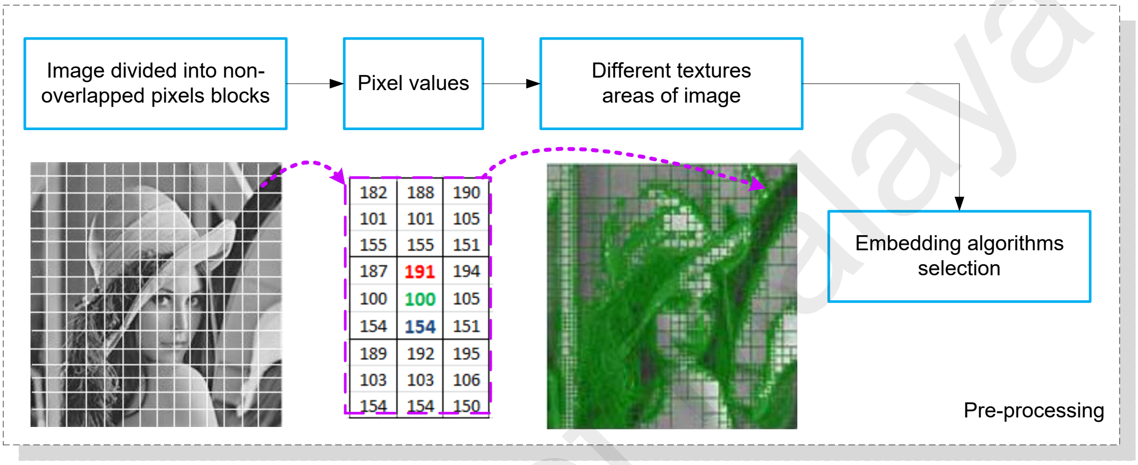


Image divided into non-overlapped pixels blocks
Pixel values
Different textures areas of image
Embedding algorithms selection
Pre-processing

182	188	190
101	101	105
155	155	151
187	191	194
100	100	105
154	154	151
189	192	195
103	103	106
154	154	150

Figure 3.3: Embedding Pre-processing Phase of Cover-image

Therefore, based on above computed features, the output of pre-processing phase decides the embedding algorithms or some internal steps of selected algorithm. This pre-processing stage is bounded with each proposed steganography algorithm and briefly discussed in Chapters 4 and 5. Meanwhile, these pre-processing steps, i.e. '*X*' size and other employed features must be synchronized with the extraction phase of proposed techniques. Generally, this type of extra information becomes the part of stego-key.

(b) ***Embedding Algorithm Phase***

The embedding phase is one of the most important phases of the proposed research methodology because this employs the actual embedding algorithm/procedure for secret data embedding. Differences in embedding procedures lie in the process of embedding that can be seen when the complete embedding procedure is carried out. Additionally, the embedding capacity, visual quality, and security of stego-images are depended on its embedding process. In this study, we proposed two singular (RMDR, PBPVD) and two hybrids (RMDR+PBPVD) steganography techniques to achieve the research objectives. Furthermore, the core proposed steganography algorithms discussed in Chapter 4 and 5. The selection of respective proposed embedding algorithm based on the previous pre-processing stage of this methodology. The next section discusses the post-processing stage of methodology.

(c) ***Embedding Post-Processing***

Once the embedding algorithm phase completed for a certain number of pixels in a block, the resultant stego-pixels are generated. Meanwhile, this embedding algorithm phase repeated for rest of the cover image to generate the complete stego-image. Furthermore, post-processing phase verifies the embedded secret data by recovering and comparing it from stego-image. Finally, the stego-image and its respective stego-key are considered as the output of this methodology as shown in Figure 3.2.

3.3.2.2 Extracting Phase of Steganography Method

In this section, we present the extracting methodology of proposed steganography techniques under the phase II as showed in Figure 3.1. This also consists of input, pre-processing, extracting algorithm and output stages as illustrated in Figure 3.4. The input stage requires the stego-image (and stego-key) for pre-processing and extracting process as shown in Figure 3.4. The detail as follows.

(a) ***Extracting Pre-Processing***

Similar to embedding pre-processing phase, it divides the image into *'X'* number of non-overlapped pixels blocks. This computes the features that employed in embedding pre-processing phase (Section 3.3.2.1). Furthermore, it decides the extracting technique or some specific steps of proposed extracting algorithm to deal the stego-image for the extraction process of secret data.

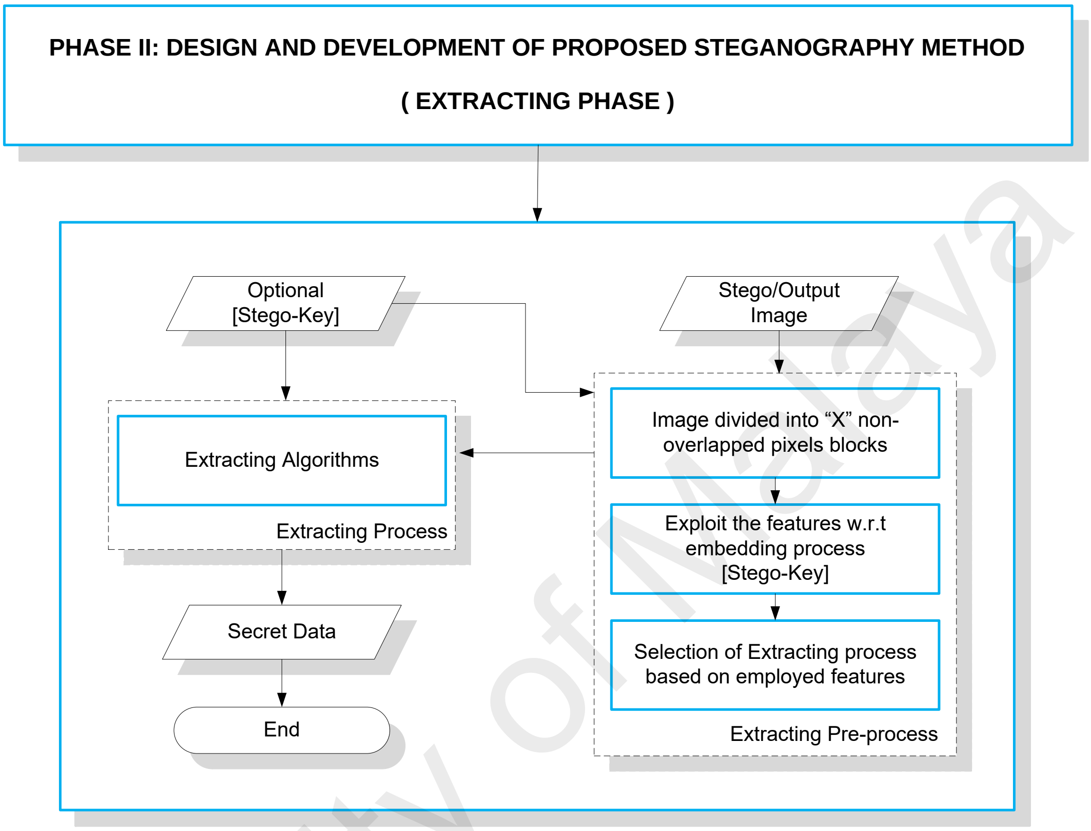

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EXTRACTING PHASE)
Optional [Stego-Key]
Stego/Output Image
Image divided into "X" non-overlapped pixels blocks
Extracting Algorithms
Extracting Process
Exploit the features w.r.t embedding process [Stego-Key]
Secret Data
Selection of Extracting process based on employed features
End
Extracting Pre-process

Figure 3.4: Steganography Extracting Phase in Research Methodology

(b) ***Extracting Algorithm Phase***

This phase is the counterpart of its respective embedding algorithm and has its own significance to complete the steganography process. Once the pre-processing steps successfully performed on stego-image, the selected extracting algorithm employed to recover the secret data. The detail of selected extracting algorithms based on pre-processing phase discussed in proposed methods of Chapter 4 and 5.

3.3.3 Phase III: Performance Evaluation of Proposed Steganography Methods

Phase III of research methodology consists of three categories, embedding capacity, visual quality and security evaluation measures (Figure 3.5). In this section, the proposed steganography algorithms performances evaluated using above measures. Furthermore, the exact metrics used in the evaluation process showed in Figure 3.5 and its detail discussed in Chapter 2.

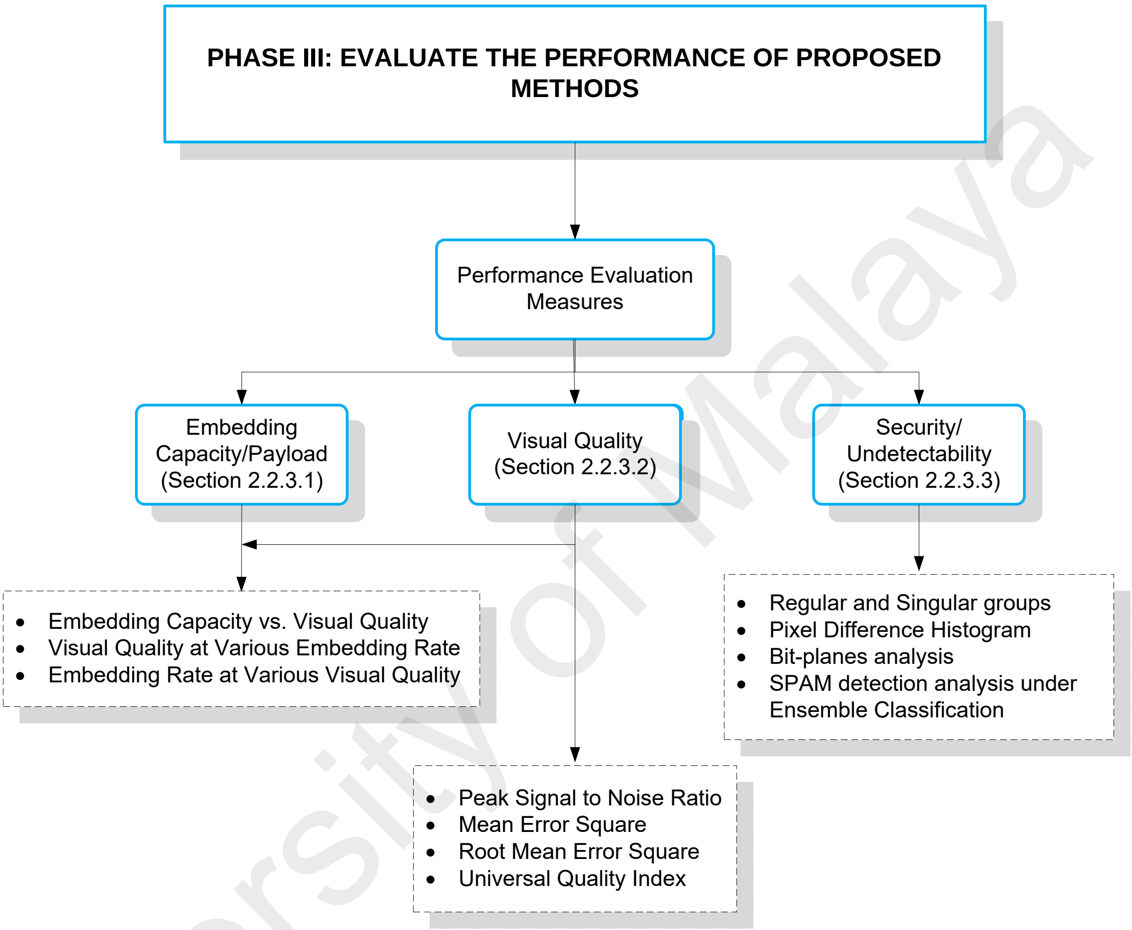

PHASE III: EVALUATE THE PERFORMANCE OF PROPOSED METHODS
Performance Evaluation Measures
Embedding Capacity/Payload (Section 2.2.3.1)
Visual Quality (Section 2.2.3.2)
Security/ Undetectability (Section 2.2.3.3)
Embedding Capacity vs. Visual Quality
Visual Quality at Various Embedding Rate
Embedding Rate at Various Visual Quality
Regular and Singular groups
Pixel Difference Histogram
Bit-planes analysis
SPAM detection analysis under Ensemble Classification
Peak Signal to Noise Ratio
Mean Error Square
Root Mean Error Square
Universal Quality Index

Figure 3.5: Performance Evaluation Matrices for Proposed Methodology

3.4 General Mathematical Modeling of Proposed Methods

In this section, we present the general mathematical modeling of proposed steganography techniques. This modeling is divided into two phases, namely embedding and extracting modeling. The embedding mathematical modeled functions represented as below.

$$R \quad = \alpha\ (C) \tag{3.1}$$

$$M' = \beta\ (M) \tag{3.2}$$

$$S = \gamma\ (R,\ C,\ M') \tag{3.3}$$

Suppose *M*, *C* denoted as a secret message and cover image, respectively. R. represents the internal strategies of the proposed steganography techniques (e.g. range levels, threshold, block size etc.) The resultant stego-image represented by *S*. Three functions *α, β*, and γ are used in the embedding process to compute the *R, M'* and *S*. The function *α* is used to decide the internal strategy of proposed steganography technique, where *C* and *R* represent the input and output parameters, respectively. Similarly, the function *β* represents the encryption or compression strategy of proposed embedding techniques, where the *M*, *M'* are the input and output parameters, respectively. However, the usage of function *β* is optional in proposed steganography techniques. Finally, the function *γ* takes *R*, *C*, and *M'* as input and return the proposed *S*. The function *γ* is the proposed embedding technique. The exact embedding techniques discussed in Chapter 4 and Chapter 5.

The extracting mathematical modeled functions represented as below.

$$R' \ = \alpha\ (S) \tag{3.4}$$

$$M' = \gamma'\ (R',\ S) \tag{3.5}$$

$$M \ = \beta\ (M') \tag{3.6}$$

In the above extracting modeling, the *R'* represents the internal strategy of proposed extracting technique. The function *α* is used to decide the internal strategy of extracting process (e.g. range levels, threshold, block size etc.), where the *S* and *R'* represents the input and output parameters. The inverse function of *γ* is represented as *γ'*, where it is the extracting procedure of proposed steganography technique. The γ' function takes *R'*, and *S* as input and returns the *M'*. Furthermore, function *β* is optional in proposed steganography techniques, where it represents the inverse encrypted and decompressed strategy of proposed steganography technique. This function β takes the *M'* as input and return the *M* as the core secret message.

3.5 Chapter Summary

In this chapter, the research methodology presented which used in the design and implementation of proposed image steganography algorithms. However, the detail of each contribution briefly explained in Chapter 4 and 5, respectively.

CHAPTER 4: RIGHT MOST DIGIT REPLACEMENT (RMDR) AND RMDR ADAPTIVE HYBRID METHODS

In this chapter, we initiate our research investigations into spatial domain image based steganography by developing and testing techniques that manipulate the efficient digit substitution to minimize the cover and stego-pixels differences problem. The main objectives are to improve the visual quality, maximize the security against structural and statistical steganalysis while retaining the high embedding capacity of stego-images.

This chapter proposes the two singular and hybrid steganography techniques, respectively. First, a substitution based embedding method presented namely right most digit replacement (RMDR). This improves the visual quality and undetectability compared to most common singular steganography approaches i.e. LSB, PVD, adaptive LSB, and LSB-module three (Chan & Cheng, 2004; D.-C. Wu & Tsai, 2003; Xu et al., 2016; H. Yang et al., 2009). The basic advantage of RMDR technique is to substitute the digits instead of bits that indirectly improve the ability of security with respect to well-known RS (Jessica Fridrich et al., 2001) and modern machine learning (Pevny et al., 2010) based steganalysis detection attacks. In addition, this technique employs the similar/closest stego-pixel selection process that enhances the visual quality while retains the highest rate of embedding capacity as prove in the experimental section.

Another method presents a hybrid steganography technique that combines/integrates the RMDR with traditional adaptive LSB method in efficient manners. The proposed hybrid technique is simple and effective in order to achieve the general steganography objectives as compared to existing LSB-based hybrid embedding approaches i.e. (M Khodaei & Faez, 2012; H-C Wu et al., 2005; K. Wu et al., 2015; C.-H. Yang, Weng, Wang, & Sun, 2010). This RMDR-hybrid method exploits the basic texture characteristics of an image for embedding purpose. We shall demonstrate that adaptive

RMDR-hybrid technique does meet the stated objectives on visual imperceptibility, capacity and security.

This chapter organized into four sections. Sections 4.1 and 4.2 present the RMDR and hybrid RMDR steganography techniques. Section 4.3 presents the achieved objectives, results and discussion. Finally, Section 4.4 discusses the concluding remarks.

4.1 Right Most Digit Replacement Steganography Method

The proposed substitution based method known as right most digit replacement (RMDR) provides a novel steganographic mechanism for concealing of secret data. As already discussed, the basic notion of the RMDR embedding method is to substitute the digit of a pixel value with secret data instead of bit substitution (inspired by the LSB replacement methods). The architectural process of proposed RMDR embedding technique (Figure 4.1) is based on the phase II (design and implement) of proposed research methodology as discussed in section 3.3.2.1 (Figure 3.2). Meanwhile, the current proposed RMDR embedding method (section 4.1.1) consists of three sequential sub-phases pre-processing, the core RMDR algorithm and post processing. Similarly, the RMDR extracting also follows steganography extracting phase of research methodology including pre-processing, extracting and post-processing (see Figure 3.4). The RMDR embedding and extracting processes are briefly discussed in section (4.1.1) and (4.2.1), respectively.

4.1.1 RMDR Embedding Method

The RMDR embedding procedure i.e. pre-processing, core embedding technique and post-processing phases are shown in Figure 4.1 and in depth, discussion is as follows.

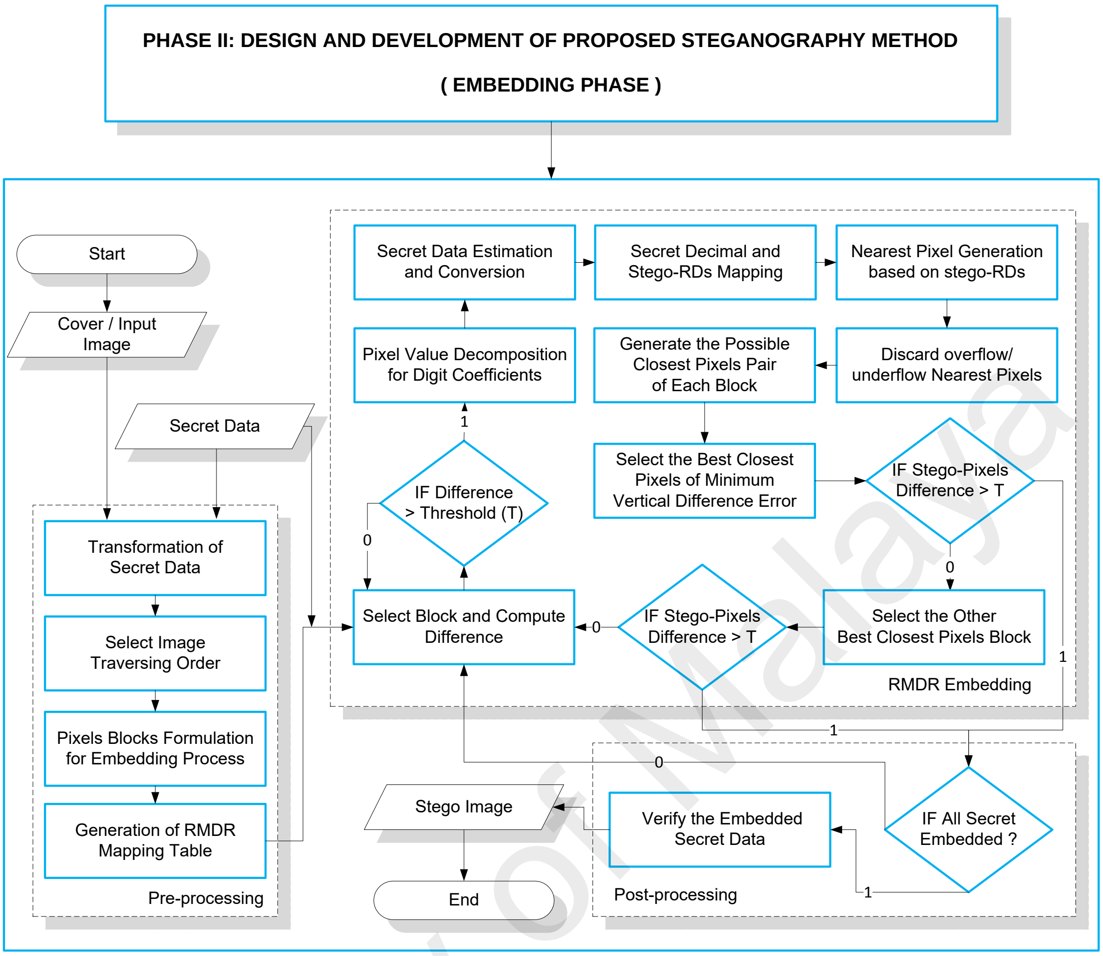

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EMBEDDING PHASE)
Start
Cover / Input Image
Secret Data
Transformation of Secret Data
Select Image Traversing Order
Pixels Blocks Formulation for Embedding Process
Generation of RMDR Mapping Table
Pre-processing
Secret Data Estimation and Conversion
Secret Decimal and Stego-RDs Mapping
Nearest Pixel Generation based on stego-RDs
Pixel Value Decomposition for Digit Coefficients
Generate the Possible Closest Pixels Pair of Each Block
Discard overflow/ underflow Nearest Pixels
IF Difference > Threshold (T)
Select the Best Closest Pixels of Minimum Vertical Difference Error
IF Stego-Pixels Difference > T
Select Block and Compute Difference
IF Stego-Pixels Difference > T
Select the Other Best Closest Pixels Block
RMDR Embedding
1
0
Stego Image
End
Verify the Embedded Secret Data
IF All Secret Embedded ?
Post-processing

Figure 4.1: The Basic Flow Diagram of RMDR Embedding

(a) *Pre-processing of RMDR Embedding Method*

According to flow diagram of RMDR embedding (Figure 4.1), prior to *pre-processing* phase, a cover image and secret data are required for further operation. This pre-processing phase consists of sub-stages, first transformation of secret data, second selecting the image traversing order, next pixels division into number of blocks and finally the generation of RMDR mapping table. The output of this stage would be the selected pixels group/block that will be employed by the core RMDR embedding process.

i Transformation of Secret Data

In secret data transforming stage, various embedding methods convert the secret data before employing the embedding procedure (Muhammad et al., 2015) . One possibility is to encrypt and compress the secret data to enhance the security and reduce the secret data size. However, all these above overhead techniques require extra computation and extra logging to maintain the process of secret data transformation, because this logging will be used as inverse transformation of secret data at extracting phase. However, this encryption and compression stages are optional and can be applied depending on the requirement of applications. In this study, the focus is to embed the plain binary secret bit stream instead of any other format.

ii Image Traversing Order

Image traversing order is basically used to choose the embedding order of cover pixels for secret data concealment. Generally, this traversing order improves the secrecy and embedding efficiency of steganography algorithms. Recently, researchers employed Hilbert (Zhao & Luo, 2012), Moore space filling curves (Amirtharajan & Rayappan, 2009) and Hamiltonian graph (Iranpour, 2013) traversing orders before employing the core embedding process. However, our proposed method is flexible where any of the above traversing orders can be employed before the embedding process. However, to avoid the biasness in performance evaluation, we followed the similar conventional zig-zag traversing order like the other compared schemes used to evaluate its performances. The detail is discussed in core RMDR embedding procedure.

iii Pixels Blocks Formulation for Embedding Process

In this phase, cover image is divided into M x N non-overlapped pixels blocks, currently assuming M=2 and N=1. The RMDR embedding efficiently utilizes the correlation of *M x N* block pixels for its closest selection process in order to achieve the optimized stego-pixels.

iv RMDR Mapping Table Generation

The core of RMDR embedding process requires a mapping table, which generates the possible closest digits with respect to cover pixels. This mapping table is briefly discussed in section 4.1.1 (b (iv)).

(b) ***RMDR Embedding***

In this phase, the core RMDR embedding process is employed. The RMDR concept is to substitute the secret data using closest and efficient digits replacement. Therefore, this embedding mechanism requires some certain stages as shown in Figure 4.1 are discussed below. Meanwhile, the complete/core RMDR embedding process steps in tabular form is presented in the end of this section (Table 4.3).

i Selection of Block

The first stage is to select the pixels block for embedding process (see Figure 4.1). The selection of block is dependent on its pixels difference value d. For example, $d = |p_0 - p_1|$, where p_0 and p_1 are denoted as pixels of a block. This difference must satisfy the threshold T value, where the T can be random value with satisfying the T ϵ [0, 255] range. The purpose of T is to utilize the RMDR embedding in adaptive manners and improve the secrecy at lower embedding rate. The additional detail and usage of T threshold can be seen in the embedding algorithm steps (Table 4.3).

ii Pixel Value Decomposition for Digit Coefficients

As mentioned earlier the notion of RMDR embedding method is based on pixel digits substitution. Therefore, the pixel digit decomposition is required, where, a pixel p intensity/value decomposes into following coefficients, left digit (D_l), middle digit (D_m), and right digit (D_r), as described equation 4.1

$$p = (100 \times D_l + 10 \times D_m + 1 \times D_r) \tag{4.1}$$

$$e.g. \quad 238 = (100 \times 2 + 10 \times 3 + 1 \times 8)$$

For example, a pixel $p \in$ [0, 255] range with the value of 238 and its respective values for D_l, D_m, and D_r are 2, 3, and 8 (Figure 4.2). If a pixel value consists of only one/two coefficient(s), then a leading zero(s) is added to employ D_l and D_m, i.e., p = 38, where D_l is 0, and D_m and D_r are 3 and 8, respectively. Similarly, for p = 8, D_l and D_m are 0 and D_r is 8.

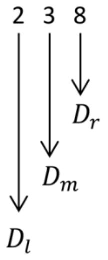


Figure 4.2: Pixel Value Digit Coefficients

iii Secret Data Estimation and Conversion

This step is supposed to choose the number of secret bits from the secret message buffer and further converts or transform into its respective equivalent decimal values. For better understanding, assume 6 secret bits are $(011\ 101)_2$ and its two sets of 3 bit equivalent decimal values are $(3)_{10}$ and $(5)_{10}$, respectively. The term secret bits buffer denotes the secret data whether this can be transformed by any encryption/compression technique. However, for simplicity proposed scheme takes the plain text as mention in the pre-processing stage see section 4.1.1 (a).

iv RMDR Mapping Table Generation

Proposed system designs a RMDR mapping table as shown in Table 4.1. This RMDR mapping table actually provides the possible closest stego-RDs (equivalent of secret data) values against the cover pixel D_r. The above equivalent decimal values that mapped/replaced with the stego-digits are known as stego-RDs. The generation of RMDR mapping table for 3 bits per pixel embedding ratio is as follows.

Assume a 3-bit secret digit represents the 2^3 = 8 possible digits and digit range would be [0, 7]. Similarly, a pixel p of D_r range would be [0, 9]. For example, p = 239 and after applying equation 4.1, its D_r = 9. If we apply one to one mapping of 3-bit secret (2^3) digit range [0, 7] with the p of D_r [0, 9] range, as a result p of D_r range has two extra digits [8, 9] that can further be reused with 2^3 secret data digit range, i.e., [3, 4]. These two extra digits minimize the difference of D_r between cover and stego-pixels. Moreover, these extra digits can be generated by adapting the frequency of D_r coefficient from the cover image. For better understanding, Table 4.1 shows the RMDR embedding table of Stego-RD, where $(b_i \mid b_{i+1})$ are the digit value of selected secret bits for ith block. The $\mathrm{S}_0(b_i \mid b_{i+1})$ or $\mathrm{S}_1(b_i \mid b_{i+1})$ are denoted as the equivalent Stego-RD based on $(b_i \mid b_{i+1})$.

Table 4.1: RMDR Embedding Table for Stego-RDs

Secret decimal	$\boldsymbol{b_i \mid b_{i+1}}$	0	1	2	3	4	5	6	7
Stego-RD	$\boldsymbol{S_{0(bi \mid bi+1)}}$	*	*	*	*	*	*	*	*
	$\boldsymbol{S_{1(bi \mid bi+1)}}$	-1	-1	-1	8	9	-1	-1	-1

* *The resultant stego-RD $S_{0(bi)}$ is replaced by respective b_i and $S_{0(bi+1)}$ is replaced by respective b_{i+1} value.*

v Secret Decimal and Stego-RDs Mapping

After secret data estimation, conversion and generation of RMDR mapping table, next phase is to find or locate the equivalent stego-RD against its secret decimal denoted as b from Table 4.1. The output of this stage is to compute the least digit of stego-pixels that known as stego-RD. For example, a secret decimal denoted as b_i = 3. Therefore, after employing the RMDR mapping there would be two stego-RDs denoted as S_0 (3) = '3' and S_1 (3) = '8'.

vi Nearest Pixel Generation based on Stego-RDs

This stage utilizes the stego-RDs to generate the three nearest pixels against each cover pixel of a block e.g. For $S_{0(b_i)}$ case, p_i can have three nearest pixels as high, medium and low denoted as (S_0p_{iL}, S_0p_{iM}, S_0p_{iH}). Similarly, for $S_{1(b_i)}$ case, p_i have again three nearest pixels as high, medium and low denoted as (S_1p_{iL}, S_1p_{iM}, S_1p_{iH}). The generations of these nearest pixels for p_i can be computed by equation 4.2.

$$\begin{aligned}
S_0p_{iL} &= NearestPixels\left(p_i - 10\ ,\ S_{0(b_i)}\right)\\
S_0p_{iM} &= NearestPixels\left(p_i\ ,\ S_{0(b_i)}\right)\\
S_0p_{iH} &= NearestPixels\left(p_i + 10\ ,\ S_{0(b_i)}\right)\\
\\
S_1p_{iL} &= NearestPixels\left(p_i - 10\ ,S_{1(b_i)}\ \right)\\
S_1p_{iM} &= NearestPixels\left(p_i\ ,S_{1(b_i)}\right)\\
S_1p_{iH} &= NearestPixels\left(p_i + 10\ ,S_{1(b_i)}\ \right)
\end{aligned} \tag{4.2}$$

$$NearestPixels(param1\ ,param2) = \left(\left(floor\left(\frac{param1}{10}\right) \times 10\right) +\ param2\right)$$

Where NearestPixels is the function with two input parameters, i.e. param1 and param2. The p_i denotes the pixel value. Furthermore, the $S_{0(b_i)}$, $S_{1(b_i)}$ values are generated by Table 4.1 against its respective b_i (secret decimal). Finally, to maintain the embedding of secret data, each nearest pixel i.e. (S_0p_{iL}, S_0p_{iM}, S_0p_{iH}) and (S_1p_{iL}, S_1p_{iM}, S_1p_{iH}) D_r value should be equivalent/satisfied the respective stego-RD. Similarly, this step is repeated to generate the next nearest pixels for p_{i+1} cover pixel. Therefore, the p_{i+1} will have the nearest pixels as (S_0p_{i+1L}, S_0p_{i+1M}, S_0p_{i+1H}) and (S_1p_{i+1L}, S_1p_{i+1M}, S_1p_{i+1H}) against respective $S_{0(b_{i+1})}$ and $S_{1(b_{i+1})}$.

vii Discarding Overflow/Underflow of Nearest Pixels

In this stage, proposed algorithm discards the overflow/underflow of nearest pixels values that exists beyond the ±10 of cover pixels range. The purpose is to reduce the possible combination that will be employed in next step which increases the chances of selecting the best closest stego-pixels against cover pixels for high imperceptibility.

viii Generation of Possible Closest Pixels Pair of Each Block

After discarding the overflow/underflow nearest high, medium and low pixels, this stage will generates the all possible combination of remaining nearest pixels for p_i and p_{i+1} for stego-pixel block. The possible combinations of each block are generated as '*ClosestBlk'* array that are shown in Table 4.2. Where the Table 4.2 represents the nearest (S_0p_{iL}, S_0p_{iM}, S_0p_{iH}) and (S_1p_{iL}, S_1p_{iM}, S_1p_{iH}) pixels that belongs to p_i. Similarly, the nearest of p_{i+1} are (S_0p_{i+1L}, S_0p_{i+1M}, S_0p_{i+1H}) and (S_1p_{i+1L}, S_1p_{i+1M}, S_1p_{i+1H}).

Table 4.2: The Possible Combination of Closest Stego-pixels Blocks from *Closestblk*$_f$ array, where $f \in [1, 36]$.

ClosestBlk1	=(S_0p_{iL},S_0p_{i+1L}),	*ClosestBlk2*	=(S_0p_{iL}, S_0p_{i+1M}),	*ClosestBlk3*	=(S_0p_{iL}, S_0p_{i+1H})
ClosestBlk4	=(S_0p_{iL}, S_1p_{i+1L}),	*ClosestBlk5*	=(S_0p_{iL},S_1p_{i+1M}),	*ClosestBlk6*	=(S_0p_{iL}, S_1p_{i+1H})
ClosestBlk7	=(S_0p_{iM}, S_0p_{i+1L}),	*ClosestBlk8*	=(S_0p_{iM}, S_0p_{i+1M}),	*ClosestBlk9*	=(S_0p_{iM}, S_0p_{i+1H})
ClosestBlk10	=(S_0p_{iM}, S_1p_{i+1L}),	*ClosestBlk11*	=(S_0p_{iM}, S_1p_{i+1M}),	*ClosestBlk12*	=(S_0p_{iM}, S_1p_{i+1H})
ClosestBlk13	=(S_0p_{iH}, S_0p_{i+1L}),	*ClosestBlk14*	=(S_0p_{iH}, S_0p_{i+1M}),	*ClosestBlk15*	=(S_0p_{iH}, S_0p_{i+1H})
ClosestBlk16	=(S_0p_{iH}, S_1p_{i+1L}),	*ClosestBlk17*	=(S_0p_{iH}, S_1p_{i+1M}),	*ClosestBlk18*	=(S_0p_{iH}, S_1p_{i+1H})
ClosestBlk19	=(S_1p_{iL},S_0p_{i+1L}),	*ClosestBlk20*	=(S_1p_{iL}, S_0p_{i+1M}),	*ClosestBlk21*	= (S_1p_{iL}, S_0p_{i+1H})
ClosestBlk22	=(S_1p_{iL}, S_1p_{i+1L}),	*ClosestBlk23*	=(S_1p_{iL}, S_1p_{i+1M}),	*ClosestBlk24*	= (S_1p_{iL}, S_1p_{i+1H})
ClosestBlk25	=(S_1p_{iM}, S_0p_{i+1L}),	*ClosestBlk26*	=(S_1p_{iM}, S_0p_{i+1M}),	*ClosestBlk27*	=(S_1p_{iM}, S_0p_{i+1H})
ClosestBlk28	=(S_1p_{iM}, S_1p_{i+1L}),	*ClosestBlk29*	=(S_1p_{iM}, S_1p_{i+1M}),	*ClosestBlk30*	=(S_1p_{iM}, S_1p_{i+1H})
ClosestBlk31	=(S_1p_{iH}, S_0p_{i+1L}),	*ClosestBlk32*	=(S_1p_{iH}, S_0p_{i+1M}),	*ClosestBlk33*	=(S_1p_{iH}, S_0p_{i+1H})
ClosestBlk34	=(S_1p_{iH} , S_1p_{i+1L}),	*ClosestBlk35*	=(S_1p_{iH}, S_1p_{i+1M}),	*ClosestBlk36*	=(S_1p_{iH}, S_1p_{i+1H})

ix Selection of Best Closest Pixels

In this stage, proposed algorithm chooses the best closest pixels (for stego) block against its respective cover-block. The selection of the best closest pixels depends on the minimum vertical difference error from equation 4.3.

$$(p'_i, p'_{i+1}) = ClosestBlk_{(\text{Min}\,(\,dV'_f))} \tag{4.3}$$

Where the (p'_i, p'_{i+1}) are the selected stego-pixels of a block by computing the $_{\text{Min}\,(\,dV'_f)}$ minimum of vertical difference block from possible combinations of *ClosestBlk*$_f$ block pairs by

$$dV'_f = (\,|\,ClosestBlk_f\,(arg1) - p_i| + |\,ClosestBlk_f\,(arg2) - p_{i+1}|\,)$$

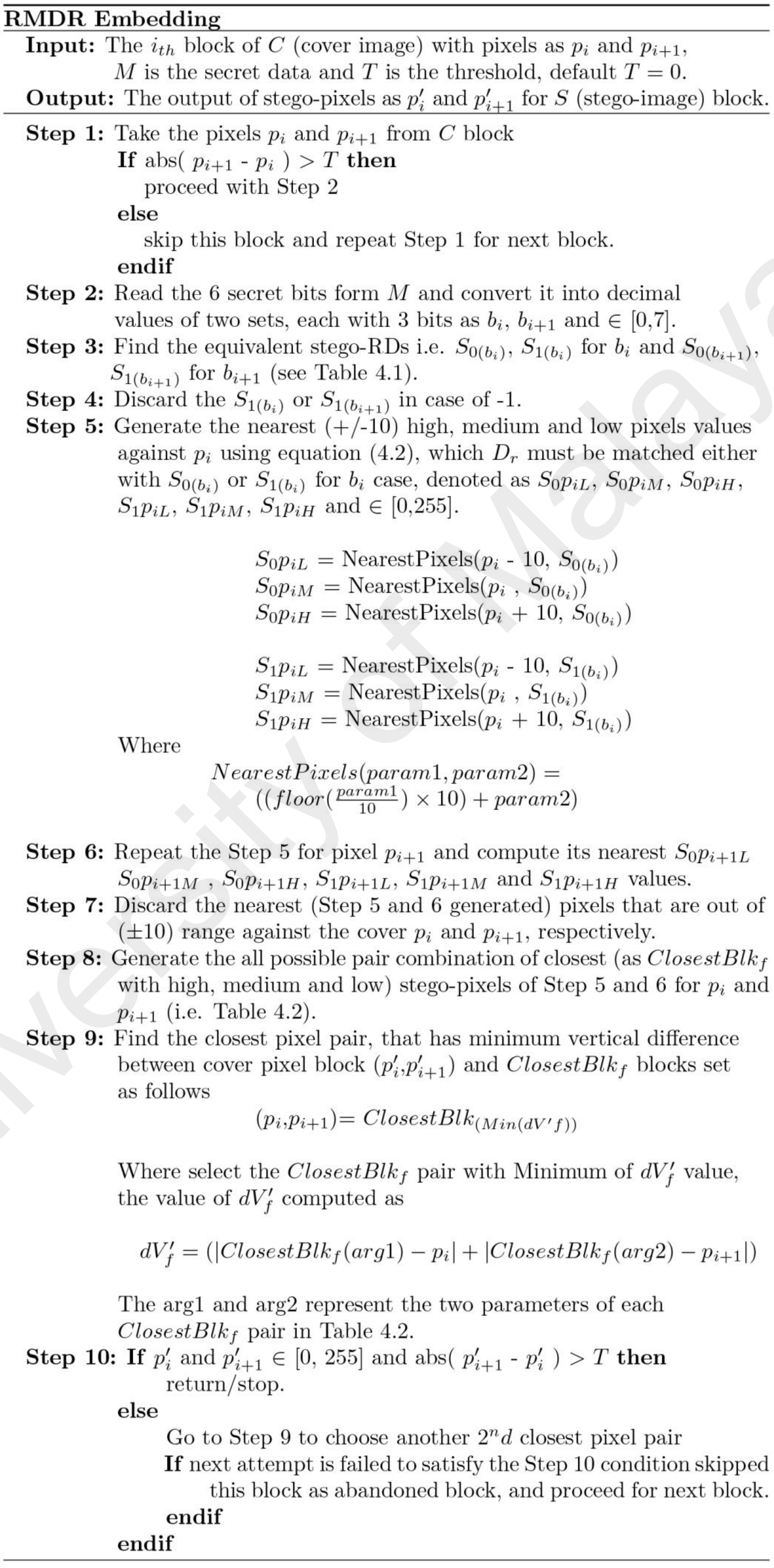
Where the dV'_f denotes the difference between cover pixels and *ClosestBlk* pixels at *f* index, the p_i, p_{i+1} are the cover pixels, *arg1*, *arg2* are pixel pair values of $ClosestBlk_f$ block array.

Finally, the proposed RMDR embedding verifies the range level [0, 255] and computes the difference between proposed stego-pixels. If the difference is greater than T threshold then the RMDR embedding will proceed with next embedding block. Otherwise, choose the 2nd, 3rd until the last best closest block from *ClosestBlk*$_{\text{f}}$ array which satisfy the threshold condition. If the stego-pixels block is failed to satisfy the T threshold and range levels conditions, this considered as a skipped/abandoned block. The embedded secret data inside the skipped block are re-embedded into the next selected block. The concept of introducing the skipped block increases the embedding efficiency and visual quality of stego-image, because through experiments, we found that most of the skipped blocks were from smooth regions when the T value was set as highest value. Therefore, during embedding process, skipping of those blocks that belongs to smooth regions may produce less distortion in stego-images.

(c) *Post-processing of RMDR Embedding Method*

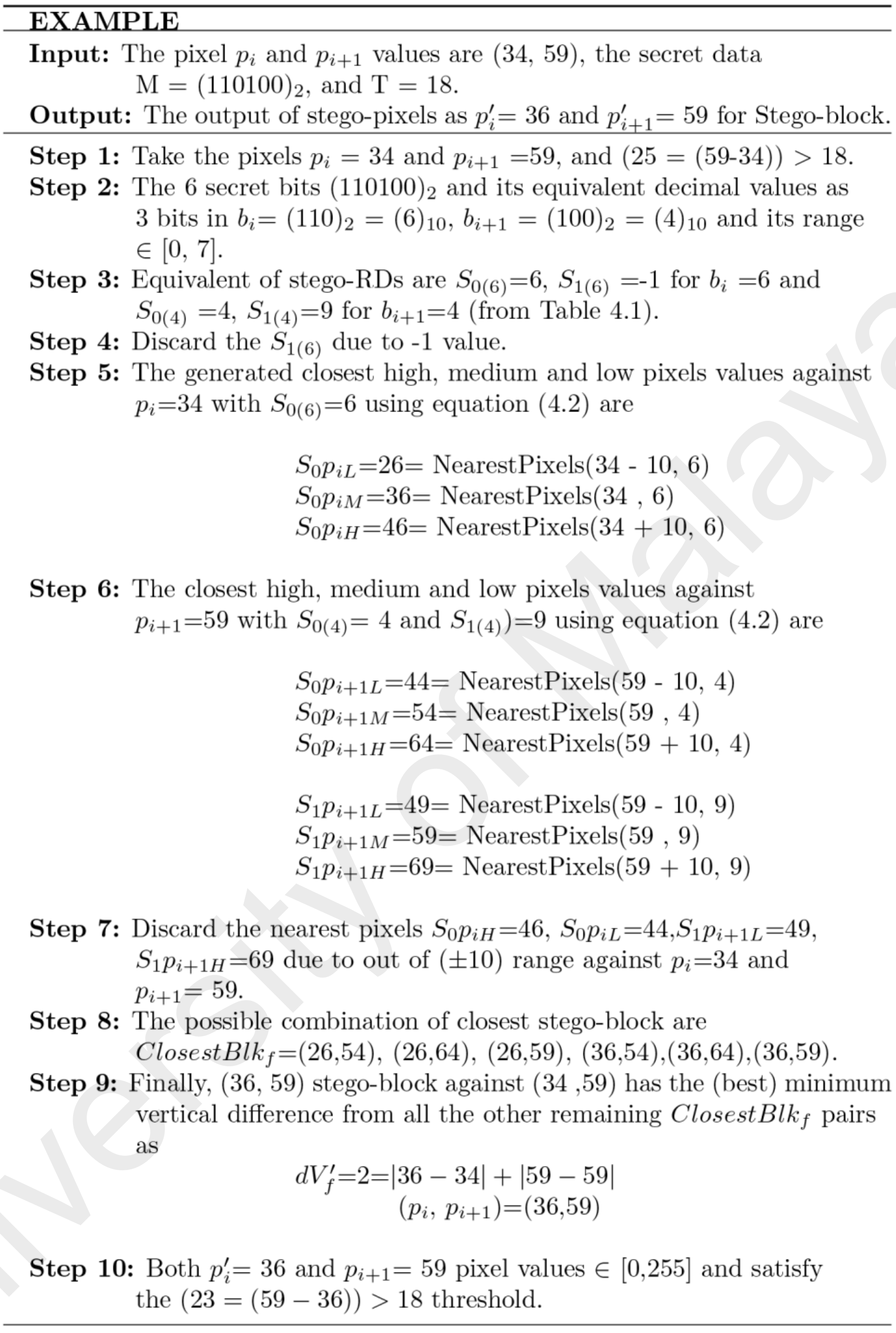
In post-processing stage of RMDR embedding, if the secret data or image blocks are remaining to embed, this will repeat the RMDR embedding phase for next secret data or next cover pixels block. Once the all secret data is embedded into the stego-image, it verifies the integrity of secret data. This verification process can be applied by employing the extraction algorithm as stated in next section 4.1.2. Furthermore, the complete proposed RMDR embedding algorithm steps and its example is defined in Table 4.3.

Table 4.3: RMDR Embedding Steps and Example



```
RMDR Embedding
  Input: The $i_{th}$ block of $C$ (cover image) with pixels as $p_i$ and $p_{i+1}$,
         $M$ is the secret data and $T$ is the threshold, default $T = 0$.
  Output: The output of stego-pixels as $p'_i$ and $p'_{i+1}$ for $S$ (stego-image) block.

  Step 1: Take the pixels $p_i$ and $p_{i+1}$ from $C$ block
          If abs( $p_{i+1}$ - $p_i$ ) $>$ $T$ then
             proceed with Step 2
          else
             skip this block and repeat Step 1 for next block.
          endif
  Step 2: Read the 6 secret bits form $M$ and convert it into decimal
          values of two sets, each with 3 bits as $b_i$, $b_{i+1}$ and $\in$ [0,7].
  Step 3: Find the equivalent stego-RDs i.e. $S_{0(b_i)}$, $S_{1(b_i)}$ for $b_i$ and $S_{0(b_{i+1})}$,
          $S_{1(b_{i+1})}$ for $b_{i+1}$ (see Table 4.1).
  Step 4: Discard the $S_{1(b_i)}$ or $S_{1(b_{i+1})}$ in case of -1.
  Step 5: Generate the nearest (+/-10) high, medium and low pixels values
          against $p_i$ using equation (4.2), which $D_r$ must be matched either
          with $S_{0(b_i)}$ or $S_{1(b_i)}$ for $b_i$ case, denoted as $S_0p_{iL}$, $S_0p_{iM}$, $S_0p_{iH}$,
          $S_1p_{iL}$, $S_1p_{iM}$, $S_1p_{iH}$ and $\in$ [0,255].

                   $S_0p_{iL}$ = NearestPixels($p_i$ - 10, $S_{0(b_i)}$)
                   $S_0p_{iM}$ = NearestPixels($p_i$ , $S_{0(b_i)}$)
                   $S_0p_{iH}$ = NearestPixels($p_i$ + 10, $S_{0(b_i)}$)

                   $S_1p_{iL}$ = NearestPixels($p_i$ - 10, $S_{1(b_i)}$)
                   $S_1p_{iM}$ = NearestPixels($p_i$ , $S_{1(b_i)}$)
                   $S_1p_{iH}$ = NearestPixels($p_i$ + 10, $S_{1(b_i)}$)
          Where
               $NearestPixels(param1, param2) =$
                   $((floor(\frac{param1}{10}) \times 10) + param2)$

  Step 6: Repeat the Step 5 for pixel $p_{i+1}$ and compute its nearest $S_0p_{i+1L}$
          $S_0p_{i+1M}$ , $S_0p_{i+1H}$, $S_1p_{i+1L}$, $S_1p_{i+1M}$ and $S_1p_{i+1H}$ values.
  Step 7: Discard the nearest (Step 5 and 6 generated) pixels that are out of
          ($\pm$10) range against the cover $p_i$ and $p_{i+1}$, respectively.
  Step 8: Generate the all possible pair combination of closest (as $ClosestBlk_f$
          with high, medium and low) stego-pixels of Step 5 and 6 for $p_i$ and
          $p_{i+1}$ (i.e. Table 4.2).
  Step 9: Find the closest pixel pair, that has minimum vertical difference
          between cover pixel block ($p'_i$,$p'_{i+1}$) and $ClosestBlk_f$ blocks set
          as follows
                   ($p_i$,$p_{i+1}$)= $ClosestBlk_{(Min(dV'f))}$

          Where select the $ClosestBlk_f$ pair with Minimum of $dV'_f$ value,
          the value of $dV'_f$ computed as

            $dV'_f = (|ClosestBlk_f(arg1) - p_i| + |ClosestBlk_f(arg2) - p_{i+1}|)$

          The arg1 and arg2 represent the two parameters of each
          $ClosestBlk_f$ pair in Table 4.2.
  Step 10: If $p'_i$ and $p'_{i+1}$ $\in$ [0, 255] and abs( $p'_{i+1}$ - $p'_i$ ) $>$ $T$ then
              return/stop.
           else
              Go to Step 9 to choose another $2^nd$ closest pixel pair
              If next attempt is failed to satisfy the Step 10 condition skipped
                  this block as abandoned block, and proceed for next block.
              endif
           endif
```

Table 4.3, Continued.



EXAMPLE

Input: The pixel p_i and p_{i+1} values are (34, 59), the secret data
M = $(110100)_2$, and T = 18.

Output: The output of stego-pixels as p'_i= 36 and p'_{i+1}= 59 for Stego-block.

Step 1: Take the pixels p_i = 34 and p_{i+1} =59, and (25 = (59-34)) > 18.

Step 2: The 6 secret bits $(110100)_2$ and its equivalent decimal values as 3 bits in b_i= $(110)_2$ = $(6)_{10}$, b_{i+1} = $(100)_2$ = $(4)_{10}$ and its range $\in$ [0, 7].

Step 3: Equivalent of stego-RDs are $S_{0(6)}$=6, $S_{1(6)}$ =-1 for b_i =6 and $S_{0(4)}$ =4, $S_{1(4)}$=9 for b_{i+1}=4 (from Table 4.1).

Step 4: Discard the $S_{1(6)}$ due to -1 value.

Step 5: The generated closest high, medium and low pixels values against p_i=34 with $S_{0(6)}$=6 using equation (4.2) are

$$S_0p_{iL}=26= \text{NearestPixels}(34 - 10, 6)$$
$$S_0p_{iM}=36= \text{NearestPixels}(34 , 6)$$
$$S_0p_{iH}=46= \text{NearestPixels}(34 + 10, 6)$$

Step 6: The closest high, medium and low pixels values against p_{i+1}=59 with $S_{0(4)}$= 4 and $S_{1(4)}$)=9 using equation (4.2) are

$$S_0p_{i+1L}=44= \text{NearestPixels}(59 - 10, 4)$$
$$S_0p_{i+1M}=54= \text{NearestPixels}(59 , 4)$$
$$S_0p_{i+1H}=64= \text{NearestPixels}(59 + 10, 4)$$

$$S_1p_{i+1L}=49= \text{NearestPixels}(59 - 10, 9)$$
$$S_1p_{i+1M}=59= \text{NearestPixels}(59 , 9)$$
$$S_1p_{i+1H}=69= \text{NearestPixels}(59 + 10, 9)$$

Step 7: Discard the nearest pixels S_0p_{iH}=46, S_0p_{iL}=44,S_1p_{i+1L}=49, S_1p_{i+1H}=69 due to out of (±10) range against p_i=34 and p_{i+1}= 59.

Step 8: The possible combination of closest stego-block are $ClosestBlk_f$=(26,54), (26,64), (26,59), (36,54),(36,64),(36,59).

Step 9: Finally, (36, 59) stego-block against (34 ,59) has the (best) minimum vertical difference from all the other remaining $ClosestBlk_f$ pairs as

$$dV'_f=2=|36-34|+|59-59|$$
$$(p_i,\ p_{i+1})=(36,59)$$

Step 10: Both p'_i= 36 and p_{i+1}= 59 pixel values $\in$ [0,255] and satisfy the (23 = (59 − 36)) > 18 threshold.

Furthermore, for more clear view Figure 4.3 illustrates the example of RMDR. The selections of similar/closest stego-pixels of RMDR are compared with 3-bit LSB embedding method. The example shows that RMDR based stego-pixels have less difference error instead of LSB based substitution technique.

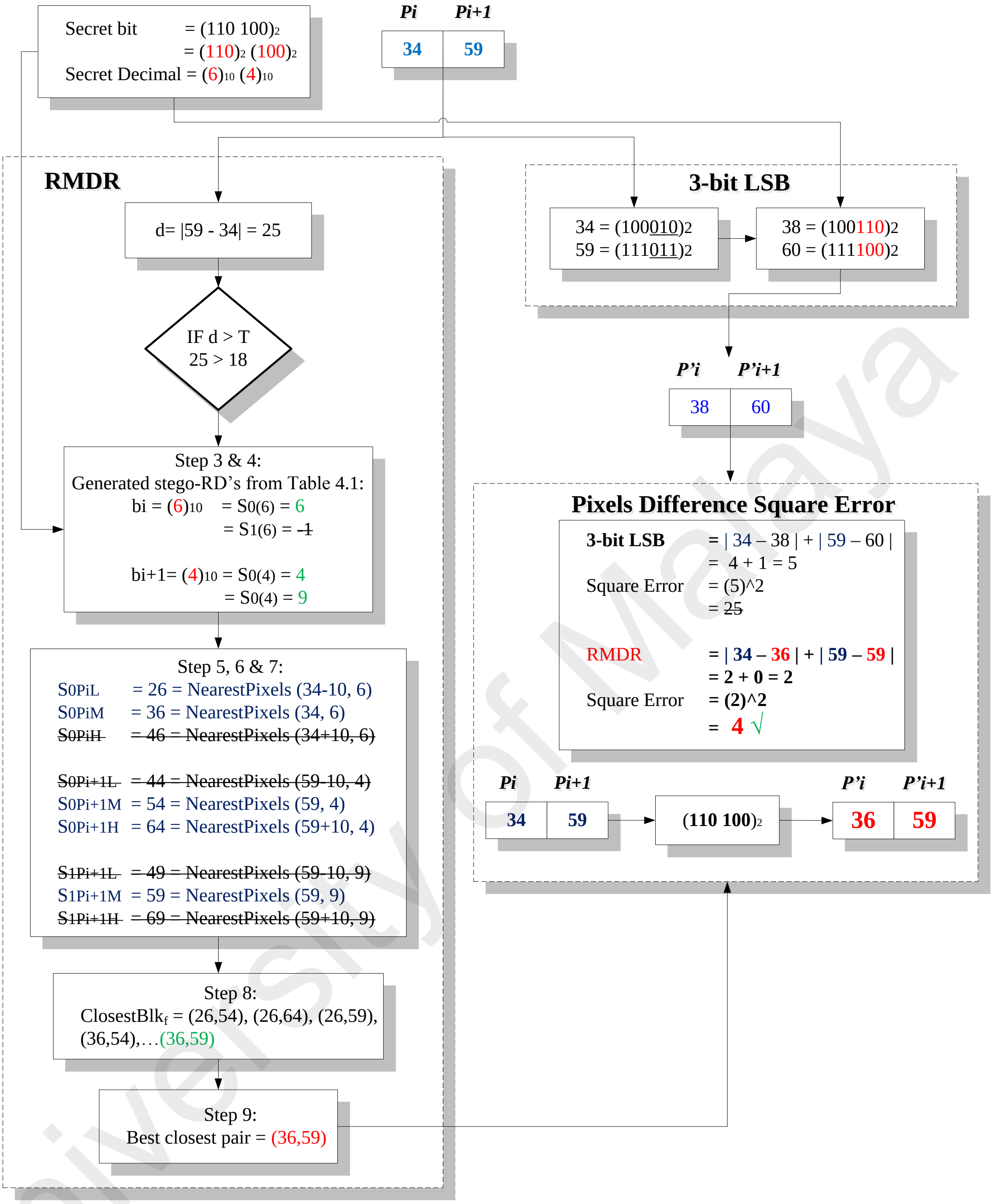

Secret bit = (110 100)2
= (110)2 (100)2
Secret Decimal = (6)10 (4)10
Pi
Pi+1
34
59
RMDR
d= |59 - 34| = 25
IF d > T
25 > 18
Step 3 & 4:
Generated stego-RD's from Table 4.1:
bi = (6)10 = S0(6) = 6
= S1(6) = ~~-1~~
bi+1= (4)10 = S0(4) = 4
= S0(4) = 9
Step 5, 6 & 7:
S0PiL = 26 = NearestPixels (34-10, 6)
S0PiM = 36 = NearestPixels (34, 6)
~~S0PiH = 46 = NearestPixels (34+10, 6)~~
~~S0Pi+1L = 44 = NearestPixels (59-10, 4)~~
S0Pi+1M = 54 = NearestPixels (59, 4)
S0Pi+1H = 64 = NearestPixels (59+10, 4)
~~S1Pi+1L = 49 = NearestPixels (59-10, 9)~~
S1Pi+1M = 59 = NearestPixels (59, 9)
~~S1Pi+1H = 69 = NearestPixels (59+10, 9)~~
Step 8:
ClosestBlkf = (26,54), (26,64), (26,59),
(36,54),…(36,59)
Step 9:
Best closest pair = (36,59)
3-bit LSB
34 = (100010)2
59 = (111011)2
38 = (100110)2
60 = (111100)2
P'i
P'i+1
38
60
Pixels Difference Square Error
3-bit LSB = | 34 – 38 | + | 59 – 60 |
= 4 + 1 = 5
Square Error = (5)^2
= ~~25~~
RMDR = | 34 – 36 | + | 59 – 59 |
= 2 + 0 = 2
Square Error = (2)^2
= 4 √
Pi
Pi+1
34
59
(110 100)2
P'i
P'i+1
36
59

Figure 4.3: Example of Closest/Similar Stego-pixels Selection in RMDR vs. 3-bit LSB

4.1.2 RMDR Extracting Method

Similar to RMDR embedding procedure, the RMDR extracting method follows steganography-extracting phase of research methodology (Figure 3.4). It also consists of pre-processing, extracting and post-processing phases as shown in Figure 4.4 and detail is as follows.

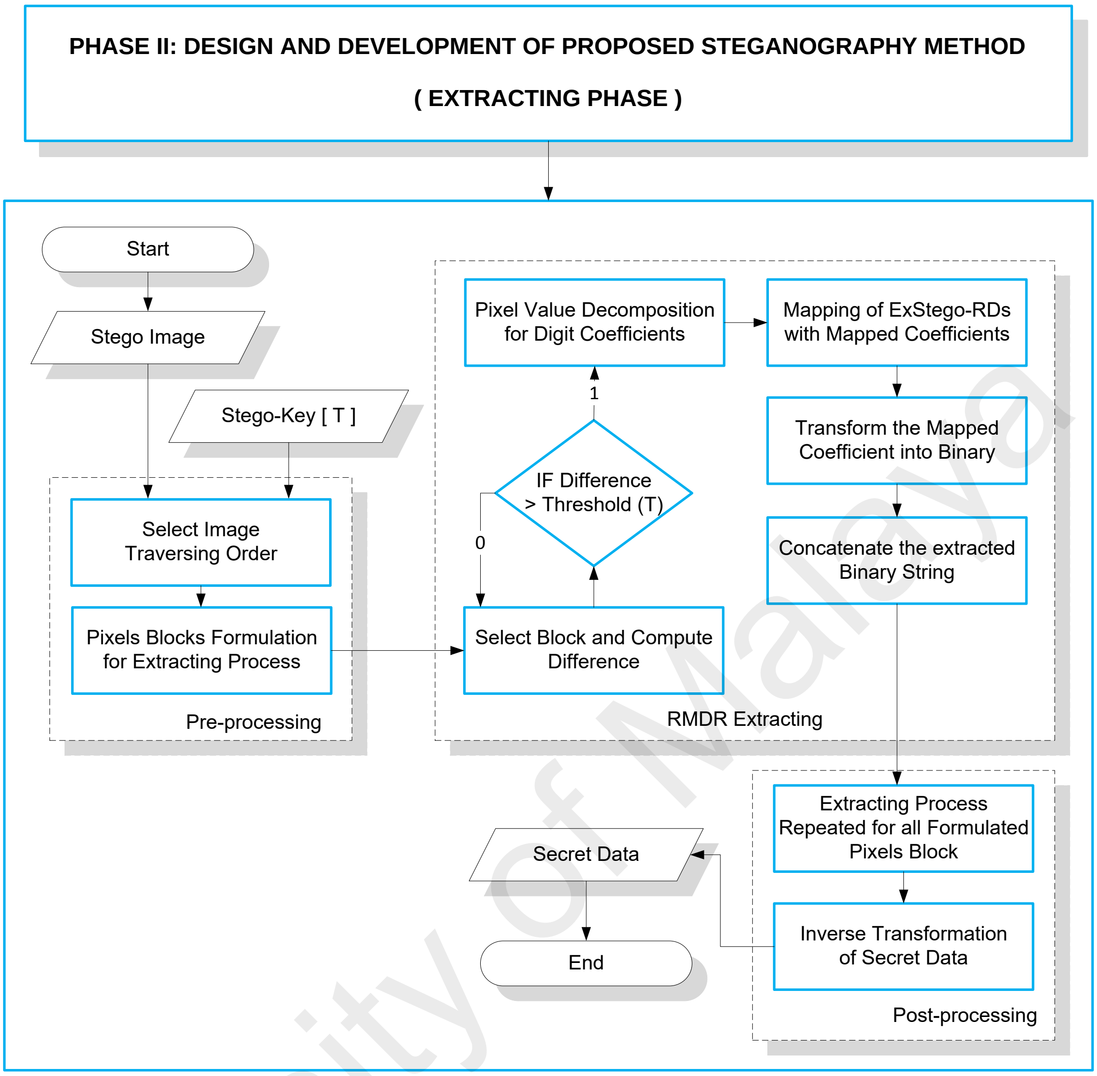

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EXTRACTING PHASE)
Start
Stego Image
Stego-Key [T]
Select Image Traversing Order
Pixels Blocks Formulation for Extracting Process
Pre-processing
Pixel Value Decomposition for Digit Coefficients
Mapping of ExStego-RDs with Mapped Coefficients
1
IF Difference > Threshold (T)
0
Transform the Mapped Coefficient into Binary
Concatenate the extracted Binary String
Select Block and Compute Difference
RMDR Extracting
Extracting Process Repeated for all Formulated Pixels Block
Secret Data
End
Inverse Transformation of Secret Data
Post-processing

Figure 4.4: The Basic Flow Diagram of RMDR Extracting

(a) ***Pre-processing of RMDR Extracting Method***

This pre-processing phase requires a stego-image before applying the actual RMDR extracting process (see Figure 4.4). First, this pre-processing selects the stego-image traversing order further it divides the stego-image into number of blocks like section 4.1.1 (a). The output of this stage would be the selected pixels groups, which will be employed by the core RMDR extracting process.

(b) ***RMDR Extracting***

In this process, RMDR extracting algorithm recovers the secret data bits from stego-image. First this stage identifies the status of regular and skipped blocks based on the difference between stego-pixels as shown in Figure 4.4. If the difference of stego-pixels block is smaller than T threshold, it would be rejected for recovering phase, otherwise proceeded with further steps.

This extracting procedure follows the similar pixel digit decomposition pattern that was employed in RMDR embedding process. After decomposition of stego-pixels in to digits, the output digits known as ExStego-RDs ($eD_{r(i)}$,$eD_{r(i+1)}$), that are further mapped with its equivalent decoded decimal coefficient (b_i, b_{i+1}) from Table 4.4. The Table 4.4 is a simple inverse of Table 4.1 with the notion of remapping of Stego-RDs to secret decimal values. Next extracting phase transforms the decoded decimal coefficient to its binary form and applies simple concatenation process to recover the secret message bits.

Table 4.4: RMDR Extracting Table for Stego-RDs

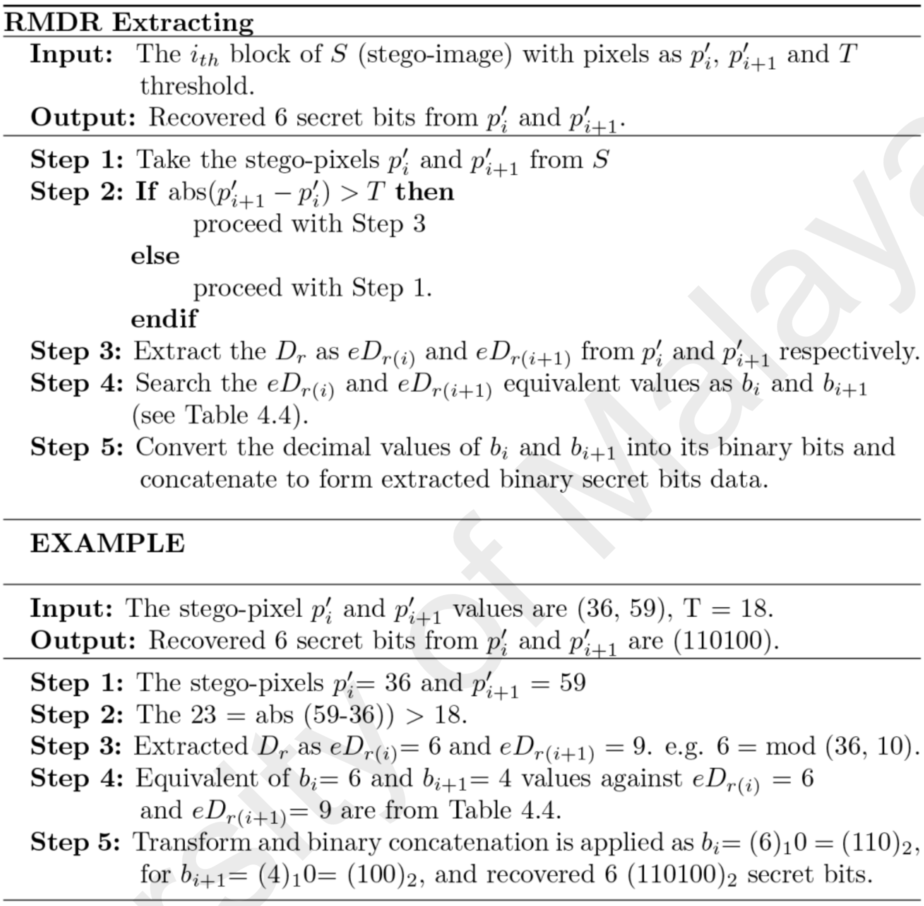
ExStego-RDs	$eD_{r(i)}\|eD_{r(i+1)}$	0	1	2	3	4	5	6	7	8	9
Decoded decimal coefficient	$b_i\| b_{i+1}$	0	1	2	3	4	5	6	7	3	4

(c) ***Post-processing of RMDR Extracting Method***

Similar to embedding process, this phase repeats the extraction process until all the secret data are recovered from the stego-image. Further, if the secret data are compressed or already been encrypted at embedding stage, then its counter decryption/decompression techniques are applied to fully recover the secret data.

Furthermore, the complete proposed RMDR extracting algorithm steps and example are defined in Table 4.5.

Table 4.5: RMDR Extracting Steps with Example



RMDR Extracting

Input: The i_{th} block of S (stego-image) with pixels as p'_i, p'_{i+1} and T threshold.

Output: Recovered 6 secret bits from p'_i and p'_{i+1}.

```
Step 1: Take the stego-pixels $p'_i$ and $p'_{i+1}$ from $S$
Step 2: If abs($p'_{i+1} - p'_i$) $> T$ then
            proceed with Step 3
        else
            proceed with Step 1.
        endif
Step 3: Extract the $D_r$ as $eD_{r(i)}$ and $eD_{r(i+1)}$ from $p'_i$ and $p'_{i+1}$ respectively.
Step 4: Search the $eD_{r(i)}$ and $eD_{r(i+1)}$ equivalent values as $b_i$ and $b_{i+1}$
        (see Table 4.4).
Step 5: Convert the decimal values of $b_i$ and $b_{i+1}$ into its binary bits and
        concatenate to form extracted binary secret bits data.
```

EXAMPLE

Input: The stego-pixel p'_i and p'_{i+1} values are (36, 59), T = 18.

Output: Recovered 6 secret bits from p'_i and p'_{i+1} are (110100).

```
Step 1: The stego-pixels $p'_i$= 36 and $p'_{i+1}$ = 59
Step 2: The 23 = abs (59-36)) > 18.
Step 3: Extracted $D_r$ as $eD_{r(i)}$= 6 and $eD_{r(i+1)}$ = 9. e.g. 6 = mod (36, 10).
Step 4: Equivalent of $b_i$= 6 and $b_{i+1}$= 4 values against $eD_{r(i)}$ = 6
        and $eD_{r(i+1)}$= 9 are from Table 4.4.
Step 5: Transform and binary concatenation is applied as $b_i = (6)_10 = (110)_2$,
        for $b_{i+1} = (4)_10 = (100)_2$, and recovered 6 $(110100)_2$ secret bits.
```

4.1.3 Experimental Results and Analysis

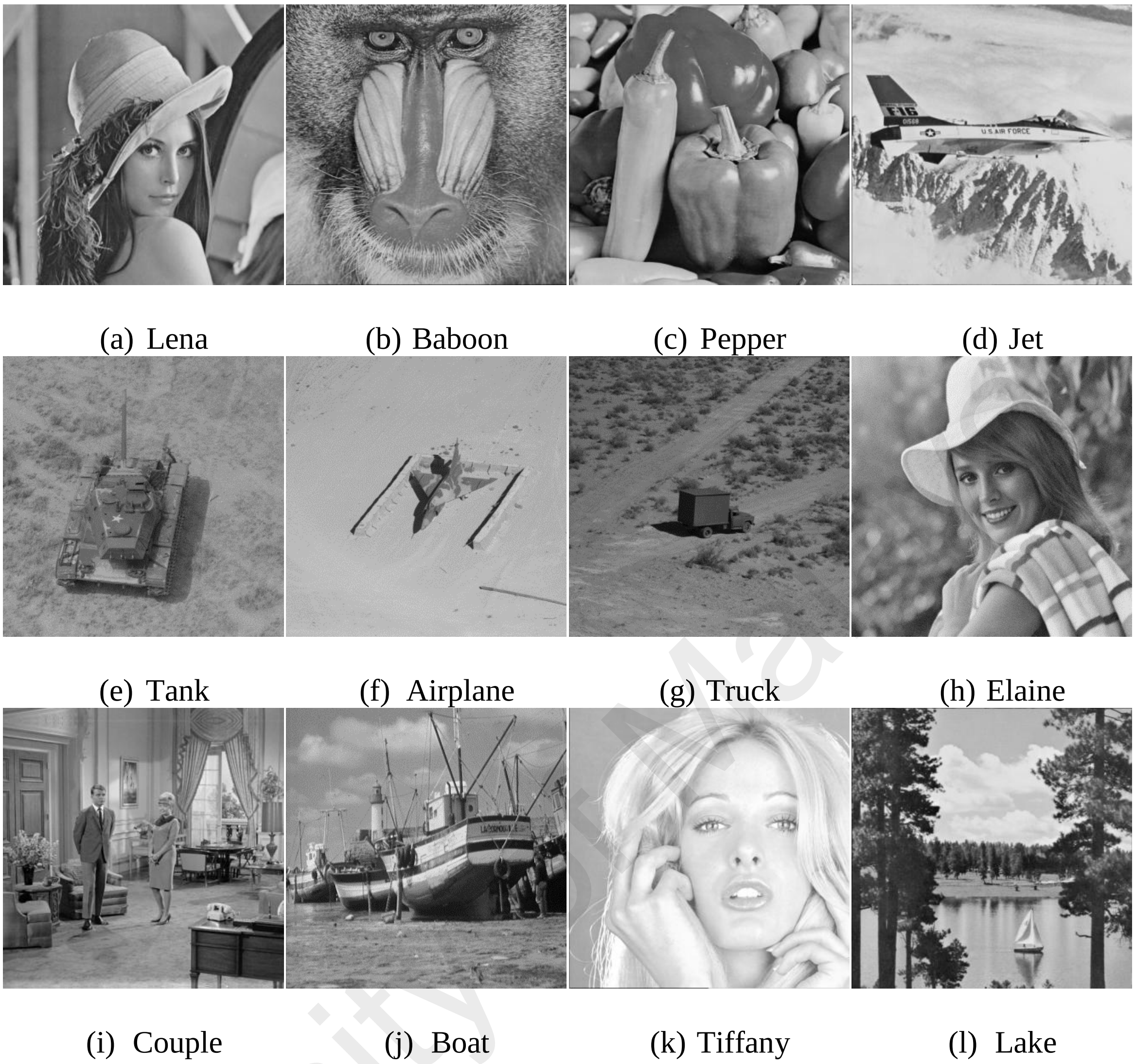
In this section, the result of this experiment is presented. To evaluate the performance of the proposed RMDR steganography method, we need to use some standard and sufficiently large image datasets that must contain various types of texture based images. Therefore, we will evaluate various measures associated with steganography success criteria i.e. stego-image quality, high embedding capacity, undetectability/security.

4.1.3.1 Dataset and Setup

In our experiments, we employed two well-known image datasets to evaluate the proposed RMDR steganography method. There are two objectives behind the selecting of these datasets. First reason, in order to determine performance of proposed method for various types of images i.e. low and high texture based images. Second reason, these datasets are considered as standard benchmarking in existing image steganography literature.

First, the Signal and Image Processing Institute dataset from University of Southern California (USC-SIPI, 2016) contains miscellaneous volume of images. This contains 144 different resolution (of 512 x 512, 128x 256) gray and colors scale images. It also includes standard images i.e. Lena, Baboon, Peppers, Jet, Tank, Airplane, Truck, Elaine, Couple, Boat, Tiffany and Lake as shown in Figure 4.5. Second, the proposed method tested with uncompressed color image database (UCID) (Schaefer & Stich, 2004), which consists of 1338 images with resolution of 512 x 384 and 384 x 512. Meanwhile, we converted the color images to grayscale before applying embedding procedure to maintain the similarity/integrity with benchmark methods. For secret data, a pseudo-random number generator is used to generate the secret bits to ensure that the probabilities of bit ‘1’ and ‘0’ in the message are identical.

We conducted majorly two sets of experiments to evaluate the performance of the proposed steganography method. First, to measure the embedding capacity and visual quality, and the second is to evaluate the proposed method security/undetectability against steganalysis. In addition we perform modern steganalysis by applying machine learning ensemble classifier using Subtractive Pixel Adjacency Matrix (SPAM) detector (Pevny et al., 2010).


(a) Lena (b) Baboon (c) Pepper (d) Jet

(e) Tank (f) Airplane (g) Truck (h) Elaine

(i) Couple (j) Boat (k) Tiffany (l) Lake

Figure 4.5: Standard Images for Experiments from (USC-SIPI, 2016) Dataset.

4.1.3.2 Embedding Capacity and Visual Quality Evaluation

This section analysis the performance of proposed RMDR embedding with existing singular steganographic methods with respect to embedding capacity and visual quality. Furthermore, the visual quality performance also measured at various embedding rates to evaluate the relation between embedding capacity and imperceptibility. Finally, both standard UCID and USC-SIPI image datasets employed to evaluate the performance of proposed and compared methods.

(a) ***Performance of Embedding Capacity and Visual Quality***

First, proposed method is compared with conventional singular 3-bit LSB (Chan & Cheng, 2004), pixel value difference (D.-C. Wu & Tsai, 2003) and adaptive LSB (H. Yang et al., 2009) steganographic methods. We employed the standard images (i.e. Lena, Baboon, Pepper …, etc.) as shown in Table 4.6 for initial performance evaluation. The results show that the average embedding capacity of proposed method is 3 bpp, it is similar to 3-bit LSB, while higher than PVD (D.-C. Wu & Tsai, 2003) and adaptive LSB (H. Yang et al., 2009) methods. Similarly, the visual quality parameter as peak signal to noise ratio (PSNR), this shows that the proposed method has higher PSNR value against all compared methods except PVD approach. The reason for higher PSNR value based on the RMDR closest stego-pixel selection process, which indirectly reduces the difference error between cover and stego-pixel and improved the visual quality. As result, proposed method showed the PSNR improvement of +1.85 dB against 3-bit LSB, while retained the similar PSNR against adaptive LSB method. From Table 4.6, it is observed that PSNR value of proposed method is lower than PVD method (-1.09 dB) but the embedding capacity is almost the doubled (373,708 bits). Because, the objective of PVD method is to enhance the visual quality PSNR value without considering the embedding rate. In addition, PVD method adjusts the differences between two pixels instead of applying any direct substitution. The substitution-based techniques can retain the high embedding capacity as achieved in our proposed method.

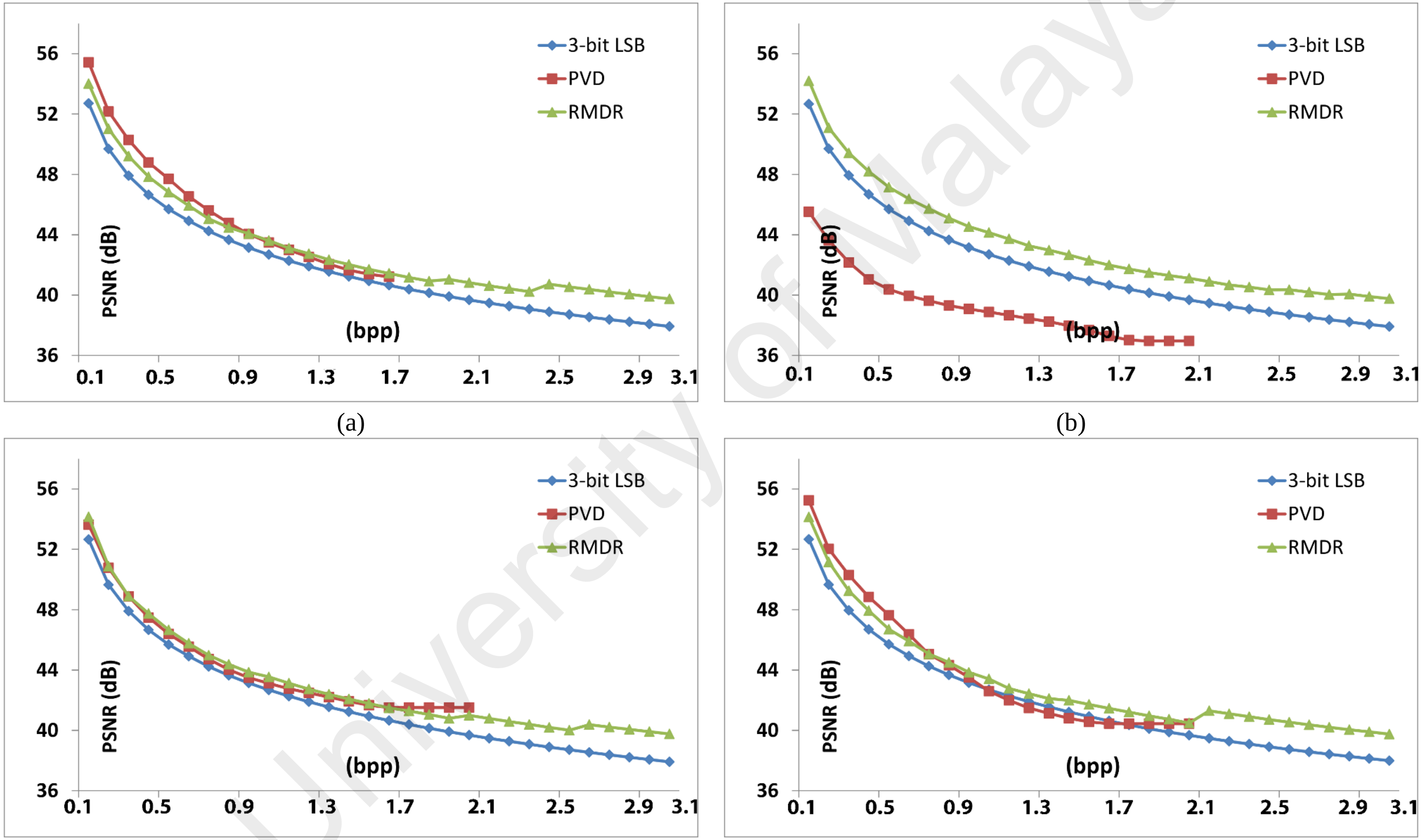
Table 4.6: Performance Comparison of Proposed and Existing Classic Singular Steganography Methods

Images	3-bit LSB				(D.-C. Wu & Tsai, 2003) PVD				(H. Yang et al., 2009) Adaptive LSB				RMDR Method T= 0			
	Capacity	**PSNR**	**Q**	**RMSE**	**Capacity**	**PSNR**	**Q**	**RMSE**	**Capacity**	**PSNR**	**Q**	**RMSE**	**Capacity**	**PSNR**	**Q**	**RMSE**
Lena	786,429	37.92	0.9977	3.24	409,779	41.14	0.9989	2.24	757,332	39.31	0.9978	2.76	786,432	39.75	0.9985	2.62
Baboon	786,429	37.91	0.9971	3.24	456,953	36.98	0.9964	3.61	785,572	39.16	0.9972	2.82	786,432	39.76	0.9981	2.62
Pepper	786,429	37.91	0.9982	3.24	405,425	41.55	0.9992	2.13	786,014	39.06	0.9983	2.73	786,432	39.76	0.9988	2.62
Jet	786,429	37.98	0.9976	3.22	409,531	40.42	0.9986	2.43	735,236	39.55	0.9977	2.76	786,432	39.75	0.9984	2.62
Tank	786,429	37.85	0.9928	3.27	403,990	42.38	0.9975	1.94	784,019	39.03	0.9930	2.78	786,432	39.72	0.9954	2.63
Airplane	786,429	37.70	0.9889	3.32	397,904	42.19	0.9960	1.98	773,101	39.09	0.9890	2.84	786,432	39.69	0.9931	2.64
Truck	786,429	37.83	0.9928	3.27	400,504	42.87	0.9977	1.83	775,572	39.15	0.9931	2.79	786,432	39.75	0.9955	2.62
Elaine	786,429	37.89	0.9975	3.25	408,582	41.88	0.9990	2.05	761,204	39.32	0.9985	2.83	786,432	39.76	0.9984	2.62
Couple	786,429	37.91	0.9973	3.24	419,901	39.78	0.9983	2.62	756,019	39.06	0.9974	2.81	786,432	39.76	0.9983	2.62
Boat	786,429	37.94	0.9976	3.23	419,317	39.52	0.9983	2.69	755,528	39.04	0.9986	2.86	786,432	39.76	0.9985	2.62
Tiffany	786,429	37.91	0.9939	3.25	398,980	41.48	0.9973	2.15	777,888	39.12	0.9941	2.89	786,432	39.65	0.9960	2.66
Lake	786,429	37.91	0.9988	3.24	421,819	39.75	0.9992	2.62	750,013	39.01	0.9986	2.87	786,432	39.75	0.9992	2.63
Average	786,429	37.89	0.9959	3.25	412,724	40.83	0.9980	2.36	766,458	39.16	0.9961	2.81	**786,432**	**39.74**	**0.9973**	**2.63**

Similar to PSNR, proposed method has higher universal quality index (Q) and best root mean square error (RMSE) ratio against all the compared methods except PVD technique. The average Q value is 0.9973 and RMSE is 2.63 that are closer to 1 and proved a good visual quality of stego-image. As results from Table 4.6 analysis, proposed method improved visual quality against standard LSB and adaptive LSB methods while maintaining the high rate i.e. 3 bpp embedding capacity.

(b) ***Performance of Visual Quality at Various Embedding Capacity Rates***

The purpose of this experiment is to evaluate the performance of visual quality at different embedding rates instead of maximum payload. Figure 4.6 shows the PSNR at 0.1 to 3.0 bpp embedding rates. Where, the x-axis and y-axis represent the embedding bits per pixel (bpp) and PSNR value in dB, respectively. From all the graphs, proposed RMDR method depicts that it has higher PSNR value at each embedding rate. Moreover, for higher texture based images i.e. Baboon as shown in graph (Figure 4.6 b), this illustrates that the PVD method retained the lower PSNR values for all embedding capacity rates. This indicates that the PVD method has poor visual performance at higher texture based images. As we observed form Table 4.6, the maximum average embedding capacity of PVD technique is around 1.58 bpp. This is the reason, PVD embedding capacity curve ended up to around 1.6 bpp rate as shown in the x-axis of Figure 4.6 graphs. On the other side, proposed method retains the similar and higher PSNR value at all the embedding rates, this shows that the RMDR performance is equally ideal for high embedding rates as well as low embedding rates for all types of low and high texture based images.



(a)

(b)

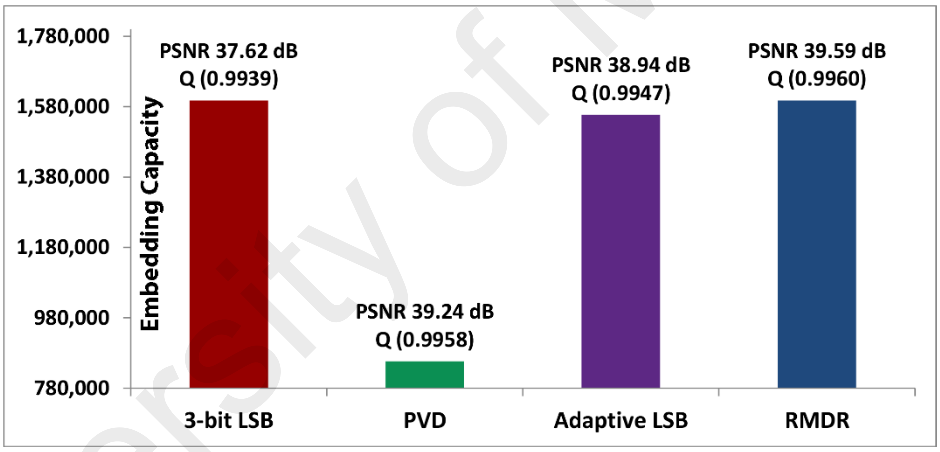
(c)

(d)

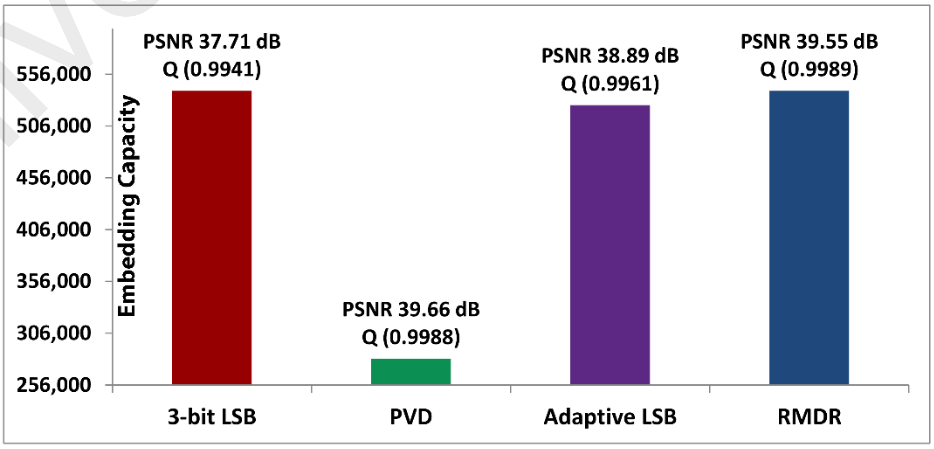
Figure 4.6: PSNR Graph at Various Embedding Rates (a) Lena, (b) Baboon, (c) Pepper (d) Jet

(c) ***Performance over UCID and USC-SIPI Image Datasets***

In this experiment, we employed the complete UCID (Schaefer & Stich, 2004) and SIPI (USC-SIPI, 2016) image datasets for in depth performance evaluation. In Figure, 4.7 (a) shows the performance of proposed RMDR (T=0) and compared methods for SIPI (144 images) dataset. Similarly, the Figure 4.7 (b) shows the embedding capacity and visual quality performance for complete UCID (1338) images. Where, in Figure 4.7 x-axis and y-axis represent the embedding methods and embedding bits, respectively. As result, both graphs depict that proposed method retains the higher embedding capacity and higher visual quality regardless of various types of textures and image resolutions.



(a)



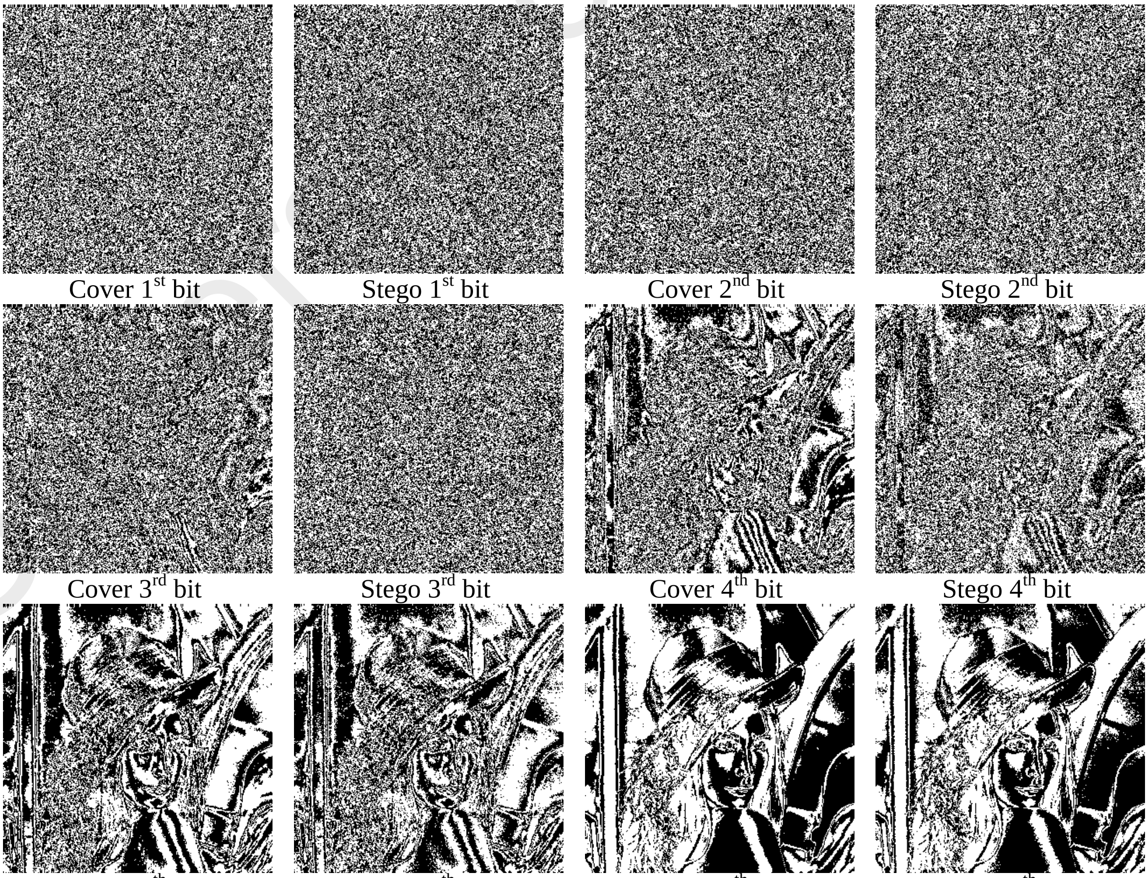
(b)

Figure 4.7: Embedding Capacity and PSNR Performance for (a) SIPI (USC-SIPI, 2016) (b) UCID (Schaefer & Stich, 2004) Datasets.

4.1.3.3 Security/Un-detectability Evaluation

(a) ***Bit-plane Analysis***

In this section, the bit-plane analysis results of proposed RMDR methods are presented for first four selected Lena, Baboon, Pepper and Jet images as shown in Figure 4.8 to 4.11. Furthermore, these results illustrate the each bit-plane decompositions separately presented for all selected stego-images. For example, Figure 4.8 shows the Lena cover and its respective stego-images for all 1 to 8 bit-planes. The visual analysis of Lena stego-image is almost similar to its cover in each bit-plane visual representation. Similarly, for all remaining Baboon, Pepper and Jet stego-images, proposed technique is able retain the similar bit-planes visual representation with its respective cover-images. Therefore, this seems that proposed RMDR stego-images can resist the visual bit-plane analysis.



Cover 1st bit

Stego 1st bit

Cover 2nd bit

Stego 2nd bit

Cover 3rd bit

Stego 3rd bit

Cover 4th bit

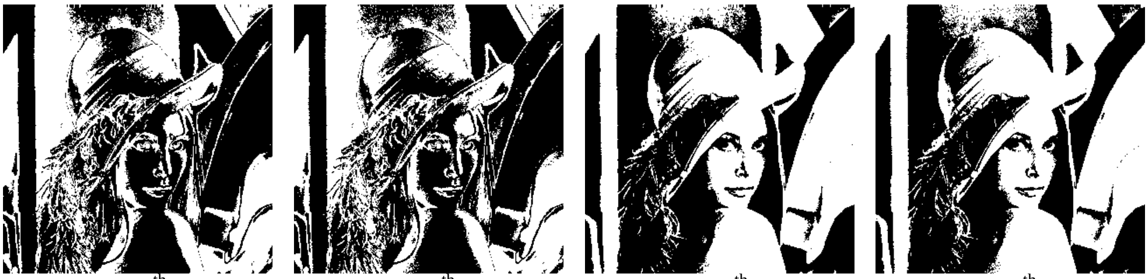
Stego 4th bit

Cover 5th bit

Stego 5th bit

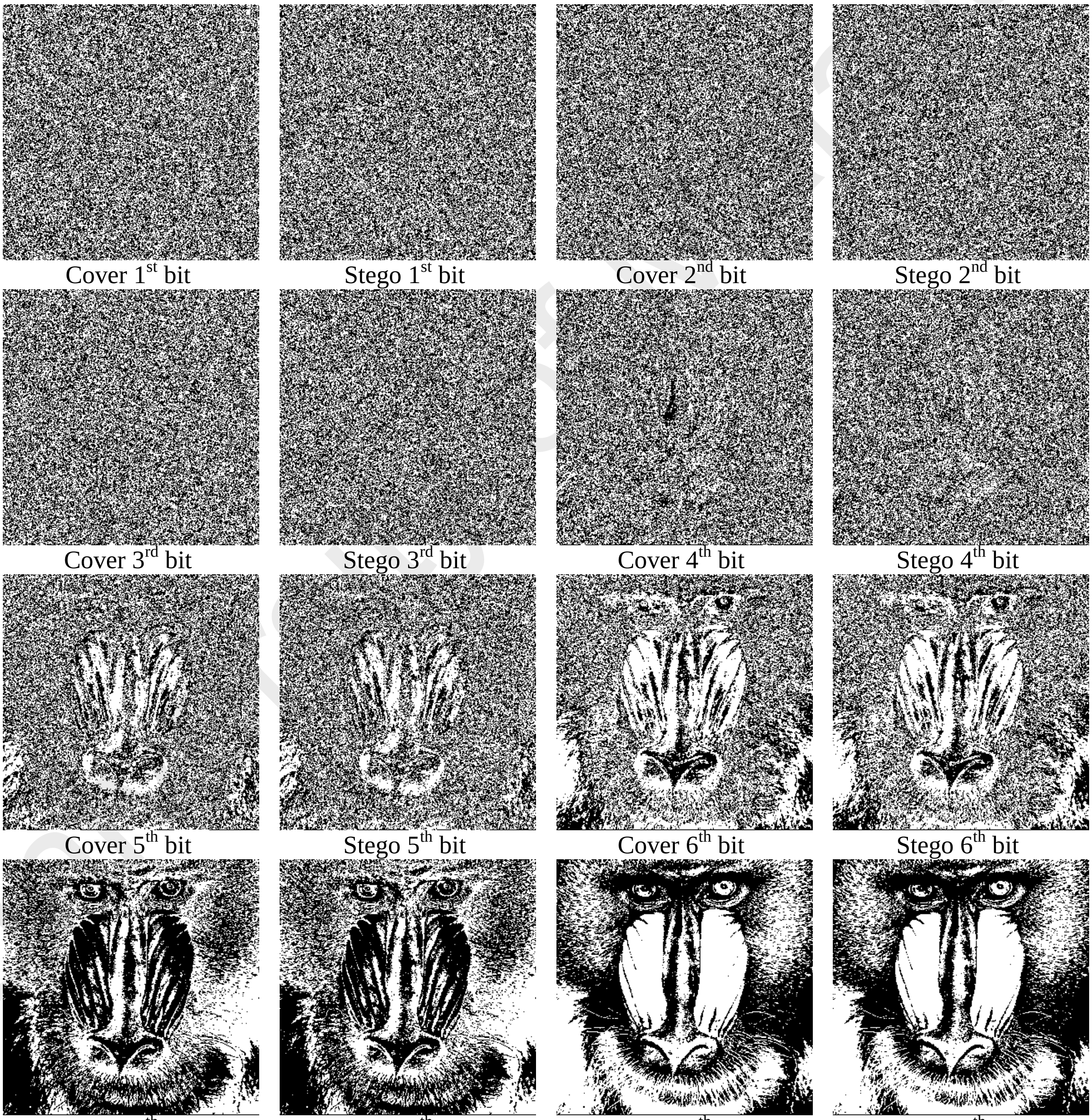
Cover 6th bit

Stego 6th bit



Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.8: Bit-plane Analysis of Proposed RMDR (T=0) Stego-image (Lena)



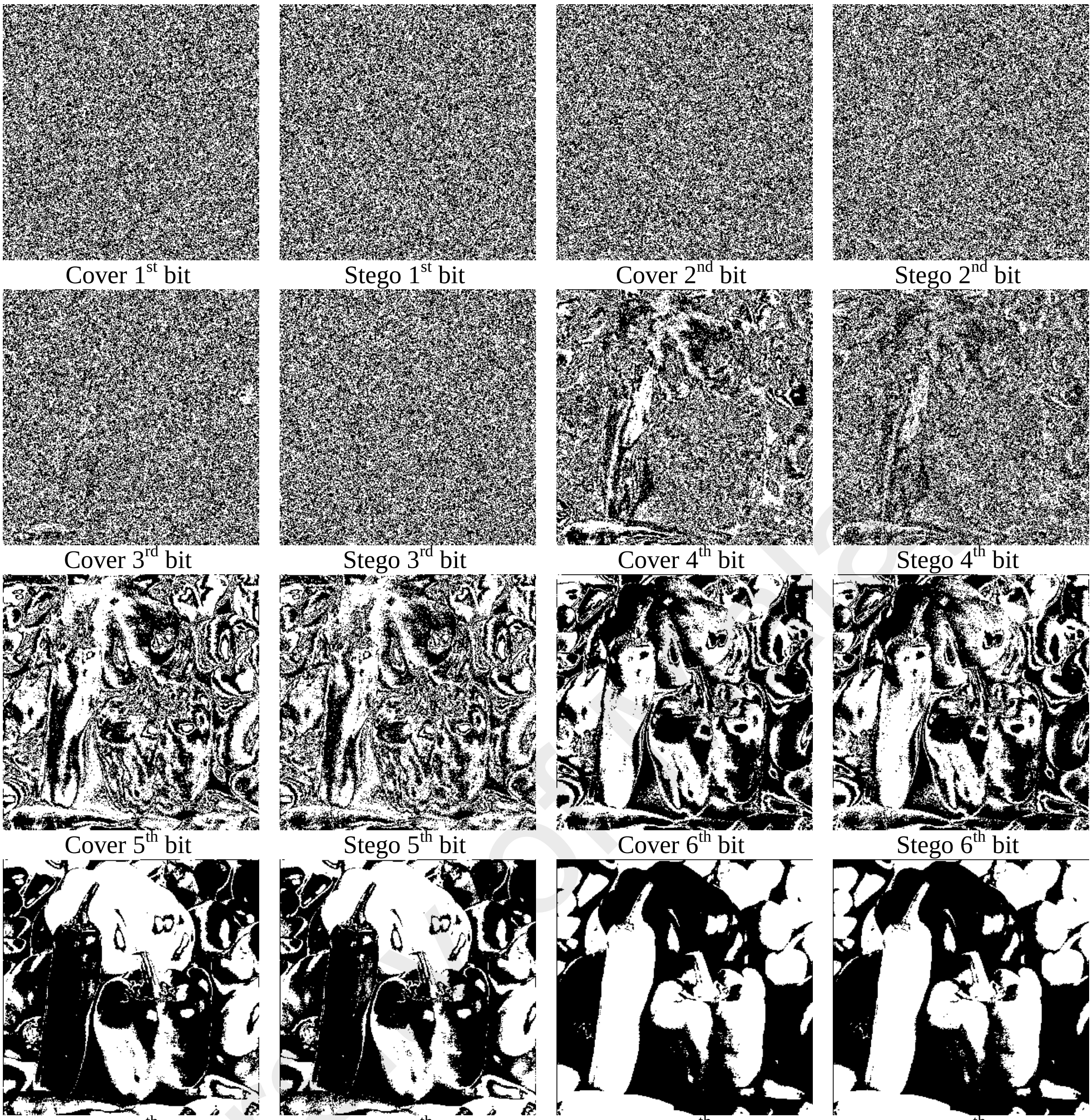
Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit

Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.9: Bit-plane Analysis of Proposed RMDR (T=0) Stego-image (Baboon)



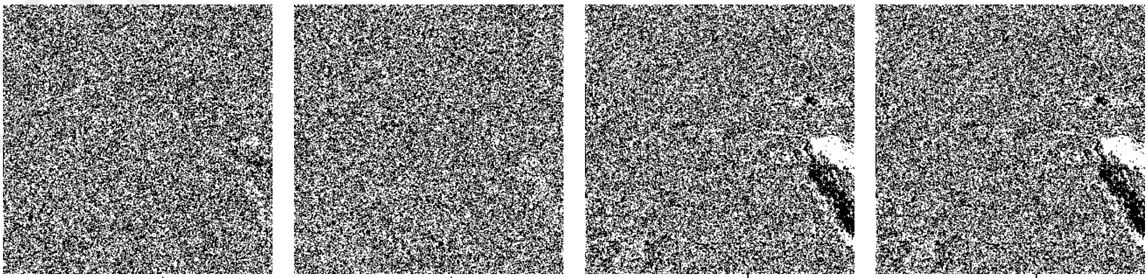
Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit

Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

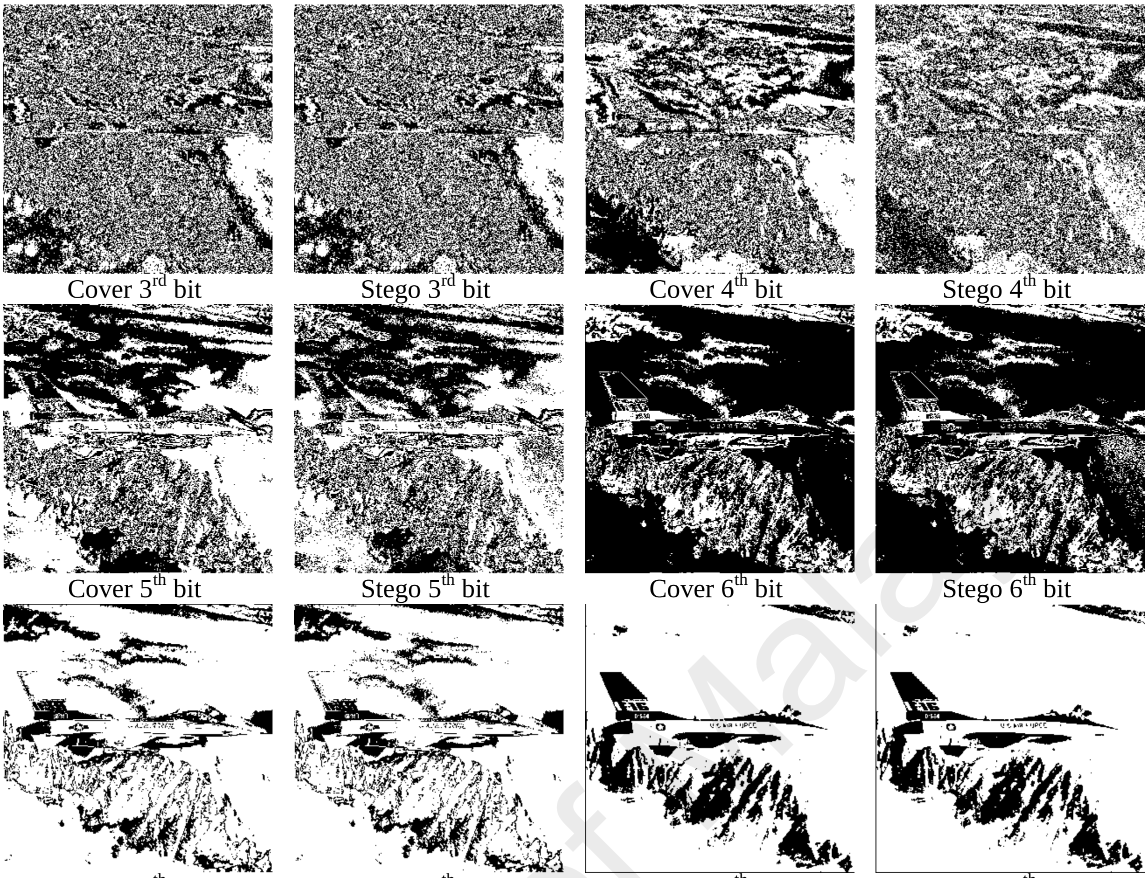
Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.10: Bit-plane Analysis of Proposed RMDR (T=0) Stego-image (Pepper)



Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit



Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

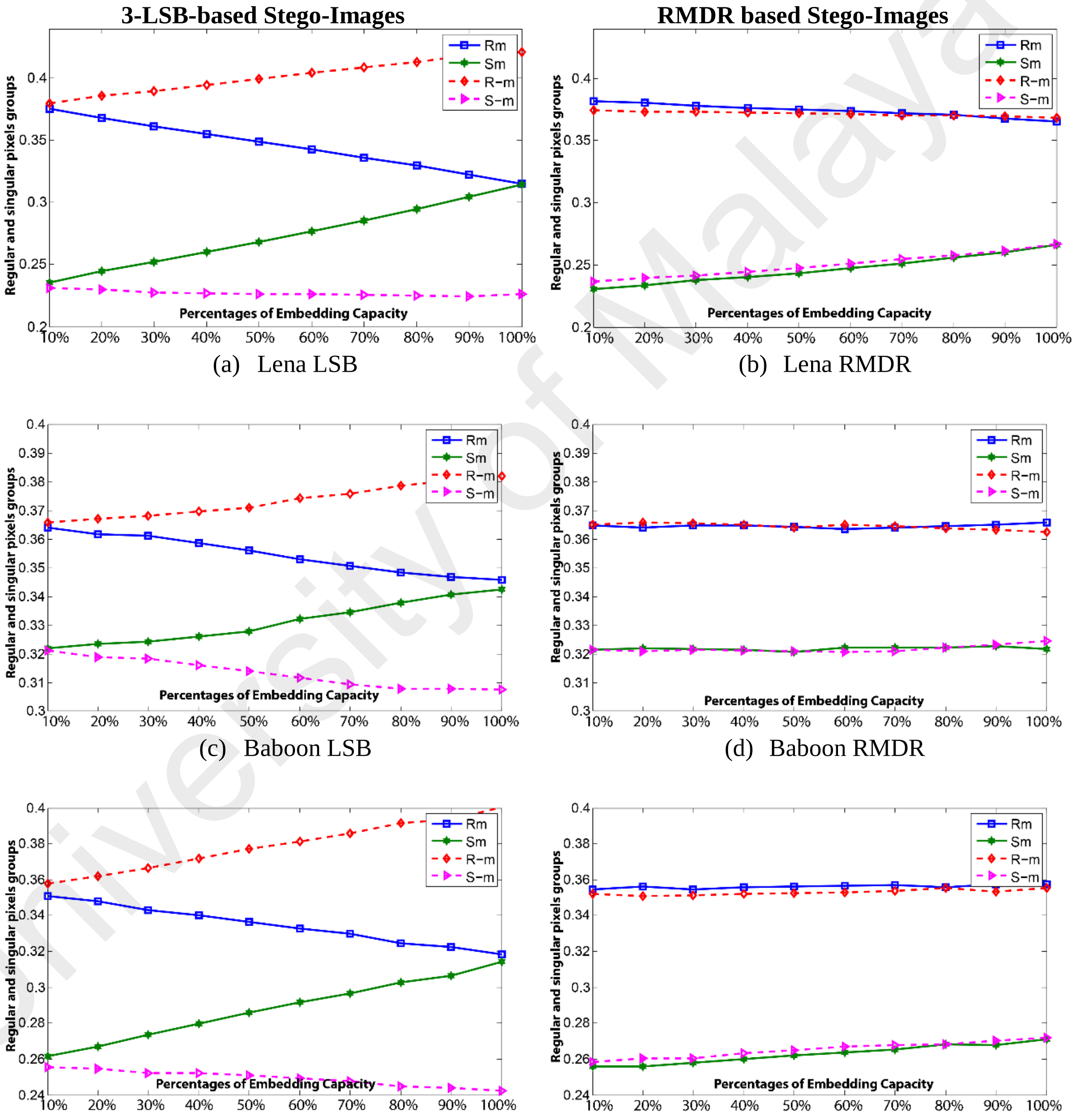
Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.11: Bit-plane Analysis of Proposed RMDR (T=0) Stego-image (Jet)

(b) ***Security under RS detection analysis***

In this analysis, Figure 4.12 presents the RS diagram for both 3-bit LSB and proposed RMDR embedding methods. The x-axes and y-axes represent the percentage of hiding capacity and percentage of regular and singular pixels groups respectively for all graphs of Figure 4.12 (a-n). The difference ratio in y-axes singular and regular pixels group’s ranges depends on the texture of the used image. Meanwhile, it is clearly noticeable that 3-bit LSB-based stego-images are not robust against RS detection analysis, because increasing rate of embedding capacity leads to increase the difference between RM and R-M, and similarly for SM and S-M parameters. Conversely, the RMDR method can retain the difference between RM and R-M, SM and S-M for all stego-images. However, the average accumulated difference between RM and R-M, SM and S-M for RMDR are less than 3-bit LSB embedding. Therefore, the overall results show that proposed RMDR method is more robust against RS detection analysis than 3-LSB embedding. The reason is that proposed method substitutes the digits instead of bits replacement. In addition, its closest selection process generate the best nearest stego-pixels against its cover pixels, thus this evade the risk of RS detection attacks.



(a) Lena LSB

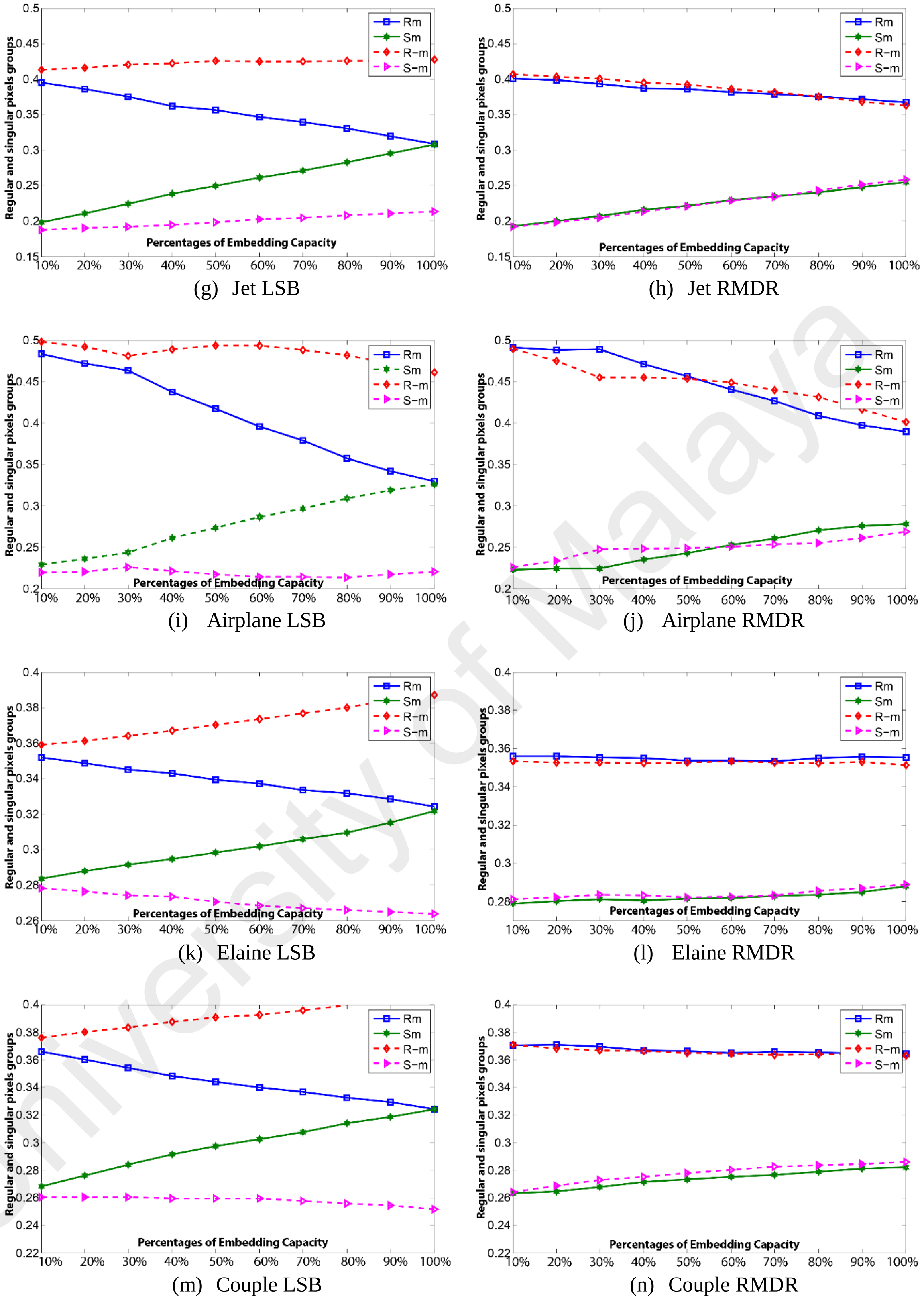
(b) Lena RMDR

(c) Baboon LSB

(d) Baboon RMDR

(e) Pepper LSB

(f) Pepper RMDR



(g) Jet LSB

(h) Jet RMDR

(i) Airplane LSB

(j) Airplane RMDR

(k) Elaine LSB

(l) Elaine RMDR

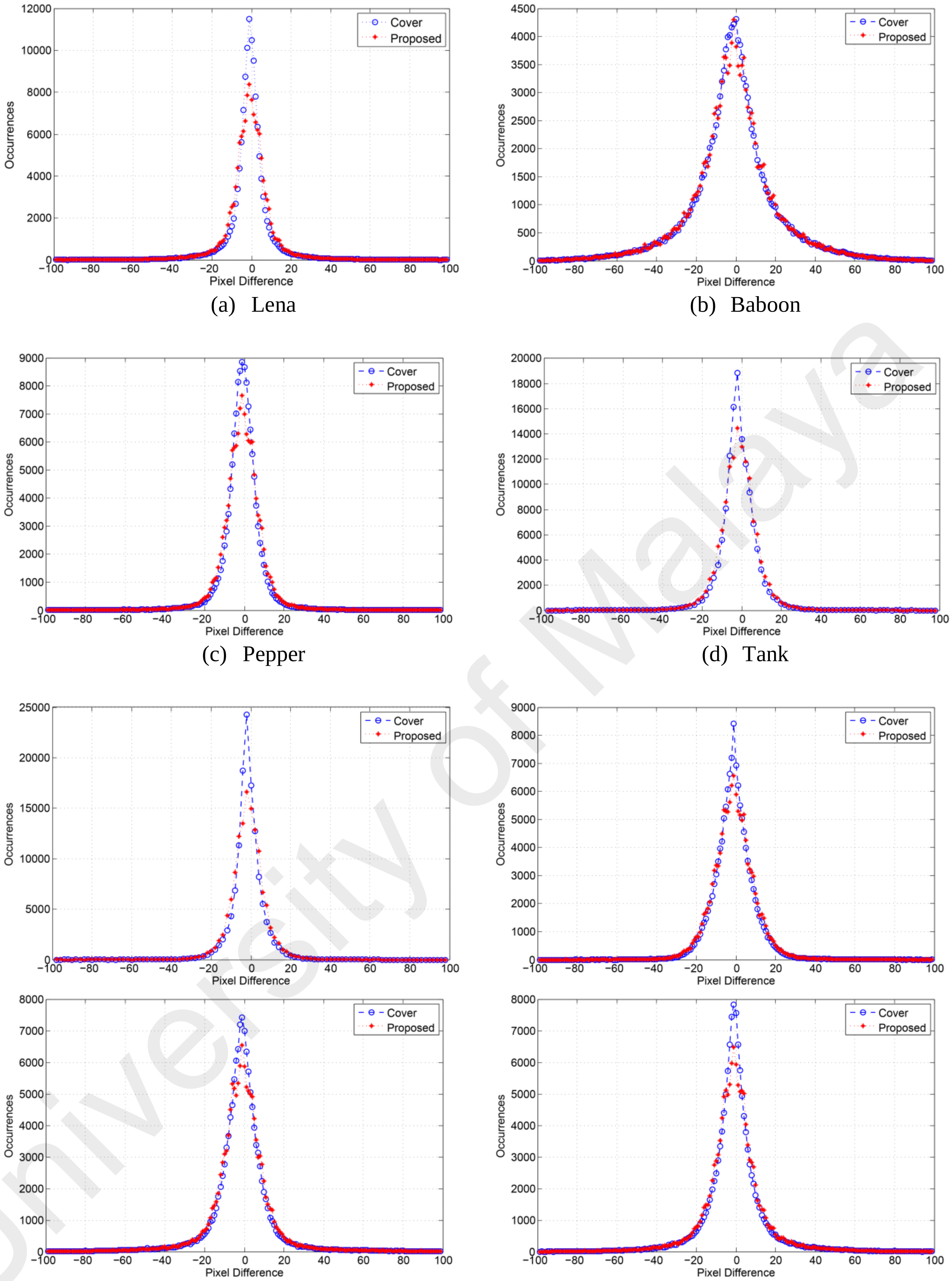
(m) Couple LSB

(n) Couple RMDR

Figure 4.12: RS Analysis Diagram for 3-Bit LSB and Proposed RMDR (T=0) Methods

(c) ***Pixel Difference Histogram Analysis***

The pixel difference histogram graphs diagrams are presented in Figure 4.13 for RMDR based stego-images. The x-axis and y-axis represent the difference range and frequency of pixels, respectively. This shows that most of the RMDR based stego-images are able to retain the symmetry curves of graph or follow the similar curves with respect to its cover images. However, still proposed method is not able to maintain the 100% identical histogram curves between cover and stego-images. On the other side, proposed method is still able to survive the visual analysis of pixel differencing histogram, in case the cover-image is not available along its stego-image. In addition, the stego-images of proposed method are also maintained the symmetry in pixel difference steps. The reason is that proposed RMDR embedding method generates the closest stego-pixels against its respective cover pixels through various underline strategies (i.e. vertical differences, nearest pixel generation etc.) that reduces the difference between cover and stego-pixels. Therefore, to some extent the proposed method has robustness against pixel-difference histogram analysis.



(a) Lena
(b) Baboon
(c) Pepper
(d) Tank
(e) Boat
(f) Lake

Figure 4.13: Pixel Difference Histogram for RMDR (T=0) Embedding Method

(d) ***Security under Ensemble Classifier using SPAM***

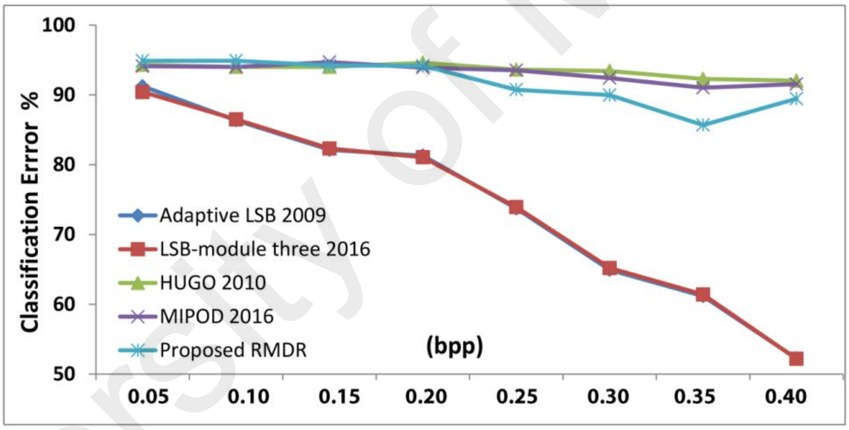
In this section, proposed method is evaluated using modern machine learning classifier i.e. ensemble classifier by (Kodovsky et al., 2012) to differentiate the cover and stego-images. In this classification, multiple classifiers (i.e. Adaboost, Bagging, and Random Forest) are employed by adopting a majority vote based classifier for more accurate predictions of unknown class labels. In addition, a modern steganalysis detector, known as Subtractive Pixel Adjacency Matrix (SPAM) detector proposed by (Pevny et al., 2010) is employed. In the literature, SPAM is possibly the most accurate state-of-the-art single-model steganalysis tool for detection of substitution based embedding techniques. Therefore, we tested the robustness of proposed method against SPAM steganalysis. Usually, the robustness in modern steganalysis is measured by the classification error or detection errors, where the higher classification error rate would be the lower the detectability of the respective embedding method. We tested the robustness of proposed RMDR method with best random threshold T = Ṝ, further compared with state-of-the-art LSB-based HUGO (Pevný et al., 2010), MiPOD (Sedighi, Cogranne, & Fridrich, 2016), adaptive LSB (H. Yang et al., 2009) and recently LSB module three (Xu et al., 2016) based embedding methods. The reason for selection of compared method is that HUGO and recently MiPOD embedding techniques are designed to produce a less distorted stego-image with at most change of ±1 pixel value. Furthermore, the both methods have high robustness against SPAM based steganalysis and considered as optimal steganography techniques with respect to security. The rest of two, adaptive LSB and LSB-module-three methods are designed to target for high embedding capacity, in addition, these methods are able to maintain the robustness of modern steganalysis at lower embedding rates.

In this experiment, we employed the second-order Markov chain SPAM 686 features set for evaluation of embedding robustness. To prove unbiased experiments, we designed and tested two types of evaluation using WEKA (Hall et al., 2009) tool. First testing type denoted as E1, which employ the 10-fold cross validation mechanism of WEKA tool. In which, respective SPAM features of cover and stego-images are divided into 10 times for randomly employing its training and testing procedure. Secondly, we evaluated the SPAM features of the cover and stego-images with general training and testing procedure denoted as E2. The UCID image dataset (Schaefer & Stich, 2004) are used for evaluation purpose, in which first 500 randomly selected cover and its corresponding stego-images used for training and rest of 500 cover and respective stego-images used for testing based of SPAM features. The classification errors rates in percentages of proposed RMDR and compared steganographic methods on various embedding rates (from 0.05 to 0.40 bpp) listed in Table 4.7.

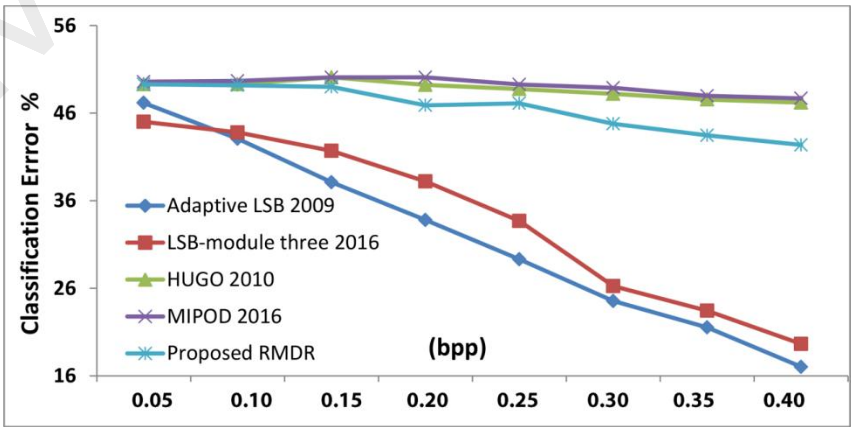
Table 4.7: Undetectability Performance under SPAM Steganalysis with Ensemble Classifier for the Proposed and Compared Methods

Embedding Method	**Testing Type**	**Classification Errors % based on Various bpp**							
		0.05	**0.10**	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**
Adaptive LSB (H. Yang et al., 2009)	E1	91.23	86.35	82.12	81.28	73.74	64.92	61.16	52.24
LSB-module-three (Xu et al., 2016)		90.41	86.49	82.31	81.05	73.92	65.19	61.39	52.19
HUGO (Pevný et al., 2010)		94.30	94.00	94.00	94.60	93.62	93.42	92.28	92.03
MIPOD (Sedighi et al., 2016)		94.10	94.00	94.70	93.90	93.53	92.40	91.02	91.54
Proposed RMDR T= Ṝ		94.89	94.89	94.21	94.18	90.74	89.97	85.68	89.46
Adaptive LSB (H. Yang et al., 2009)	E2	47.17	43.09	38.12	33.81	29.32	24.56	21.54	17.04
LSB-module-three (Xu et al., 2016)		45.01	43.80	41.70	38.20	33.70	26.25	23.45	19.65
HUGO (Pevný et al., 2010),		49.29	49.31	50.1	49.23	48.76	48.21	47.56	47.21
MIPOD (Sedighi et al., 2016)		49.59	49.69	50.1	50.1	49.28	48.89	47.98	47.69
Proposed RMDR T= Ṝ		49.29	49.19	48.99	46.89	47.12	44.78	43.46	42.37

From Table 4.7, it is easy to observe that the SPAM based classification error rate of the proposed method is throughout higher than both adaptive LSB and LSB-module-three methods and similar to state-of-the-art HUGO and MiPOD methods in both E1 and E2 evaluation cases. For example, when embedding capacity is 0.05 bpp in E1 testing case, the classification error percentage is 94.89, whereas the classification error percentage of adaptive LSB, LSB-module-three, HUGO and MiPOD are at 91.23, 90.41, 94.30 and 94.10, respectively. Similarly, in E2 testing case the classification error percentages is higher than adaptive LSB and LSB-module-three methods. For better understanding, Figure 4.14 depicts the classification errors in a graph form of SPAM based steganalysis under E1 and E1 types of experiments. It is obviously to conclude that proposed method maintains the similar classification error rate or has the similar robustness to state-of-the-art HUGO (Pevný et al., 2010) and MiPOD (Sedighi et al., 2016) methods at a lower embedding rates.



(a) SPAM Based Robustness of ‘E1’ Type Evaluation



(b) SPAM Based Robustness of ‘E2’ Type Evaluation

Figure 4.14: SPAM feature based Classification Error Rate Graphs for RMDR and Compared Methods

4.2 RMDR-based Adaptive Hybrid Steganography Method

The proposed hybrid embedding method concurrently utilized the digits and bits characteristics of pixels values to hide the secret data that confuse the statistical structural/statistical steganalysis techniques. In this section, a RMDR-based adaptive hybrid steganography method is proposed, that is based on two steganographic techniques, namely, RMDR (section 4.1) and adaptive LSB (H. Yang et al., 2009) embedding methods. In this hybrid approach, RMDR employed for high visual quality and undetectability, while adaptive LSB is utilized to achieve the high embedding capacity. The proposed hybrid technique based on the concept that higher texture areas can tolerate larger changes than the smooth area. Similar to the PVD (D.-C. Wu & Tsai, 2003) method, we employ the simple difference strategy to determine the regions i.e. lower and higher texture areas of an image, where these texture regions are used to determine the selection of best embedding process. The proposed method consists of two main phases, the embedding and extracting, which described in the subsections below.

4.2.1 RMDR-based Adaptive Hybrid Embedding Method

In embedding phase, proposed method employed the concept of texture regions inspired by (H-C Wu et al., 2005) i.e. region-1 and region-2, where these regions represent the basic lower and higher texture areas of an image. The secret data bits embedded by using RMDR and adaptive LSB embedding techniques. The selection of RMDR and adaptive LSB embedding depends on selected region level. After selecting the embedding algorithm the proposed method adaptively, determine the number of secret bits for embedding process. To estimate the exact number of secret data bits, we designed a range table R_i with continuous ranges from 0 to 255, where i denotes the number of sub-levels as shown in Table 4.8. The $R_i \in [l_i, u_i\ ]$ where l_i is the lower bound of R_i, and u_i is the upper bound of R_i. The range table R_i has four ranges $R_1 \in [0, 31]$, $R_2 \in$

[32, 63], R_3 ϵ [64, 127], and R_1 ϵ [128, 255]. In Table 4.8, the second row represents the pre-estimated number of secret bits. For example, the R_1 range exists under region-1 thus the 3 secret data bits will be employed in each pixel for embedding purpose. Furthermore, these ranges can be dynamically generated or depending on the application requirement. From experiments, we found the best regions with ranges as shown in Table 4.8, while it also meets the optimal steganography objectives for proposed method.

Table 4.8: Proposed RMDR-based Hybrid Embedding Method Range Table Divisions as Region-1 and Region-2 Levels, where *k* denotes the no. of Least Bits for Substitution

Regions	**Region-1 Level**	**Region-2 Level**		
Lower-Upper bound of *Ri*	$R_1 \epsilon [0, 31]$	$R_2 \epsilon [32, 63]$	$R_3 \epsilon [64, 127]$	$R_4 \epsilon [128, 255]$
Secret bits	3	k=4= $\log_2(63-32)-1$	k =5 = $\log_2(127-64)-1$	k = 6 = $\log_2(225-128)-1$

The basic flow diagram of proposed RMDR-based hybrid embedding method showed in Figure 4.15, and further the detailed embedding steps discussed in Table 4.9. The proposed hybrid method partitioned the cover image into two non-overlapped consecutive (horizontal) pixels blocks i.e., *block* = (p_0, p_1). Furthermore, the pixel difference d = *abs* ($p_0 - p_1$) of each block is used to determine the region level of the block, as shown in step 3 of Table 4.9. The pixels difference blocks that belongs to region-1 and region-2 employed by the RMDR (section 4.1) and k-bit LSB embedding methods, respectively. In ideal condition, after embedding process, the cover and stego-pixels blocks range level must be identical. Therefore, a range level readjustment process is required to maintain the identical range levels of cover and stego-pixels. This range level readjustment process described in next section (a). Finally, the stego-pixels of both embedding methods arranged to its respective location to form a complete stego-image.

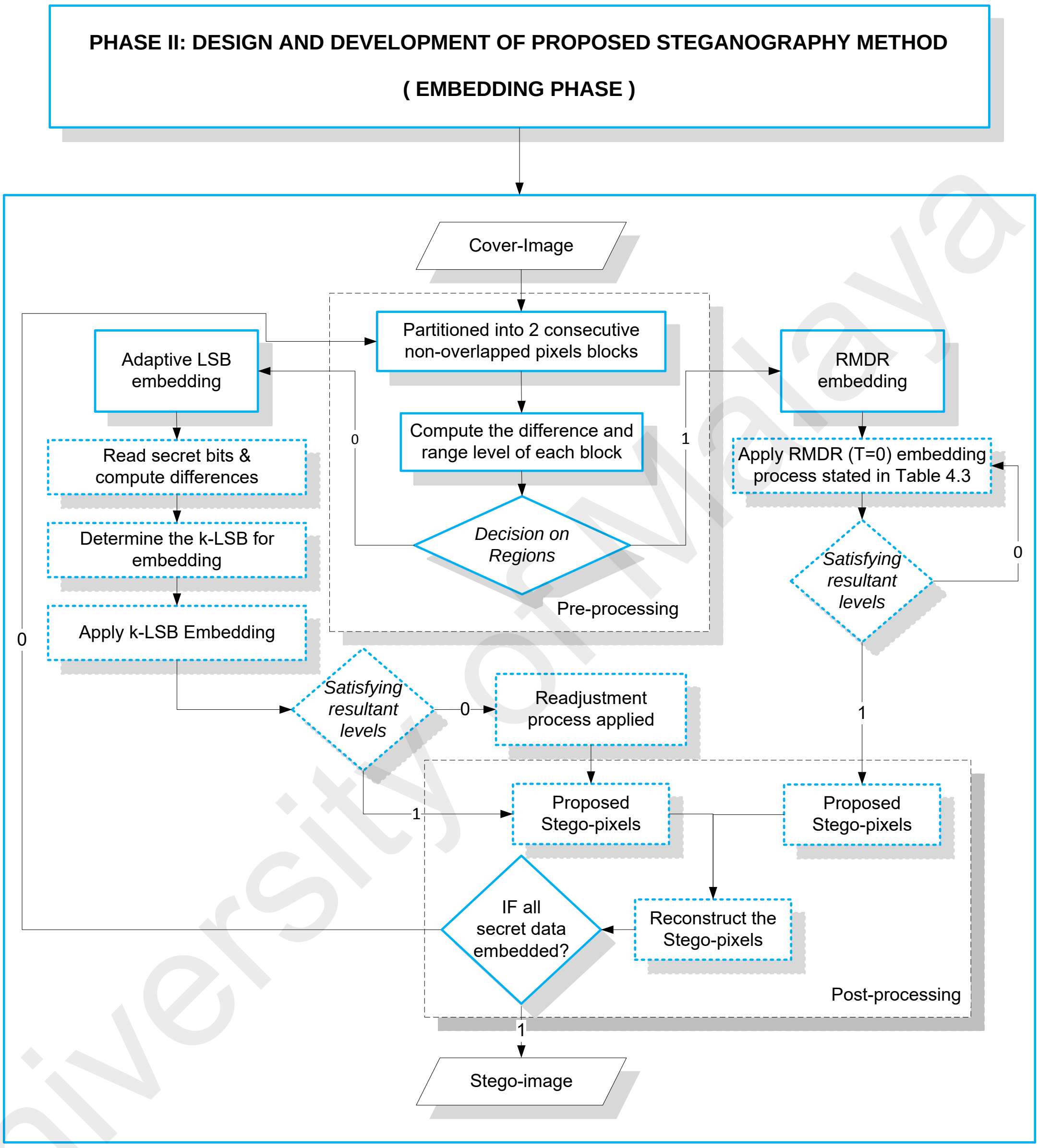
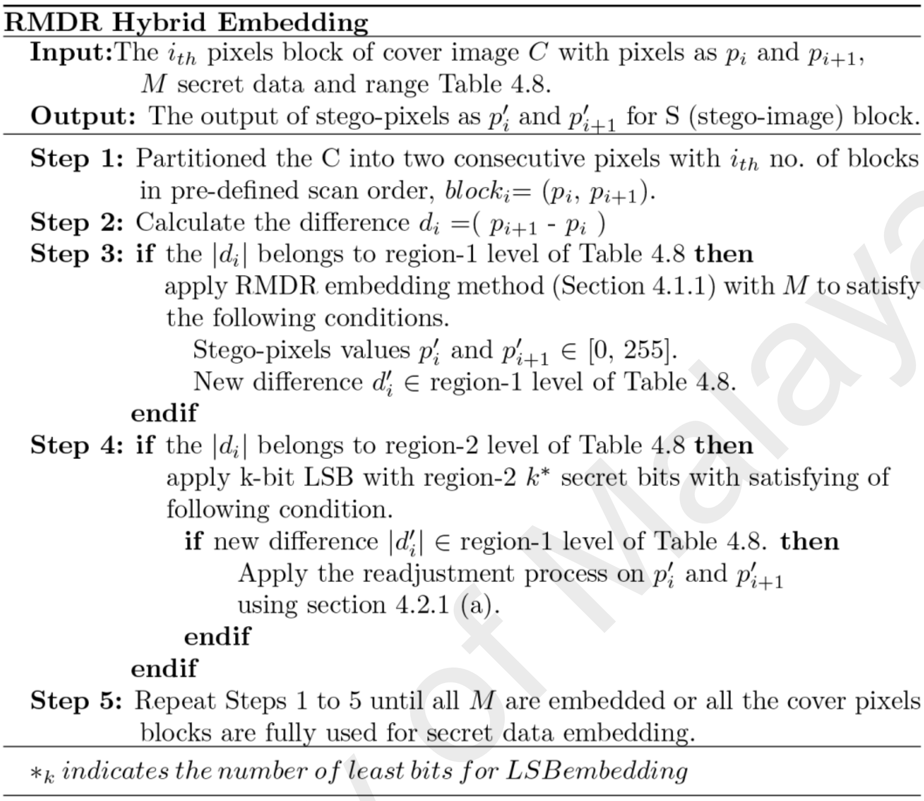

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EMBEDDING PHASE)
Cover-Image
Partitioned into 2 consecutive non-overlapped pixels blocks
Compute the difference and range level of each block
Decision on Regions
Pre-processing
0
1
Adaptive LSB embedding
Read secret bits & compute differences
Determine the k-LSB for embedding
Apply k-LSB Embedding
Satisfying resultant levels
0
1
Readjustment process applied
RMDR embedding
Apply RMDR (T=0) embedding process stated in Table 4.3
Satisfying resultant levels
0
1
Proposed Stego-pixels
Proposed Stego-pixels
Reconstruct the Stego-pixels
IF all secret data embedded?
0
1
Post-processing
Stego-image

Figure 4.15: Basic Flow Diagram of Proposed RMDR-based Hybrid Embedding Method

Table 4.9: Proposed RMDR-based Hybrid Embedding Steps



```
RMDR Hybrid Embedding
  Input: The $i_{th}$ pixels block of cover image $C$ with pixels as $p_i$ and $p_{i+1}$,
         $M$ secret data and range Table 4.8.
  Output: The output of stego-pixels as $p'_i$ and $p'_{i+1}$ for S (stego-image) block.

  Step 1: Partitioned the C into two consecutive pixels with $i_{th}$ no. of blocks
          in pre-defined scan order, $block_i$= ($p_i$, $p_{i+1}$).
  Step 2: Calculate the difference $d_i$ =( $p_{i+1}$ - $p_i$ )
  Step 3: if the $|d_i|$ belongs to region-1 level of Table 4.8 then
             apply RMDR embedding method (Section 4.1.1) with $M$ to satisfy
             the following conditions.
                Stego-pixels values $p'_i$ and $p'_{i+1} \in$ [0, 255].
                New difference $d'_i \in$ region-1 level of Table 4.8.
          endif
  Step 4: if the $|d_i|$ belongs to region-2 level of Table 4.8 then
             apply k-bit LSB with region-2 $k^*$ secret bits with satisfying of
             following condition.
               if new difference $|d'_i| \in$ region-1 level of Table 4.8. then
                   Apply the readjustment process on $p'_i$ and $p'_{i+1}$
                   using section 4.2.1 (a).
               endif
          endif
  Step 5: Repeat Steps 1 to 5 until all $M$ are embedded or all the cover pixels
          blocks are fully used for secret data embedding.
  $*_k$ indicates the number of least bits for LSBembedding
```

(a) ***Readjustment for Region Inconsistent Pixels Block***

However, from the experimental results, we found that some stego-blocks of region-2 switched to region-1 during the k-LSB embedding process. Therefore, the proposed extraction process failed to recover the 100% of the secret bits. For example, (p_0, p_1) = (146, 178) and secret bits are (1010 0010), where its difference d = |32|, belongs to region-2 of Table 4.8. Therefore, region-2 employed the adaptive LSB embedding and extraction process with k-bit as k=4 due to R_2 range level. After applying 4-bit LSB embedding, the stego-block values are (p'_0, p'_1) = (154, 178), and the new difference becomes d' = |24|, where this stego-block loses its region consistency from region-2 to region-1. As result, adaptive LSB based block of region-2 would be considered as the RMDR based block of region-1. In addition, during the extraction process, it is impossible to recover the 100% original secret data from stego-image due to region inconsistency problem in stego-blocks. Therefore, a readjustment process stated in Table 4.10 is applied on the adaptive LSB based stego-block (p'_0, p'_1) when a region inconsistency problem occurs. This readjustment process computes the new stego-block (p'_0, p'_1) while maintains the region's consistency and retains the secret data inside stego-block. After readjustment process, the resultant stego-block values are (p'_0, p'_1) = (138, 178) with the new d' = |40| that belongs to region-2 of Table 4.8, and this ensures the 100% of the secret data recovery through extraction process.

This readjustment process consists of two phases as shown in Table 4.10, first computes the expected number of modified pixels of region-2 blocks, further it finds the error differences against the cover pixels. Second, choose the pixel pair that belongs to region-2 with minimum difference error. In addition, this readjustment process helps to reduce the differences between cover and stego-pixels, which indirectly reduce the distortion of stego-image. Furthermore, Figure 4.16 represents the detail example of readjustment process for a region inconsistent block.

Table 4.10: Readjustment Process for Region Inconsistent Blocks

```
Phases 1

1: Compute the expected modified values of $p'_0$ and $p'_1$.
        $p''_0 = p'_0 + 2^k$
        $p'''_0 = p'_0 - 2^k$
        $p''_0 = p'_1 + 2^k$
        $p'''_0 = p'_1 - 2^k$
2: Compute the below following with difference errors i.e. $error_1$, $error_2$ ...
     $error_8$, that satisfy the regions (range levels) of Table 4.8.
     Case 1: $(p'_0, p''_1)$
        if abs($p'_0$ - $p''_1$) $\in$ region-2 then
           $error_1$ = abs ($p_0$ - $p'_0$) + abs ($p_1$ - $p''_1$)
        endif
     Case 2: $(p'_0, p'''_1)$
        if abs($p'_0$ - $p'''_1$) $\in$ region-2 then
           $error_2$ = abs ($p_0$ - $p'_0$) + abs ($p_1$ - $p'''_1$)
        endif
     Case 3: $(p'_0, p'_1)$
        if abs($p'_0$ - $p'_1$) $\in$ region-2 then
           $error_3$ = abs ($p_0$ - $p'_0$) + abs ($p_1$ - $p'_1$)
        endif
     Case 4: $(p''_0, p''_1)$
        if abs($p''_0$ - $p''_1$) $\in$ region-2 then
           $error_4$ = abs ($p_0$ - $p''_0$) + abs ($p_1$ - $p''_1$)
        endif
     Case 5: $(p''_0, p'''_1)$
        if abs($p''_0$ - $p'''_1$) $\in$ region-2 then
           $error_5$ = abs ($p_0$ - $p''_0$) + abs ($p_1$ - $p'''_1$)
        endif
     Case 6: $(p'''_0, p'_1)$
        if abs($p'''_0$ - $p'_1$) $\in$ region-2 then
           $error_6$ = abs ($p_0$ - $p'''_0$) + abs ($p_1$ - $p'_1$)
        endif
     Case 7: $(p'''_0, p''_1)$
        if abs($p'''_0$ - $p''_1$) $\in$ region-2 then
           $error_7$ = abs ($p_0$ - $p'''_0$) + abs ($p_1$ - $p''_1$)
        endif
     Case 8: $(p'''_0, p'''_1)$
        if abs($p'''_0$ - $p'''_1$) $\in$ region-2 then
           $error_8$ = abs ($p_0$ - $p'''_0$) + abs ($p_1$ - $p'''_1$)
        endif

Phases 2

1: Select the best pixels pair that has minimum difference error and belongs
     to region-2.
     $(p^*_0 , p^*_1)$ = Select the minimum difference error pair from all cases
        pixel pairs.
        if $(p^*_0 , p^*_1) \in$ region-2 then
           $(p'_0 , p'_1) = (p^*_0 , p^*_1)$ [1]
        elseif
           Repeat this step for remaining second, third and up to eight
           cases until the pair satisfies the minimum difference
           errors pair that $\in$ region-2.
        endif
```

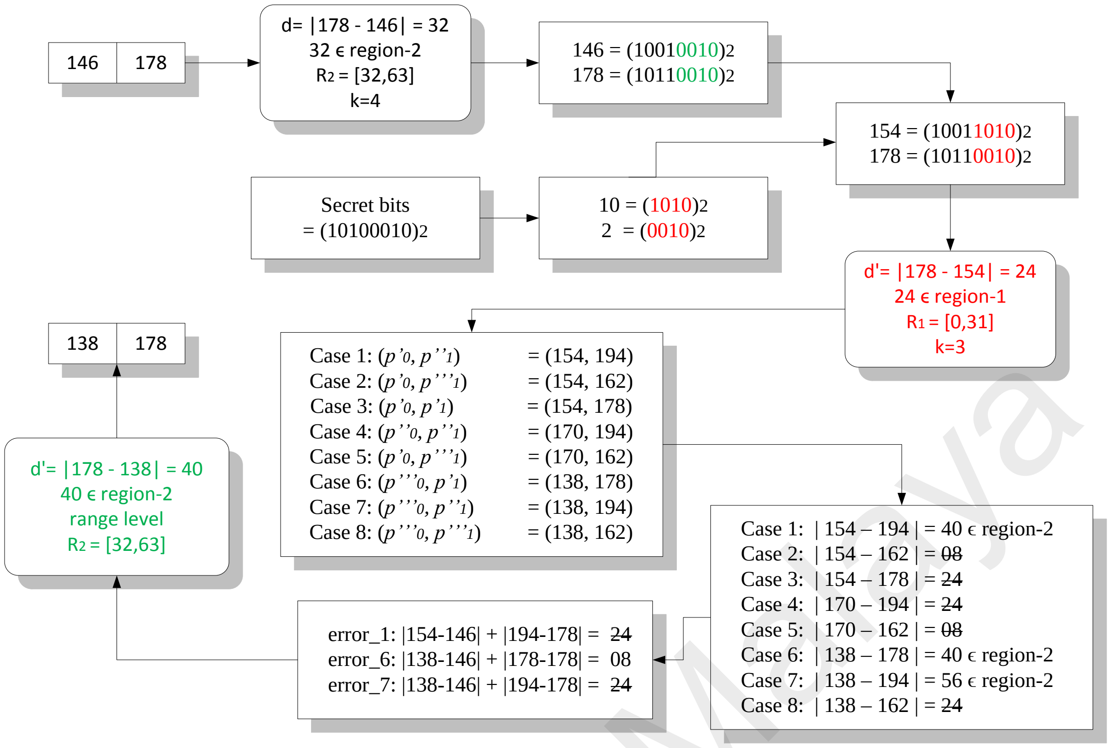

146
178
d= |178 - 146| = 32
32 ϵ region-2
R2 = [32,63]
k=4
146 = (10010010)2
178 = (10110010)2
154 = (10011010)2
178 = (10110010)2
Secret bits
= (10100010)2
10 = (1010)2
2 = (0010)2
d'= |178 - 154| = 24
24 ϵ region-1
R1 = [0,31]
k=3
138
178
Case 1: (p'0, p''1) = (154, 194)
Case 2: (p'0, p'''1) = (154, 162)
Case 3: (p'0, p'1) = (154, 178)
Case 4: (p''0, p''1) = (170, 194)
Case 5: (p'0, p'''1) = (170, 162)
Case 6: (p'''0, p'1) = (138, 178)
Case 7: (p'''0, p''1) = (138, 194)
Case 8: (p'''0, p'''1) = (138, 162)
d'= |178 - 138| = 40
40 ϵ region-2
range level
R2 = [32,63]
Case 1: | 154 – 194 | = 40 ϵ region-2
Case 2: | 154 – 162 | = ~~08~~
Case 3: | 154 – 178 | = ~~24~~
Case 4: | 170 – 194 | = ~~24~~
Case 5: | 170 – 162 | = ~~08~~
Case 6: | 138 – 178 | = 40 ϵ region-2
Case 7: | 138 – 194 | = 56 ϵ region-2
Case 8: | 138 – 162 | = ~~24~~
error_1: |154-146| + |194-178| = ~~24~~
error_6: |138-146| + |178-178| = 08
error_7: |138-146| + |194-178| = ~~24~~

Figure 4.16: An Example of Embedding and Readjustment Process for Region-2 Block

4.2.2 RMDR-based Adaptive Hybrid Extracting Method

In extraction process, this requires the stego-image as input and range table division. Similar to the embedding process, the stego-image *S* partitioned into two consecutive non-overlapped pixel blocks, i.e., *block* = (p'_0, p'_1). If the difference of block *d* = *abs* ($p'_0 - p'_1$) value exists in the region-1 level (of Table 4.8), the RMDR extraction (section 4.1.2) is employed. Conversely, the k-bit LSB extraction is applied on that block. The basic block diagram of RMDR-based hybrid extracting procedure and its algorithm steps are shown in Figure 4.17 and Table 4.11, respectively.

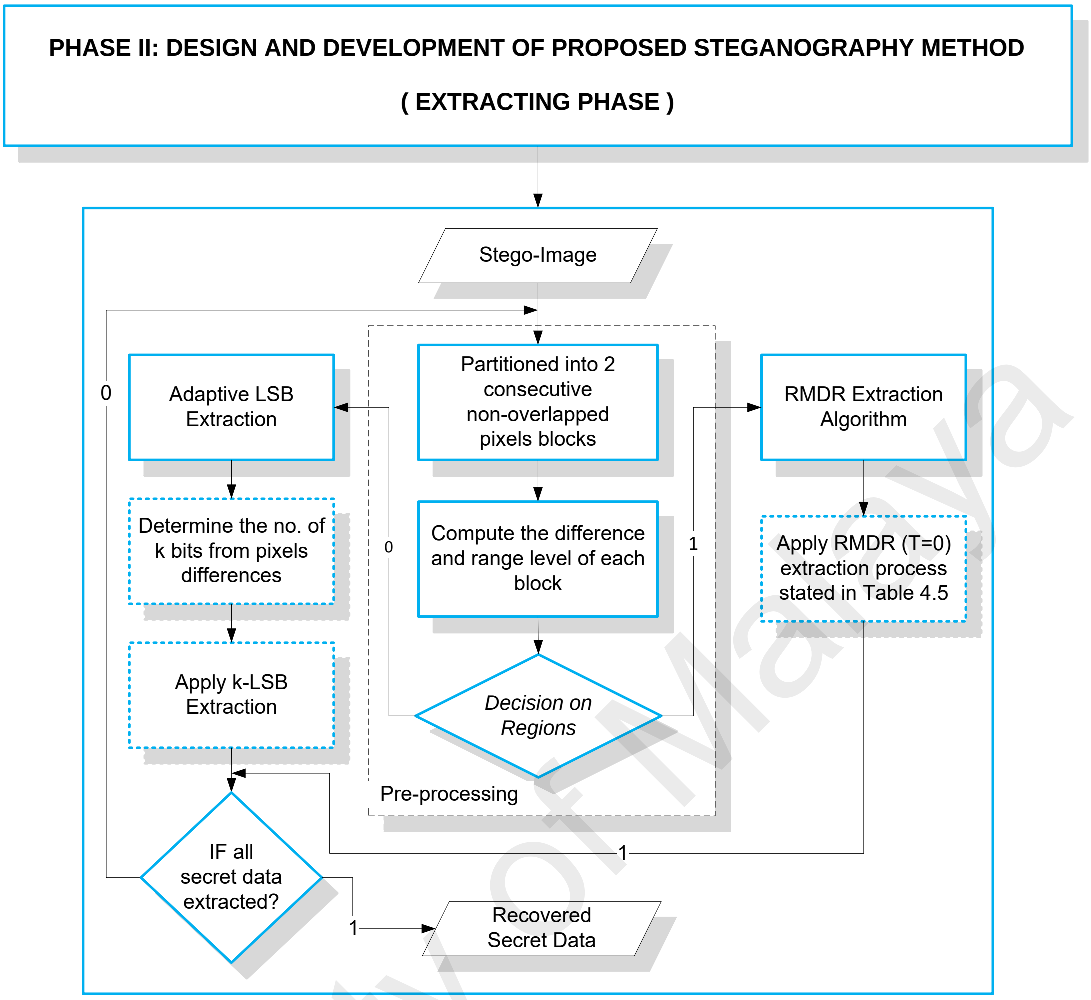

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EXTRACTING PHASE)
Stego-Image
Partitioned into 2 consecutive non-overlapped pixels blocks
Adaptive LSB Extraction
RMDR Extraction Algorithm
0
1
0
Determine the no. of k bits from pixels differences
Compute the difference and range level of each block
Apply RMDR (T=0) extraction process stated in Table 4.5
Apply k-LSB Extraction
Decision on Regions
Pre-processing
1
IF all secret data extracted?
1
Recovered Secret Data

Figure 4.17: The Basic Flow Diagram of Proposed RMDR-based Hybrid Extraction Process

Table 4.11: Proposed RMDR-based Hybrid Extracting Steps

```
RMDR Hybrid Extracting Steps
  Input: The $i_{th}$ block of $S$ (stego-image) with pixels denoted as $p'_i$ , $p'_{i+1}$
         and Table 4.8 for range and region level decision
  Output: Recovered secret bit stream.
  Step 1: Partitioned $S$ into two consecutive pixels with i no. of blocks
          in predefined scan order, $block_i$= ($p'_i$, $p'_{i+1}$).
  Step 2: Calculate the difference $d'_i$ =( $p'_{i+1}$ - $p'_i$ )
  Step 3: If the $|d'_i|$ belongs to region-1 level of Table 4.8 then
            apply RMDR extraction method (section 4.1.2)
          else
            apply the k-bit LSB extraction using Table 4.8 with k secret bits.
          endif
  Step 4: Repeat Steps 1 to 4 until the all secret bits are extracted from $S$.
```

4.2.3 Experimental Results and Analysis

In this section, we will evaluate the performance of the proposed RMDR-based hybrid steganography method. For performance analysis, we will follow the identical RDMR experimental (section 4.1.3) evaluation metrics to measure the embedding capacity, visual quality and security. Furthermore, for image dataset, both UCID (Schaefer & Stich, 2004) and USC-SIPI (USC-SIPI, 2016) databases are employed. For secret data, a pseudo-random number generator used to generate the secret bits.

4.2.3.1 Embedding Capacity and Visual Quality Evaluation

In this section, first the performance of the proposed RMDR-based hybrid steganography method evaluated with existing singular steganographic approaches. Secondly, performance measured with well-known LSB and PVD-based hybrid methods. Similar to RMDR section (4.1.3.2), various quality measures are considered and even with different embedding rates, we will follow the same pattern to evaluate the performance of proposed hybrid technique. Finally, the performances on various texture-based images are measured on larger datasets i.e. UCID and USC-SIPI databases.

(a) ***Performance of Embedding Capacity and Visual Quality***

This section analyzes the performance of hidden capacity and visual quality of proposed and existing hybrid embedding methods in two parts. First, compared the proposed RMDR-based hybrid method with existing well-known singular steganographic methods i.e., LSB, PVD, adaptive LSB (D.-C. Wu & Tsai, 2003; H. Yang et al., 2009) as shown in Table 4.12. Secondly, the proposed method compared with existing LSB and PVD-based hybrid embedding i.e. (M Khodaei & Faez, 2012; H-C Wu et al., 2005; K. Wu et al., 2015; C.-H. Yang, Weng, et al., 2010) methods as stated in Table 4.13.

Table 4.12: Performance Comparison of Proposed RMDR-based Hybrid and Existing Singular Steganography Methods

Images	3-bit LSB				(D.-C. Wu & Tsai, 2003) PVD				(H. Yang et al., 2009) Adaptive LSB				RMDR-based Hybrid Method			
	Capacity	PSNR	Q	RMSE	Capacity	PSNR	Q	RMSE	Capacity	PSNR	Q	RMSE	Capacity	PSNR	Q	RMSE
Lena	786,429	37.92	0.9977	3.24	409,779	41.14	0.9989	2.24	757,332	39.31	0.9978	2.76	793,810	39.40	0.9984	2.73
Baboon	786,429	37.91	0.9971	3.24	456,953	36.98	0.9964	3.61	785,572	39.16	0.9972	2.82	820,774	38.40	0.9974	3.07
Pepper	786,429	37.91	0.9982	3.24	405,425	41.55	0.9992	2.13	786,014	39.06	0.9983	2.73	792,384	39.49	0.9987	2.71
Jet	786,429	37.98	0.9976	3.22	409,531	40.42	0.9986	2.43	735,236	39.55	0.9977	2.76	795,726	39.35	0.9983	2.75
Tank	786,429	37.85	0.9928	3.27	403,990	42.38	0.9975	1.94	784,019	39.03	0.9930	2.78	788,884	39.56	0.9951	2.68
Airplane	786,429	37.70	0.9889	3.32	397,904	42.19	0.9960	1.98	773,101	39.09	0.9890	2.84	799,482	39.55	0.9927	2.68
Truck	786,429	37.83	0.9928	3.27	400,504	42.87	0.9977	1.83	775,572	39.15	0.9931	2.79	799,958	39.67	0.9952	2.65
Elaine	786,429	37.89	0.9975	3.25	408,582	41.88	0.9990	2.05	761,204	39.32	0.9985	2.83	798,204	39.63	0.9983	2.66
Couple	786,429	37.91	0.9973	3.24	419,901	39.78	0.9983	2.62	756,019	39.06	0.9974	2.81	811,556	39.07	0.9980	2.84
Boat	786,429	37.94	0.9976	3.23	419,317	39.52	0.9983	2.69	755,528	39.04	0.9986	2.86	800,042	39.19	0.9982	2.80
Tiffany	786,429	37.91	0.9939	3.25	398,980	41.48	0.9973	2.15	777,888	39.12	0.9941	2.89	799,862	39.36	0.9956	2.74
Lake	786,429	37.91	0.9988	3.24	421,819	39.75	0.9992	2.62	750,013	39.01	0.9986	2.87	799,930	39.15	0.9991	2.81
Average	786,429	37.89	0.9959	3.25	412,724	40.83	0.9980	2.36	766,458	39.16	0.9961	2.81	**800,051**	**39.32**	**0.9971**	**2.76**

Table 4.13: Performance Comparison of Proposed RMDR-based Hybrid and Existing LSB-based Hybrid Steganography Methods

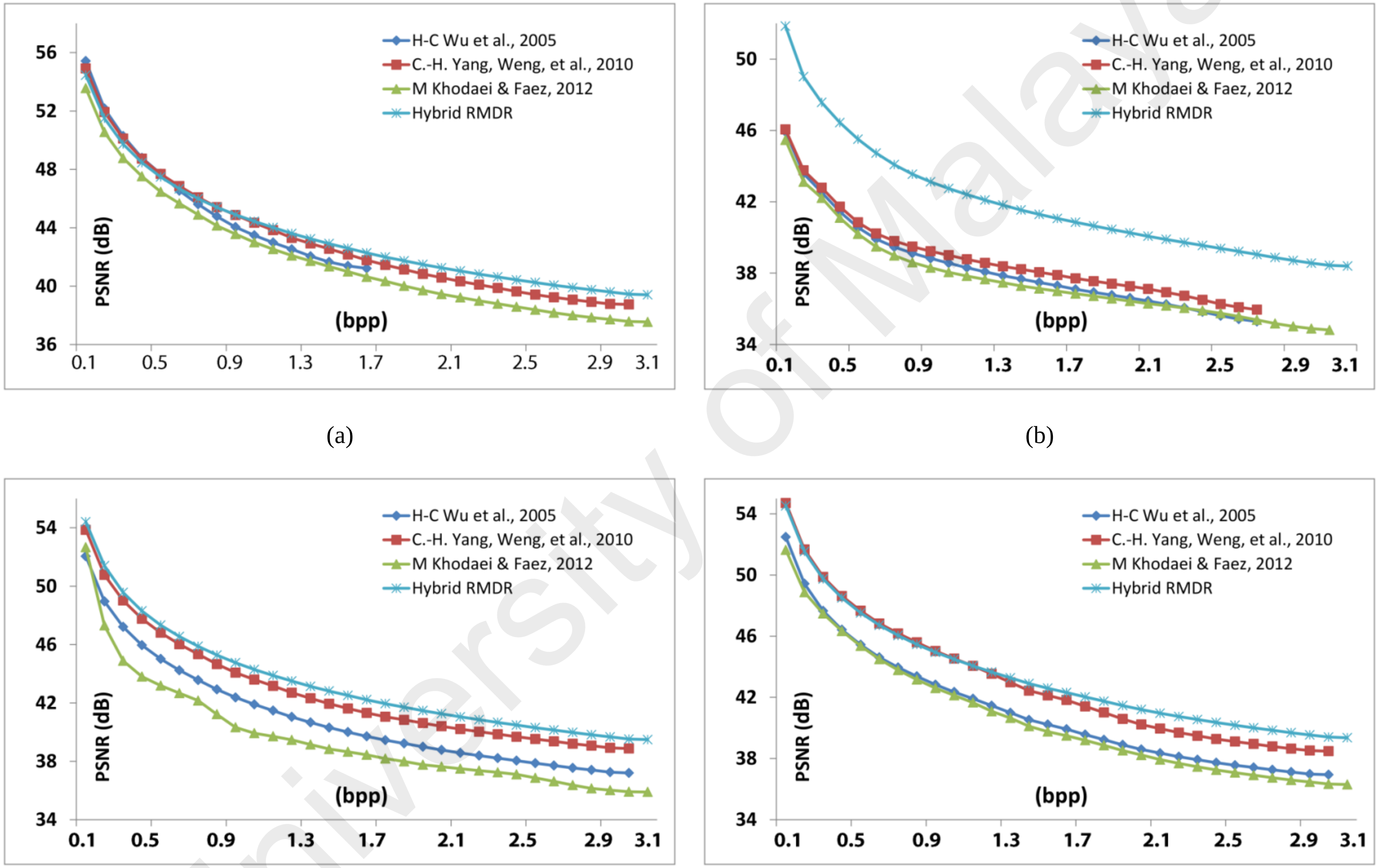
Images	**(H-C Wu et al., 2005)**			**(C.-H. Yang, Weng, et al., 2010)**			**(M Khodaei & Faez, 2012)**			**(K. Wu et al., 2015)**			**RMDR-based Hybrid**		
	LSB + PVD			**LSB+PVD**			**LSB + PVD T =1 *k*=3**			**LSB+EMD+MPE**			**Method**		
	Capacity	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**
Lena	765,969	37.12	0.9973	765,969	38.91	0.9982	791443	37.56	0.9975	639,761	35.10	0.9959	793,810	39.40	0.9984
Baboon	717,749	35.30	0.9947	717,749	36.19	0.9957	809435	34.85	0.9940	603,894	35.10	0.9948	820,774	38.40	0.9974
Pepper	768,455	37.20	0.9979	768,455	39.05	0.9986	790299	35.88	0.9971	620,920	35.10	0.9967	792,384	39.49	0.9987
Jet	770,176	36.98	0.9970	770,176	38.65	0.9979	792443	36.29	0.9965	650,362	35.10	0.9957	795,726	39.35	0.9983
Tank	768,709	37.41	0.9920	768,709	39.52	0.9951	788107	38.36	0.9936	627,602	35.10	0.9874	788,884	39.56	0.9951
Airplane	782,309	37.38	0.9881	782,309	39.68	0.9929	788227	38.29	0.9903	655,846	35.10	0.9813	799,482	39.55	0.9927
Truck	773,407	37.53	0.9923	773,407	39.81	0.9954	787157	38.61	0.9939	635,396	35.10	0.9876	799,958	39.67	0.9952
Elaine	760,170	37.28	0.9971	760,170	39.26	0.9982	788356	38.17	0.9977	615,116	35.10	0.9956	798,204	39.63	0.9983
Couple	754,155	36.63	0.9964	754,155	38.08	0.9974	795729	36.63	0.9964	632,722	35.10	0.9953	811,556	39.07	0.9980
Boat	754,999	36.50	0.9967	754,999	37.93	0.9976	795458	34.93	0.9952	622,261	35.10	0.9957	800,042	39.19	0.9982
Tiffany	766,663	37.25	0.9929	766,663	39.11	0.9954	790503	37.78	0.9937	643,305	35.10	0.9893	799,862	39.36	0.9956
Lake	750,313	36.62	0.9984	750,313	38.14	0.9988	795471	36.36	0.9983	616,261	35.10	0.9978	799,930	39.15	0.9991
Average	761,090	36.93	0.9951	761,090	38.69	0.9968	792,719	36.98	0.9953	630,287	35.10	0.9927	**800,051**	**39.32**	**0.9971**

In Table 4.12, the results showed that the average embedding capacity of proposed method is 3.05bpp, that is higher than the all compared (D.-C. Wu & Tsai, 2003; H. Yang et al., 2009) methods. Furthermore, this shows that proposed method has higher PSNR value except the PVD approach, but proposed hybrid method also gained the double embedding capacity with respect to PVD. Similar to PSNR, proposed method has higher universal quality index (Q) and best root mean square error (RMSE) ratio against all compared method except the PVD. In general, proposed method showed the better results against well-known singular compared methods while retaining the average PSNR +39 dB and average embedding payload at 3.05 bpp.

Table 4.13 presents the performance of the payload and imperceptibility of the proposed RMDR-based hybrid and existing well known LSB and PVD-based hybrid methods. This shows that proposed hybrid method gained the higher average embedding capacity (800,051 bits) and PSNR (39.32 dB) value among all the other compared (M Khodaei & Faez, 2012; H-C Wu et al., 2005; K. Wu et al., 2015; C.-H. Yang, Weng, et al., 2010) methods. The reason for higher embedding capacity is to efficiently utilize the LSB method (with adaptive k-bit substitution) based on image texture characteristics. Similarly, the employing of RMDR enhanced the visual quality of stego-images. As result, this experiment shows that the proposed hybrid method improved the embedding capacity and visual quality.

(b) ***Performance of Visual Quality at Various Embedding Capacity Rates***

In this experiment, the performance of visual quality of the proposed RMDR-based hybrid method measured at different embedding rates instead of maximum embedding rate. Figure 4.18 is illustrated the complete embedding range from 0.1 to 3.1 bpp with respective PSNR dB. The x-axis and y-axis represent the embedding bits per pixel (bpp) and PSNR values in dB, respectively.



(a)

(b)

(c)

(d)

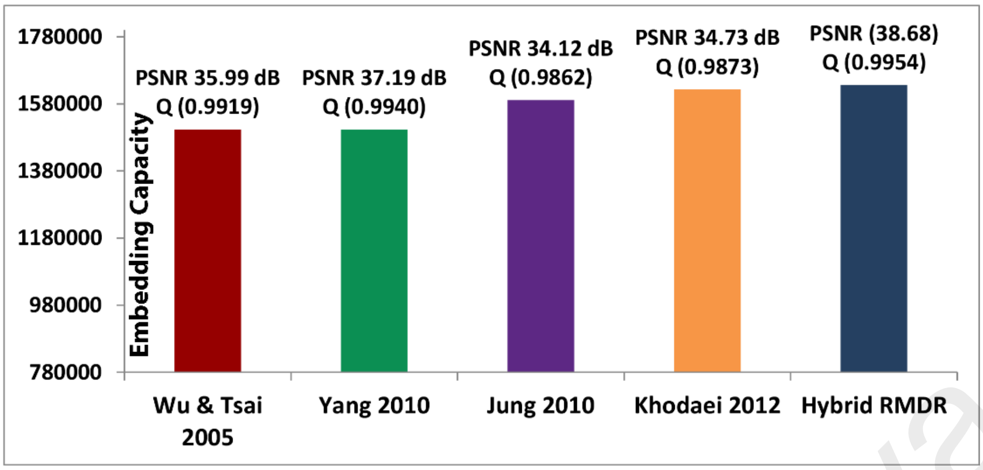
Figure 4.18: PSNR Graph at Various Embedding Rates for (a) Lena, (b) Baboon, (c) Pepper, (d) Jet

From Figure 4.18 (a-d) all graphs depict that proposed hybrid method retains the higher PSNR value at each embedding rate. This concludes that the performance of visual quality in the proposed hybrid method is good and similar to RMDR technique. This also proves that the proposed hybrid method is equally ideal for both types of high and low embedding capacity based applications, even for all types of lower and higher texture based images.

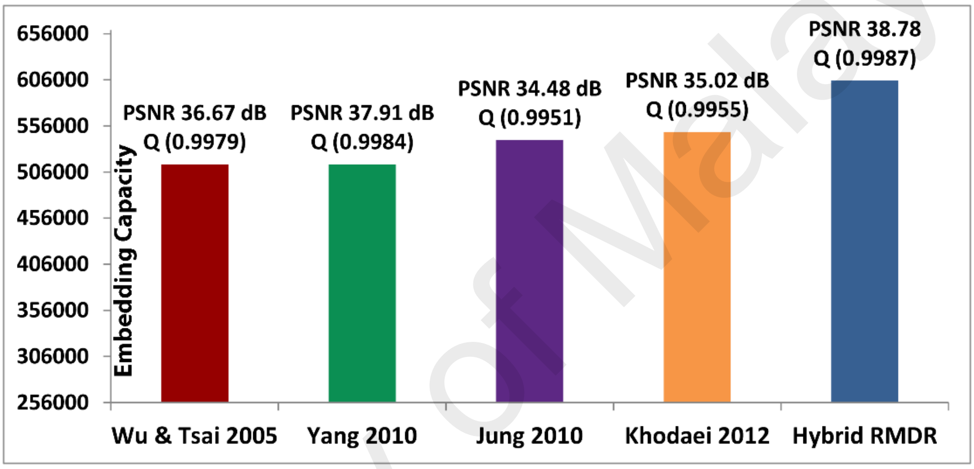
(c) ***Performance over UCID and USC-SIPI Image Datasets***

To obtain the performance of the RMDR-based hybrid method over larger and versatile texture based images, both UCID (Schaefer & Stich, 2004) and SIPI (USC-SIPI, 2016) image datasets are employed for evaluation of its embedding capacity and imperceptibly. In Figure, 4.19 (a) shows the performance of the proposed hybrid method on 144 images of SIPI dataset. Similarly, Figure 4.19 (b) depicts the performance of embedding capacity and visual quality for UCID 1338 images. In Figure 4.19, the x-axis and y-axis represent the steganography methods and embedding bits, respectively.

The proposed hybrid payload for UCID and SIPI datasets are 605,096 and 1,636,102 bits respectively and shows higher than all the other compared LSB-based hybrid methods. Similarly, PSNR dB values for UCID and SIPI datasets are 38.78 and 38.68 dB respectively. The overall results of both graphs depict that the proposed RMDR-based hybrid method retains the higher embedding capacity and higher visual quality in terms of PSNR dB and Q values against existing LSB and PVD-based hybrid methods for larger and well-known datasets.



(a)



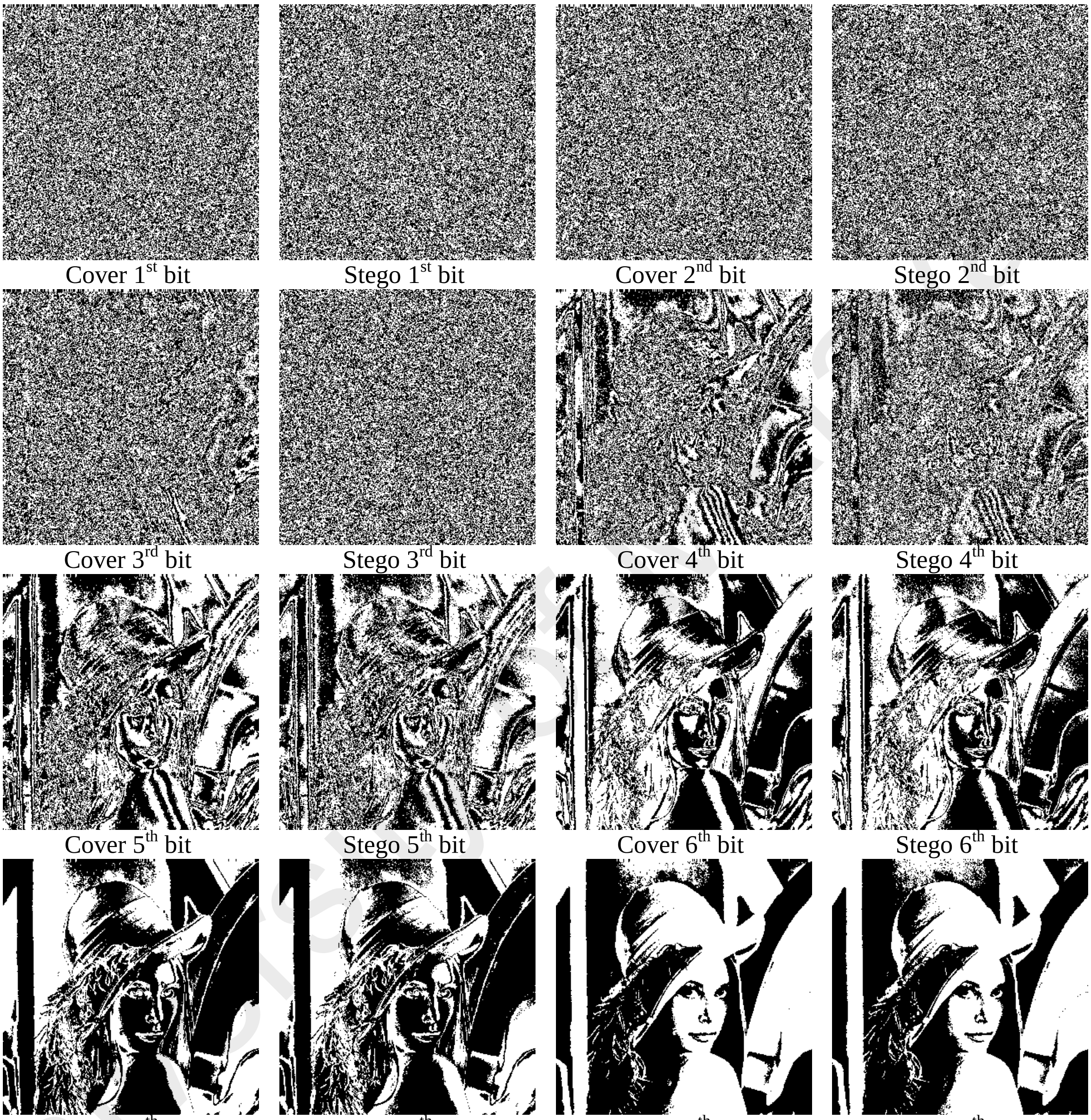
(b)

Figure 4.19: Embedding Capacity with PSNR Performance for (a) SIPI (USC-SIPI, 2016) (b) UCID (Schaefer & Stich, 2004) Datasets

4.2.3.2 Security/Un-detectability Evaluation

(a) ***Bit-plane Analysis***

This experiment presents the bit-plane analysis for the RMDR-based hybrid embedding method as shown in Figure 4.20 to 4.21. In these Figures, the complete 1-8 bit-planes analysis of each image are presented. For example, Figure 4.20 shows the Lena cover and its respective stego-image for all 1 to 8 bit-planes images. Each bit-plane analysis shows that the 'Lena' stego-image is almost similar to respective cover image bit-planes. Similarly, for all other remaining Baboon, Pepper and Jet stego-images, the visual representation of bit-planes are almost identical with respect to its cover-images. This concludes that proposed hybrid stego-images can also resist the visual bit-plane analysis.



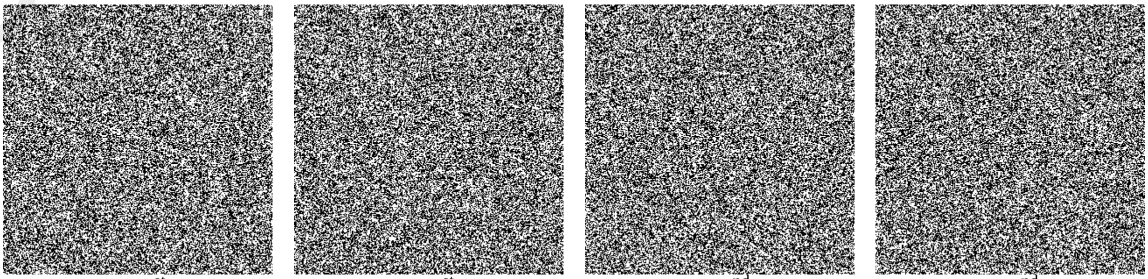
Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit

Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

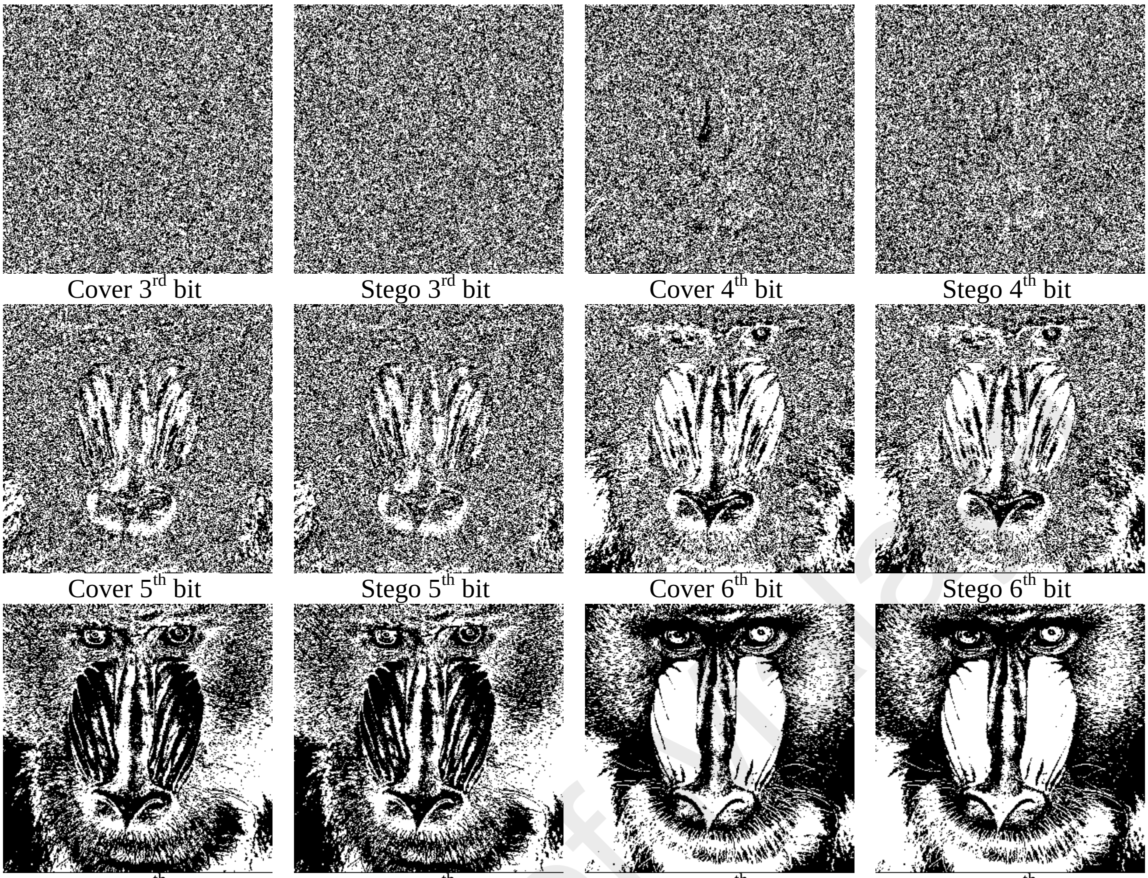
Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.20: Bit-plane Analysis of RMDR-based Hybrid Stego-image (Lena)



Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit



Cover 3rd bit

Stego 3rd bit

Cover 4th bit

Stego 4th bit

Cover 5th bit

Stego 5th bit

Cover 6th bit

Stego 6th bit

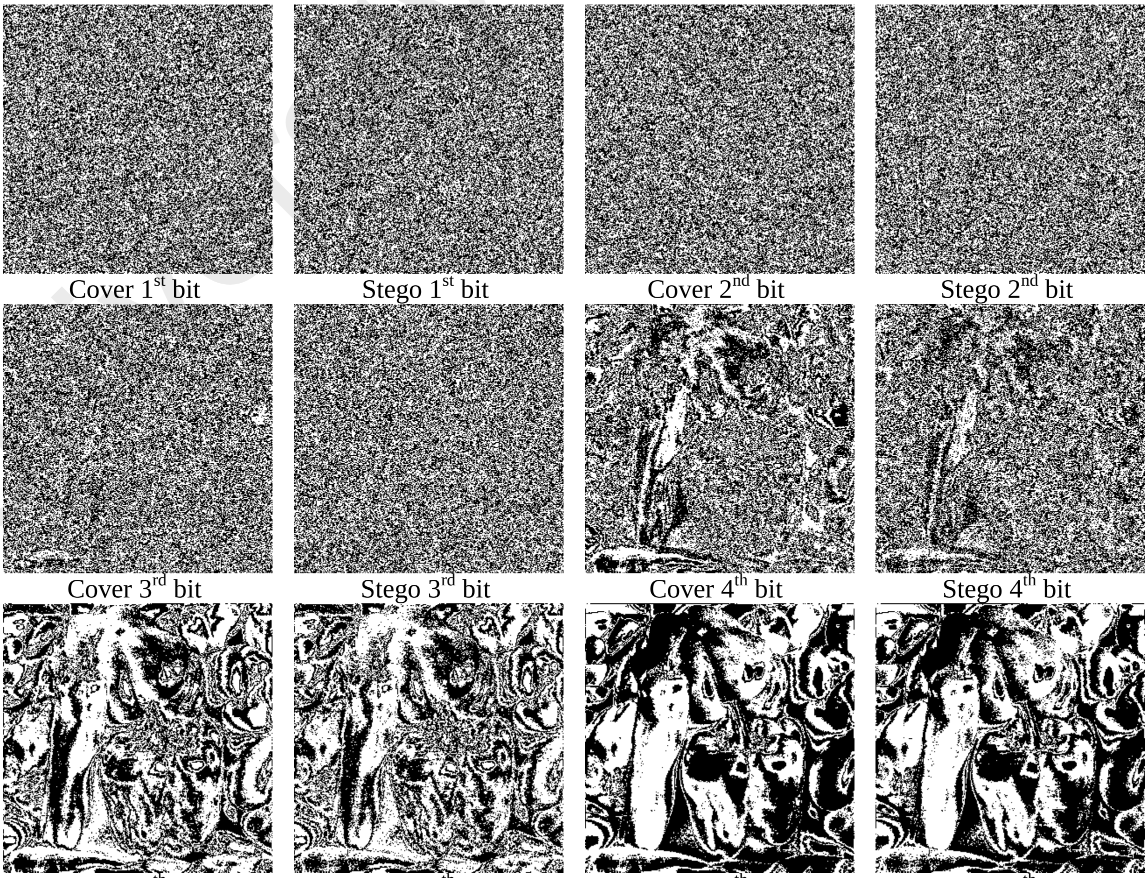
Cover 7th bit

Stego 7th bit

Cover 8th bit

Stego 8th bit

Figure 4.21: Bit-plane Analysis of RMDR-based Hybrid Stego-image (Baboon)



Cover 1st bit

Stego 1st bit

Cover 2nd bit

Stego 2nd bit

Cover 3rd bit

Stego 3rd bit

Cover 4th bit

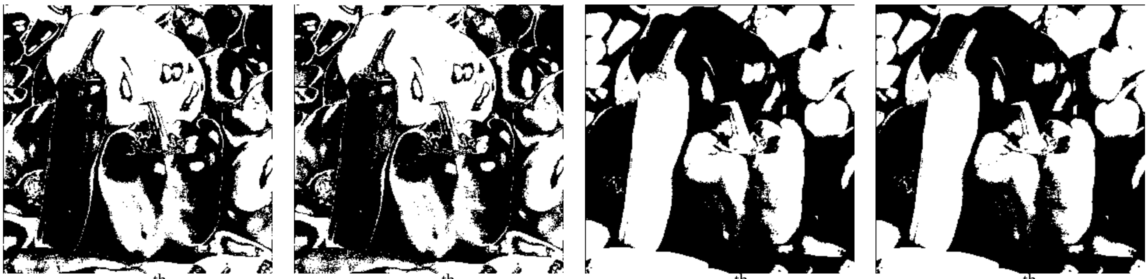
Stego 4th bit

Cover 5th bit

Stego 5th bit

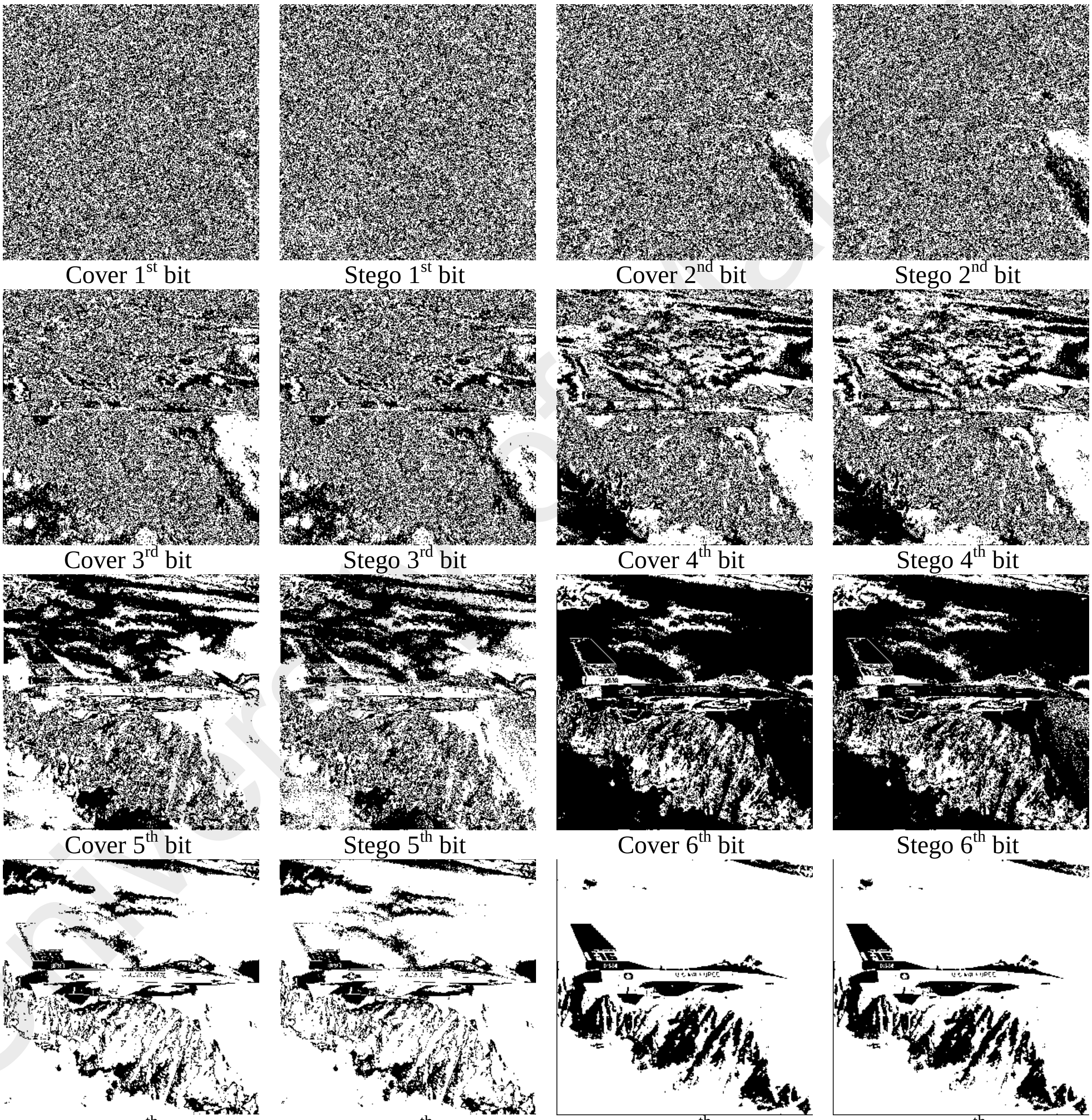
Cover 6th bit

Stego 6th bit



Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.22: Bit-plane Analysis of RMDR-based Hybrid Stego-image (Pepper)



Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit

Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 4.23: Bit-plane Analysis of RMDR-based Hybrid Stego-image (Jet)

Furthermore, the visual distortion artifacts of Lena image for proposed hybrid and existing i.e., classical 3-bit LSB, Khodaei et al, and Wu et al. (M Khodaei & Faez, 2012; K. Wu et al., 2015) methods are illustrated in Figure 4.24. This shows that the RMDR-based hybrid method has less human perceivable differences than compared methods. This is because the proposed method employed the RMDR that has closest pixels selection process for stego-images. Meanwhile, the readjustment process also reduces the stego-image distortion even at higher rate of embedding, because it selects the stego-pixels that have minimum error differences against respective cover-pixels.

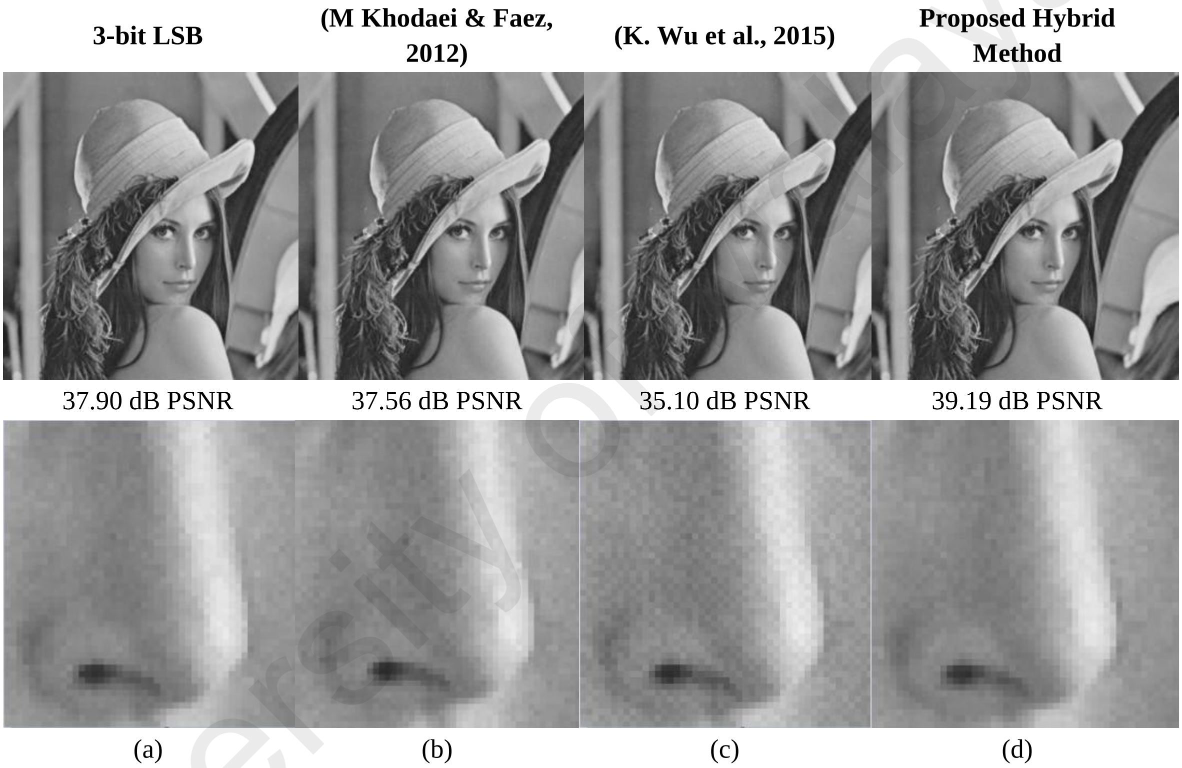
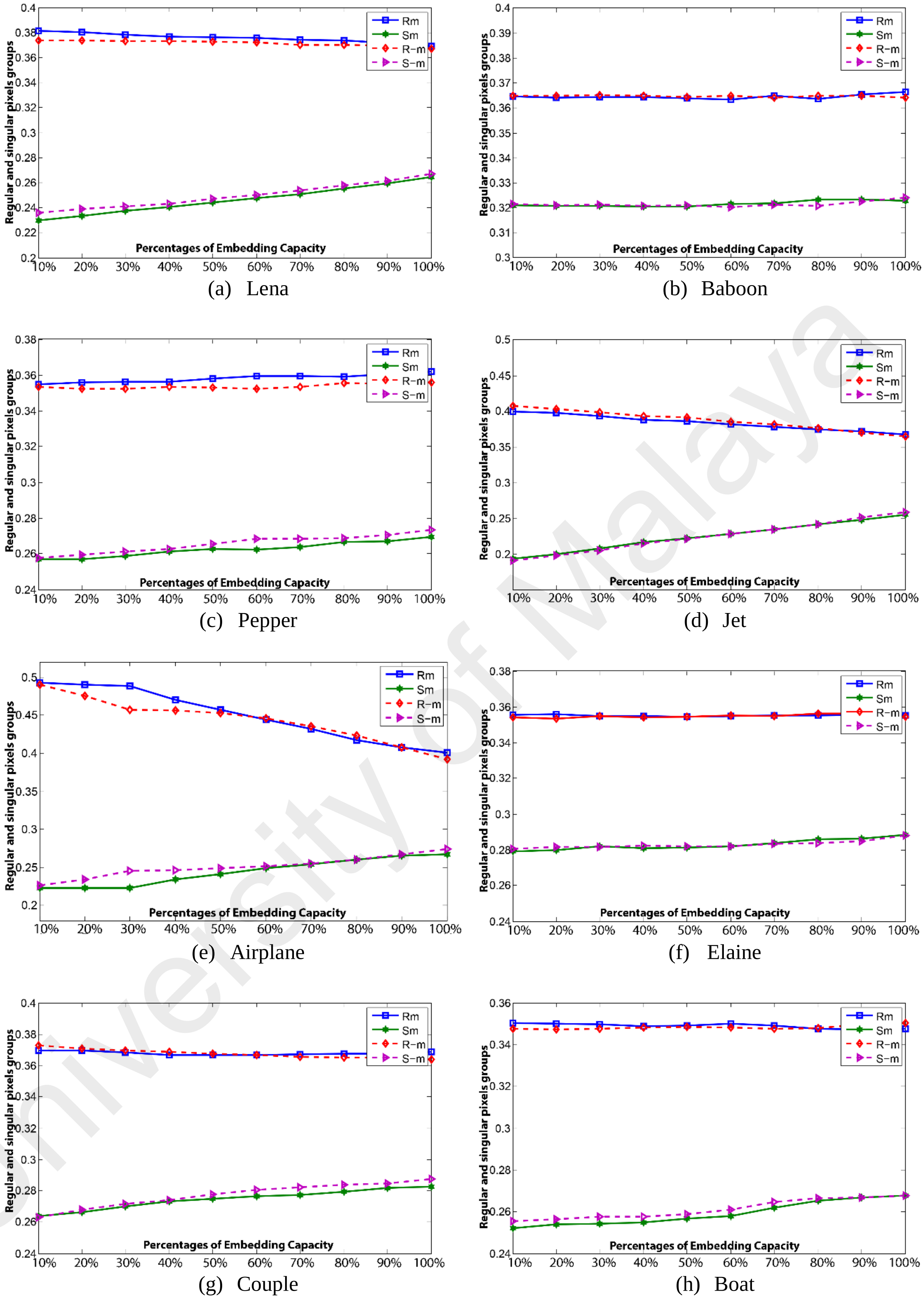


Figure 4.24: Visual Analysis of Stego-Images and Specific Zoomed Area of Proposed RMDR-based Hybrid and Compared Methods

(b) ***Security under RS detection analysis***

In this analysis section, the RS diagrams of RMDR-based hybrid embedding method depicted in Figure 4.25. The x-axes and y-axes represent the percentage of hiding capacity and percentage of regular and singular pixels groups respectively for all graphs of Figure 4.25 (a-h). The graphs depict that the proposed hybrid method retains the minimum differences between RM and R-M, SM and S-M for all stego-images.



(a) Lena (b) Baboon

(c) Pepper (d) Jet

(e) Airplane (f) Elaine

(g) Couple (h) Boat

Figure 4.25: RS Analysis Diagram of Proposed RMDR-based Hybrid Method

This concludes that the RMDR-based hybrid method is robust against RS detection analysis. The reason is that the proposed hybrid method employed the RMDR embedding that utilized the digit substitution and further the hybrid effects of RMDR and k-LSB embedding reduce the RS detection efficiency for analysis perspective. Therefore, RMDR-based hybrid method has secured under RS detection attacks analysis.

(c) ***Security under Ensemble Classifier using SPAM***

In this section, we followed the similar pattern/procedure as detailed discussed in section 4.1.3.3 (d). We evaluated the undetectability performance of RMDR-based hybrid method by machine learning based classification. The ensemble classifier by (Kodovsky et al., 2012) is employed to classify the cover and stego-images, with the utilization of SPAM features (Pevny et al., 2010). As we discussed before that the robustness of embedding method measured by the high detection error rate or classification error rate. We will evaluate the robustness of proposed hybrid method and compared with LSB-based HUGO (Pevný et al., 2010), MiPOD (Sedighi et al., 2016), adaptive LSB (H. Yang et al., 2009) and recently LSB-module-three (Xu et al., 2016) embedding methods.

The UCID image dataset (Schaefer & Stich, 2004) were used for evaluation purpose, in which first 500 randomly selected cover and its corresponding stego-images are trained by SPAM features. Furthermore, the rest of 500 cover and corresponding stego-images used for testing. The detection errors ratios on various embedding rates (i.e. 0.05 to 0.40 bpp) presented in Table 4.14 for RMDR-based hybrid and existing compared steganographic methods.

From graph as shown in Figure 4.26, the SPAM feature based classification error ratios of the proposed method is throughout higher and have significant differences against adaptive LSB (H. Yang et al., 2009) and LSB-module-three (Xu et al., 2016) methods. Where the proposed hybrid method have higher classification error rate at 0.30

bpp and afterword quite similar to state-of-the-art HUGO (Pevný et al., 2010) and MiPOD (Sedighi et al., 2016) methods as shown in Figure 4.26. Meanwhile, the Table 4.14 presents the detail of SPAM based steganalysis for all compared methods. The parameters i.e. true positive (TP), false positive (FP), true negative (TN) and false negative (FN) represent the classification analysis results. The TP represents that the number of cover images that are correctly classified as cover images. In FP the number of stego-images that are incorrectly classified as cover images. Similarly, for TN case the numbers of stego-images correctly classified as stego-images and finally the FN represent the cover-images that incorrectly classified as stego-images by the classifier. For simplicity, the Figure 4.26 shows the overall analysis results of all methods. In conclusion, this shows that proposed hybrid methods has more robustness against adaptive LSB and LSB module-three-methods, while retaining the similar robustness as compared to state-of-the-art HUGO and MiPOD methods at lower embedding rates. Although the proposed hybrid method objective is not to target the robustness of modern steganalysis, however, RMDR-based hybrid method still maintain the basic level of robustness on SPAM feature based analysis.

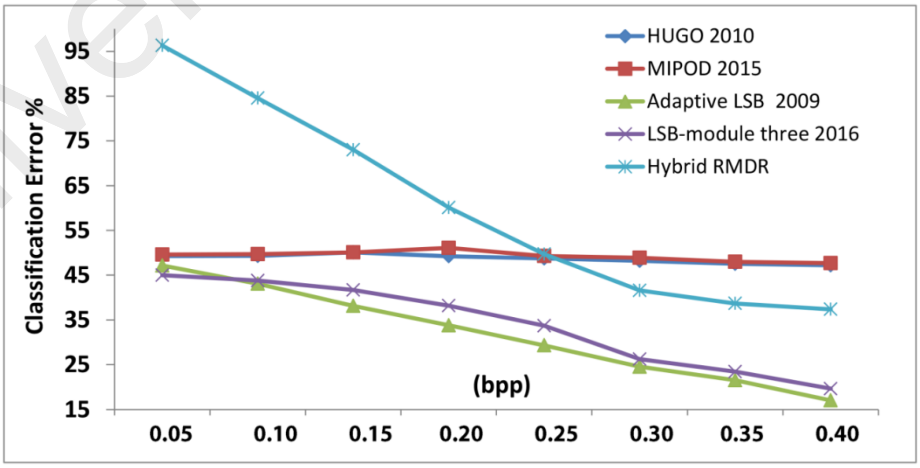


Figure 4.26: Classification Error Rate of SPAM feature based Ensemble Classifier for Proposed RMDR-based Hybrid and Other Compared Methods

Table 4.14: Undetectability Performance under SPAM feature based Steganalysis with Ensemble Classifier for RMDR-based Hybrid and Compared Methods

Methods	Bpp	TP	FP	TN	FN	Detection Error Rate %	Detection Accuracy Rate%
HUGO (Pevný et al., 2010)	0.05	270	263	237	230	49.30	50.70
MIPOD (Sedighi et al., 2016)		254	249	251	246	49.50	50.50
Adap. LSB (H. Yang et al., 2009)		251	223	277	249	47.20	52.80
LSB-module three(Xu et al., 2016)		261	211	289	239	45.00	55.00
Proposed Hybrid RMDR + k-LSB		14	477	23	486	**96.30**	3.70
HUGO (Pevný et al., 2010)	0.10	241	234	266	259	49.30	50.70
MIPOD (Sedighi et al., 2016)		258	253	247	242	49.50	50.50
Adap. LSB (H. Yang et al., 2009)		269	201	299	231	43.20	56.80
LSB-module three(Xu et al., 2016)		290	228	272	210	43.80	56.20
Proposed Hybrid RMDR + k-LSB		70	414	86	430	**84.40**	15.60
HUGO (Pevný et al., 2010)	0.15	259	259	241	241	50.00	50.00
MIPOD (Sedighi et al., 2016)		261	261	239	239	50.00	50.00
Adap. LSB (H. Yang et al., 2009)		324	213	287	176	38.90	61.10
LSB-module three(Xu et al., 2016)		303	214	286	197	41.10	58.90
Proposed Hybrid RMDR + k-LSB		139	367	133	361	72.80	27.20
HUGO (Pevný et al., 2010)	0.20	246	240	260	254	49.40	50.60
MIPOD (Sedighi et al., 2016)		224	224	276	276	50.00	50.00
Adap. LSB (H. Yang et al., 2009)		338	176	324	162	33.80	66.20
LSB-module three(Xu et al., 2016)		336	218	282	164	38.20	61.80
Proposed Hybrid RMDR + k-LSB		171	271	229	329	**60.00**	40.00
HUGO (Pevný et al., 2010)	0.25	259	246	254	241	48.70	51.30
MIPOD (Sedighi et al., 2016)		232	227	273	268	49.50	50.50
Adap. LSB (H. Yang et al., 2009)		364	157	343	136	29.30	70.70
LSB-module three(Xu et al., 2016)		356	195	305	144	33.90	66.10
Proposed Hybrid RMDR + k-LSB		237	233	267	263	**49.60**	50.40
HUGO (Pevný et al., 2010)	0.30	239	221	279	261	48.20	51.80
MIPOD (Sedighi et al., 2016)		237	222	278	263	**48.50**	51.50
Adap. LSB (H. Yang et al., 2009)		393	136	364	107	24.30	75.70
LSB-module three(Xu et al., 2016)		361	123	377	139	26.20	73.80
Proposed Hybrid RMDR + k-LSB		272	187	313	228	41.50	58.50
HUGO (Pevný et al., 2010)	0.35	242	216	284	258	47.40	52.60
MIPOD (Sedighi et al., 2016)		237	216	284	263	**47.90**	52.10
Adap. LSB (H. Yang et al., 2009)		393	107	393	107	21.40	78.60
LSB-module three(Xu et al., 2016)		389	123	377	111	23.40	76.60
Proposed Hybrid RMDR + k-LSB		282	168	332	218	38.60	61.40
HUGO (Pevný et al., 2010)	0.40	259	231	269	241	47.20	52.80
MIPOD (Sedighi et al., 2016)		242	218	282	258	**47.60**	52.40
Adap. LSB (H. Yang et al., 2009)		414	87	413	86	17.30	82.70
LSB-module three(Xu et al., 2016)		400	95	405	100	19.50	80.50
Proposed Hybrid RMDR + k-LSB		286	159	341	214	37.30	62.70

4.3 Discussion

Two innovative spatial domain image based steganography methods presented that performed the digit level substitution and further integrated it with adaptive LSB method to form a hybrid steganography technique. In the first steganography (RMDR) method, that efficiently substitutes the rightmost digits of pixels with the secret data. It exploits the correlation between secret data and cover pixels digits. Next, it generates the possible closest pixels pair based on stego digit substitution. Finally, it selects the best pixel pair that maintains the minimum vertical difference error between cover and stego-pixels. Indirectly, this closest/similar selection of stego-pixels against cover pixels enhances the visual quality and overall security without losing the embedding capacity rate. Similarly, another proposed (RMDR-based hybrid) steganography technique that exploits the image characteristics for embedding process of secret data. This technique efficiently utilized the image higher and lower texture regions with RMDR and adaptive LSB embedding techniques to achieve the set objectives.

The RMDR technique recorded the 1% embedding capacity gained in adaptive LSB approach (H. Yang et al., 2009) and almost 90% in pixel value difference (D.-C. Wu & Tsai, 2003). Similarly, the visual quality PSNR dB enhanced around 1.85% in classic LSB (Chan & Cheng, 2004), while PSNR decreases to 1% in (D.-C. Wu & Tsai, 2003). However, proposed technique retained the robustness against RS, pixel difference histogram, bit-plane, and even modern steganalysis at up to 0.4 bpp. Proposed RMDR-based hybrid method directly increased the 5.11% of capacity in LSB+PVD based methods (H-C Wu et al., 2005) (C.-H. Yang, Weng, et al., 2010). It also gained the 1% in another adaptive LSB with PVD (M Khodaei & Faez, 2012) and around 26% in LSB+EMD+MPE based method (K. Wu et al., 2015). Similarly, the proposed hybrid gained in PSNR around 2.40% in (H-C Wu et al., 2005), 0.63% in (C.-H. Yang, Weng, et al., 2010), 2.38 % (M Khodaei & Faez, 2012) and 4.22% (K. Wu et al., 2015).

The results of these analyses clearly demonstrate that these proposed techniques for data embedding recorded the highest performance in terms of visual quality, embedding capacity and security for well-known structural, statistical and modern steganalysis over the various types of texture based images.

4.4 Chapter Summary

This chapter discussed the contributions that presented the novel spatial domain based image steganography methods. The experimental results demonstrated that both proposed RMDR and RMDR-based hybrid method enhanced the visual quality, embedding capacity and security. In the light of the outcomes in this study, the proposed digit substitution based methods can be valuable for providing a balanced steganographic solution as compared to existing LSB-based techniques. Furthermore, the RMDR embedding method can be an alternative to existing LSB-based embedding to gain the improvement in visual quality and security.

CHAPTER 5: PARITY BIT PIXEL VALUE DIFFERENCING (PBPVD) AND PBPVD ADAPTIVE HYBRID METHODS

This chapter involves the innovative methodologies and experimental results of invented parity bit differencing steganography for improving the embedding capacity of existing pixel value difference (PVD) techniques. It presents two pixel value-differencing singular and hybrid steganography techniques. First, a parity bit pixel value differencing (PBPVD) method proposed that is an extension of PVD technique. The key contribution of this method is the improvement of embedding capacity and undetectability as compared to the other common PVD based singular steganography approaches i.e. PVD, Tri-way PVD (Chang et al., 2008), three-directional PVD (Jung & Yoo, 2014b). The main advantage of PBPVD technique is to efficiently utilization of pixel difference readjustment strategy with the correlation of secret data bits, which indirectly maintain the visual quality of stego-images and reduces the steganalysis detection artifacts. In addition, this method can be employed in any PVD based embedding methods to enhance the embedding capacity without degrading the visual quality.

Next, a hybrid steganography method is presented that integrates the PBPVD with previously proposed RMDR method in efficient manners. This method exploits the image texture regions for adaptive embedding which indirectly reduces the steganalysis detection attacks. Meanwhile, it designs a range table, where the higher texture based stego-pixels always keep the larger embedding rate of secret bits. The proposed PBPVD-based hybrid method achieves the optimal steganography objectives as compared to (Jung & Yoo, 2015a; M Khodaei & Faez, 2012; H-C Wu et al., 2005; C.-H. Yang, Weng, et al., 2010). The both PBPVD and hybrid PBPVD outperformed in term of embedding capacity, visual quality and security even against modern steganalysis at lower embedding rates.

This chapter is divided into five main sections, the first (section 5.1) discusses the original PVD algorithm. The second (section 5.2) presents the proposed parity bit pixel value difference (PBPVD) steganography to improve the embedding capacity of PVD, Tri-way, and three directional PVD-based methods. Section 5.3, hybrid PBPVD-based steganography presented by integrating with the previously proposed RMDR (section 4.1) method. Section 5.4 and 5.5 present the general discussion and conclusions, respectively.

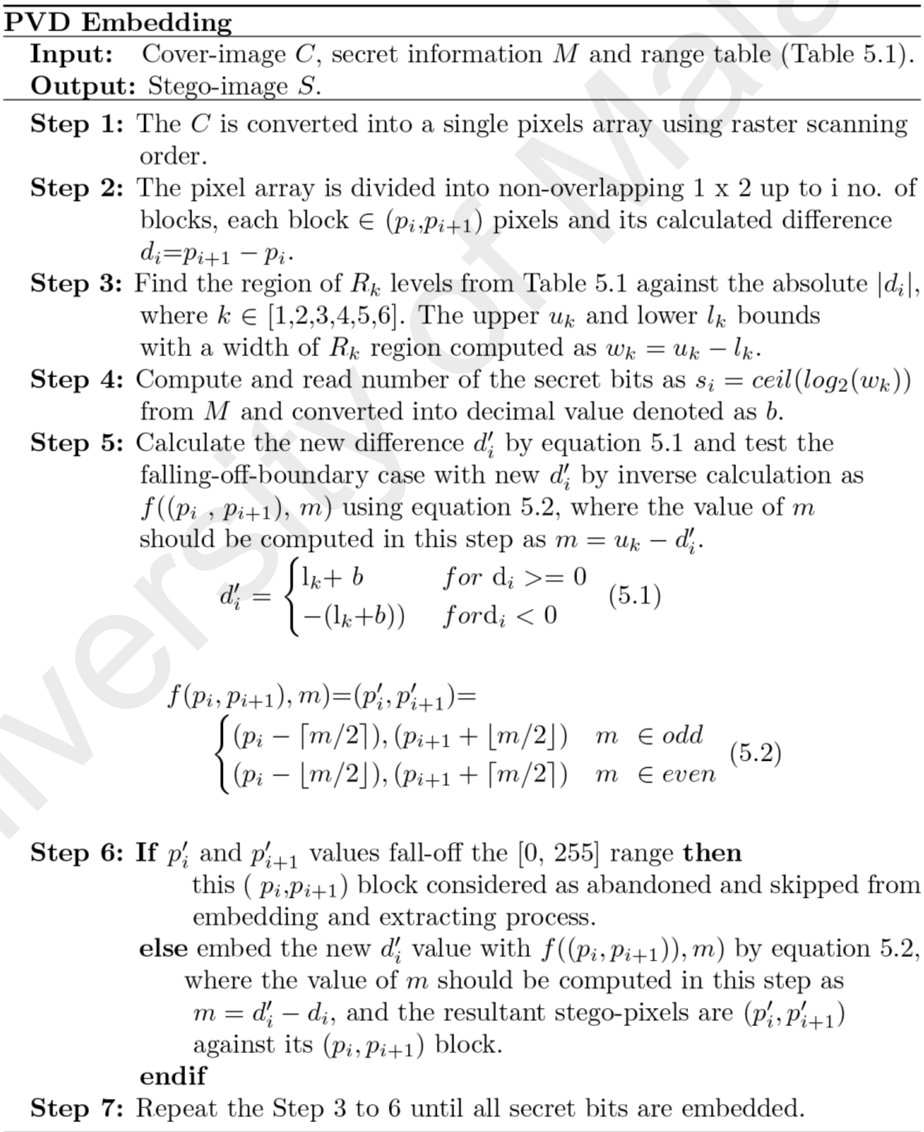
5.1 Pixel Value Difference Method

In the PVD (D.-C. Wu & Tsai, 2003) method, the secret data embedded by adjusting the difference between successive pixels. For example, in a cover image, the difference value *d* obtained from every non-overlapping block of two consecutive pixels, i.e. (p_0 , p_1). Where the *d* is computed as *d* = ($p_0 - p_1$), which may be in the range from -255 to +255. This difference *d* is located in the range R_k level of range table to determine the number of *t* secret bits for embedding. The number of *t* secret bits are computed by *t = log2 (u - l +1),* where the *'l'* and *'u'* are the lower and upper bound values of the range R_k, and *k* is (1, 2,..., *n*). The new difference *d'* is computed as *d'* = |*l* + *b*|, where *b* is the integer value of the sub-stream of M with the *t* number of secret bits. After calculating the new difference with secret data *b*, the *d'* is adjusted in the cover (p_0 , p_1) pixels block by performing an inverse calculation to yield the new stego-pixels i.e. p'_0 , p'_1 for stego-image. The PVD range table and complete embedding steps presented in Table 5.1 and Table 5.2 respectively, in addition, a basic example showed in Figure 5.1.

Table 5.1: PVD Range Table with R_k (lower and upper bounds) and Number of Secret Bits

Lower-Upper bound of $\boldsymbol{R_k}$	$\boldsymbol{R_1 \epsilon}$ $\boldsymbol{[0,7]}$	$\boldsymbol{R_2 \epsilon}$ $\boldsymbol{[8,15]}$	$\boldsymbol{R_3 \epsilon}$ $\boldsymbol{[16,31]}$	$\boldsymbol{R_4 \epsilon}$ $\boldsymbol{[32,63]}$	$\boldsymbol{R_5 \epsilon}$ $\boldsymbol{[64,127]}$	$\boldsymbol{R_6 \epsilon}$ $\boldsymbol{[128,255]}$
Secret bits	3	3	4	5	6	7

Table 5.2: Pixel Value Difference (PVD) Embedding Steps



```
PVD Embedding
  Input:   Cover-image $C$, secret information $M$ and range table (Table 5.1).
  Output:  Stego-image $S$.

  Step 1: The $C$ is converted into a single pixels array using raster scanning
          order.
  Step 2: The pixel array is divided into non-overlapping 1 x 2 up to i no. of
          blocks, each block $\in (p_i, p_{i+1})$ pixels and its calculated difference
          $d_i = p_{i+1} - p_i$.
  Step 3: Find the region of $R_k$ levels from Table 5.1 against the absolute $|d_i|$,
          where $k \in [1,2,3,4,5,6]$. The upper $u_k$ and lower $l_k$ bounds
          with a width of $R_k$ region computed as $w_k = u_k - l_k$.
  Step 4: Compute and read number of the secret bits as $s_i = ceil(log_2(w_k))$
          from $M$ and converted into decimal value denoted as $b$.
  Step 5: Calculate the new difference $d'_i$ by equation 5.1 and test the
          falling-off-boundary case with new $d'_i$ by inverse calculation as
          $f((p_i \, , p_{i+1}), m)$ using equation 5.2, where the value of $m$
          should be computed in this step as $m = u_k - d'_i$.

          $d'_i = \begin{cases} \mathrm{l}_k + b & for\ \mathrm{d}_i >= 0 \\ -(\mathrm{l}_k + b)) & for \mathrm{d}_i < 0 \end{cases} \quad (5.1)$

          $f(p_i, p_{i+1}), m) = (p'_i, p'_{i+1}) = \begin{cases} (p_i - \lceil m/2 \rceil), (p_{i+1} + \lfloor m/2 \rfloor) & m \ \in odd \\ (p_i - \lfloor m/2 \rfloor), (p_{i+1} + \lceil m/2 \rceil) & m \ \in even \end{cases} \quad (5.2)$

  Step 6: If $p'_i$ and $p'_{i+1}$ values fall-off the [0, 255] range then
              this ( $p_i, p_{i+1}$) block considered as abandoned and skipped from
              embedding and extracting process.
          else embed the new $d'_i$ value with $f((p_i, p_{i+1})), m)$ by equation 5.2,
              where the value of $m$ should be computed in this step as
              $m = d'_i - d_i$, and the resultant stego-pixels are $(p'_i, p'_{i+1})$
              against its $(p_i, p_{i+1})$ block.
          endif
  Step 7: Repeat the Step 3 to 6 until all secret bits are embedded.
```

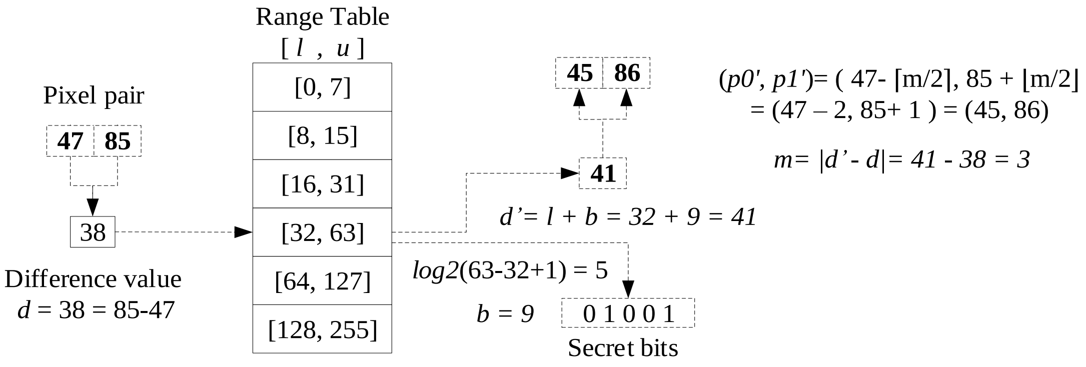


Figure 5.1: A Basic Example of PVD Method

From Figure 5.1, assume p_0 = 47, p_1= 85 and difference *d* = 38, where 38 satisfy the R_4 range level with the *l* = 32 and *u* = 63. The range level Table 5.1 shows that the range R_4 can embed the 5 secret bits in this cover-pixel pair. The 5 secret bits and its decimals values are $(0\ 1\ 0\ 0\ 1)_2$ and $b = 9_{10}$, respectively. Next step is to compute the new adjusted difference with secret decimal *b*, where the lower range *l* = 32 and *d'* = 41= |*l* + *b* | = |32+9|. Further, apply the equation 5.2 to adjust the new difference *d'* between the both cover pixels. So, the resultant stego-pixel becomes ($p'_{0\,,}\, p'_1$) = (45, 86) with the concealing of 5 secret bits i.e. $(0\ 1\ 0\ 0\ 1)_2$.

5.2 Parity Bit Pixel Value Difference Steganography Method

The concept of the proposed PBPVD embedding method is to adjust an extra (parity) secret bit in the PVD stego-pixels ($p_{\ i}\,, p_{\ i+1}$). This parity bit employed by using ±1 in one of the chosen stego-pixel with specific secret order. The secret order can be selected in different ways i.e. odd/even order, specific interval interchanging or some mathematical Fibonacci or Prime number based selection order of $p_{\ i}$ or $p_{\ i+1}$ pixel. The reason behind the selection of secret order in PBPVD method is necessary because this enhances the secrecy of secret data itself. For example, if an eavesdropper has PVD range table, even though he or she is not able to extract the actual secret data without knowing the parity bit selected order. Therefore, the secret order is necessary to recover the actual or 100% original secret data from stego-image.

After adjusting an extra secret bit inside the stego-pixel, a readjustment process used to maintain the original difference between pixels. In addition, during the embedding process, a recursive readjustment of pixel values employed to maintain the pixel range [0, 255] boundary conditions. Table 5.3 presents the range table of PBPVD method with the estimated secret bits. This PBPVD range table (Table 5.3) indirectly increases the one extra secret bit among all the range levels of PVD based range table (Table 5.1). For example, in range Table 5.1, the R_4 Є [32, 63] and the embedding secret bits were 5. Thus, as shown in Table 5.3, the R_4 embedding secret bits are increased from 5 to 6 because of parity bit adjusting as an extra secret bit in each pixels block. The embedding and extracting sections are as discussed below.

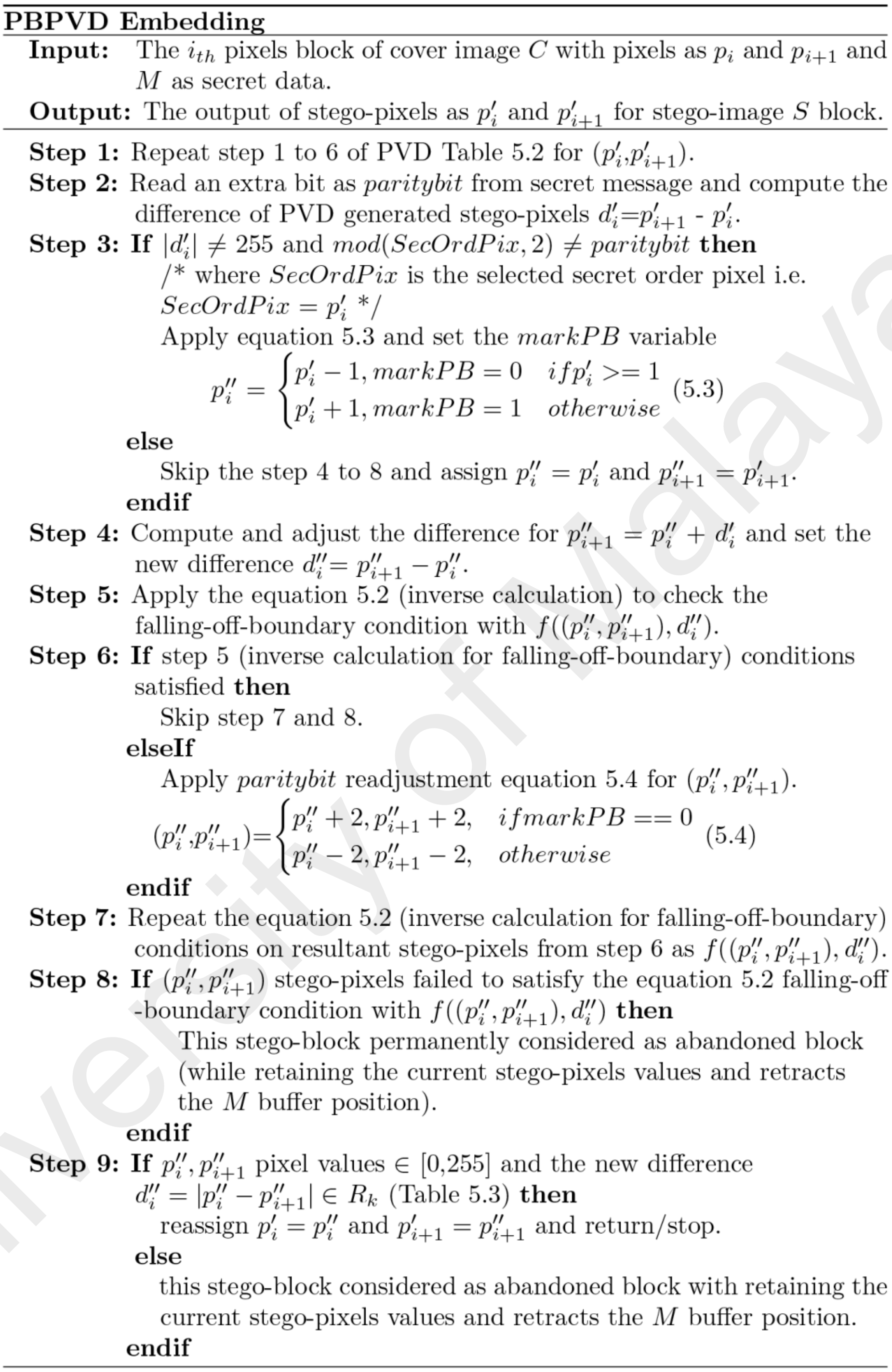
Table 5.3: PBPVD Range Table R_k (lower and upper bounds) with the Number of Secret Bits

Lower-Upper bound of $\boldsymbol{R_k}$	$\boldsymbol{R_1\epsilon}$ $[\mathbf{0}, \mathbf{7}]$	$\boldsymbol{R_2\epsilon}$ $[\mathbf{8}, \mathbf{15}]$	$\boldsymbol{R_3\epsilon}$ $[\mathbf{16}, \mathbf{31}]$	$\boldsymbol{R_4\epsilon}$ $[\mathbf{32}, \mathbf{63}]$	$\boldsymbol{R_5\epsilon}$ $[\mathbf{64}, \mathbf{127}]$	$\boldsymbol{R_6\epsilon}$ $[\mathbf{128}, \mathbf{255}]$
Secret bits	4	4	5	6	7	8

5.2.1 PBPVD Embedding Method

This section presents the proposed PBPVD embedding steps in Table 5.4. Further, a basic PBPVD based example illustrated in Figure 5.2.

Table 5.4: PBPVD Embedding Steps with Example



```
PBPVD Embedding
  Input:   The $i_{th}$ pixels block of cover image $C$ with pixels as $p_i$ and $p_{i+1}$ and
           $M$ as secret data.
  Output:  The output of stego-pixels as $p'_i$ and $p'_{i+1}$ for stego-image $S$ block.

  Step 1: Repeat step 1 to 6 of PVD Table 5.2 for $(p'_i,p'_{i+1})$.
  Step 2: Read an extra bit as $paritybit$ from secret message and compute the
          difference of PVD generated stego-pixels $d'_i$=$p'_{i+1}$ - $p'_i$.
  Step 3: If $|d'_i| \neq 255$ and $mod(SecOrdPix, 2) \neq paritybit$ then
            /* where $SecOrdPix$ is the selected secret order pixel i.e.
            $SecOrdPix = p'_i$ */
            Apply equation 5.3 and set the $markPB$ variable
              $p''_i = \begin{cases} p'_i - 1, markPB = 0 & if p'_i >= 1 \\ p'_i + 1, markPB = 1 & otherwise \end{cases}$   (5.3)
          else
            Skip the step 4 to 8 and assign $p''_i = p'_i$ and $p''_{i+1} = p'_{i+1}$.
          endif
  Step 4: Compute and adjust the difference for $p''_{i+1} = p''_i + d'_i$ and set the
          new difference $d''_i = p''_{i+1} - p''_i$.
  Step 5: Apply the equation 5.2 (inverse calculation) to check the
          falling-off-boundary condition with $f((p''_i, p''_{i+1}), d''_i)$.
  Step 6: If step 5 (inverse calculation for falling-off-boundary) conditions
          satisfied then
            Skip step 7 and 8.
          elseIf
            Apply $paritybit$ readjustment equation 5.4 for $(p''_i, p''_{i+1})$.
            $(p''_i,p''_{i+1}) = \begin{cases} p''_i + 2, p''_{i+1} + 2, & if markPB == 0 \\ p''_i - 2, p''_{i+1} - 2, & otherwise \end{cases}$   (5.4)
          endif
  Step 7: Repeat the equation 5.2 (inverse calculation for falling-off-boundary)
          conditions on resultant stego-pixels from step 6 as $f((p''_i, p''_{i+1}), d''_i)$.
  Step 8: If $(p''_i, p''_{i+1})$ stego-pixels failed to satisfy the equation 5.2 falling-off
          -boundary condition with $f((p''_i, p''_{i+1}), d''_i)$ then
              This stego-block permanently considered as abandoned block
              (while retaining the current stego-pixels values and retracts
              the $M$ buffer position).
          endif
  Step 9: If $p''_i, p''_{i+1}$ pixel values $\in$ [0,255] and the new difference
          $d''_i = |p''_i - p''_{i+1}| \in R_k$ (Table 5.3) then
            reassign $p'_i = p''_i$ and $p'_{i+1} = p''_{i+1}$ and return/stop.
          else
            this stego-block considered as abandoned block with retaining the
            current stego-pixels values and retracts the $M$ buffer position.
          endif
```

The below Figure 5.2 depicts the graphical flow of PBPVD example as discussed in Table 5.4.

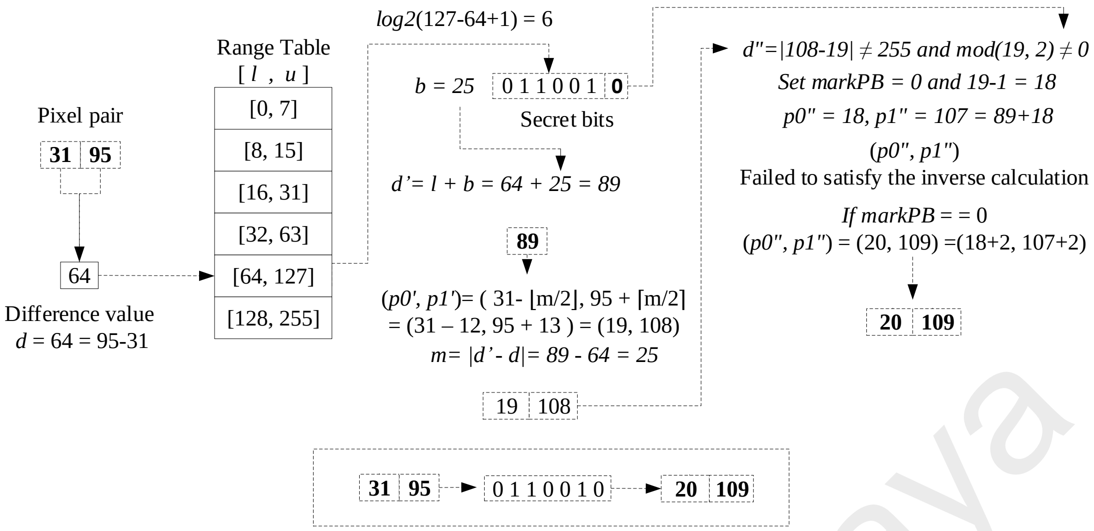


Figure 5.2: The Basic Example PBPVD Embedding Method

5.2.2 PBPVD Extracting Method

The PBPVD extraction algorithm steps and example discussed in Table 5.5.

Table 5.5: The PBPVD Extracting Steps with Example

PBPVD Extracting Steps

Input: The i_{th} block of S (stego-image) with pixels as p'_i and p'_{i+1}.
Output: Recovered secret bits from p'_i and p'_{i+1}.

Step 1: Take the stego-pixels p'_i and p'_{i+1} from S.
Step 2: Apply the PVD extraction method and recovered the secret bit into $PvdRecBits$.
Step 3: Extract the parity bit from secret order chosen stego-pixel using $paritybit = \text{mod(stego-pixel, 2)}$.
Step 4: Concatenate the $PvdRecBits$ with $paritybit$ as extracted binary secret data.

EXAMPLE

Input: The stego-pixel p'_i and p'_{i+1} values are (20, 109).
Output: The recovered secret bits from p'_i and p'_{i+1} are (0110010).

Step 1: The stego-pixels p'_i= 20 and p'_{i+1} = 109.
Step 2: Extracted $PvdRecBits$ = 011001 from PVD extraction.
Step 3: Extracted $paritybit$ = 0 = mod (20, 2).
Step 4: Concatenated 0110010 recovered bit stream.

To prove the effectiveness of PBPVD, we employed the parity bit adjustment process on two other PVD-based methods, i.e. Tri-way PVD (Chang et al., 2008), and Three directional PVD (Jung & Yoo, 2014b) methods. In both Tri-way and three directional PVD-based methods, we employed the PBPVD Table 5.4 step 2 to step 9 on Tri-way and three directional PVD-based stego-pixels. The both methods improved the embedding capacity and security, while retained the similar visual quality. The experimental section will show and discuss the complete results.

5.2.3 Experimental Results and Analysis

In this section, we will discuss the selected dataset and a setup to evaluate the performance of proposed PBPVD method. Furthermore, similar to previous experiments (section 4.1.3, 4.2.3), we will perform series of test to evaluate the performance of proposed methods with respect to all general evaluation criteria i.e., visual quality, embedding capacity, undetectability/security.

5.2.3.1 Dataset and Setup

To provide the sound justification for evaluation of proposed PBPVD steganography method, we employed the same evaluation measures i.e. embedding capacity, visual quality and security from section 4.1.3. Furthermore, for image dataset, both UCID (Schaefer & Stich, 2004) and USC-SIPI (USC-SIPI, 2016) databases are employed (discussed section 4.1.3.1). Some of the benchmarked images that frequently used in this evaluation process are already shown in Figure 4.5. A pseudo-random number generator used to generate the secret bits. In this section, we conducted the two sets of experiments. First, that measures the embedding capacity and visual quality of stego-images. Second to evaluate the proposed method security/undetectability against statistical steganalysis, and further employed a modern steganalysis by applying machine learning ensemble classifier using Subtractive Pixel Adjacency Matrix (SPAM) detector (Pevny et al., 2010).

5.2.3.2 Embedding Capacity and Visual Quality Evaluation

This section analyzes the hidden capacity and visual quality of the proposed PBPVD methods in three parts. First, a performance comparison of proposed PBPVD and the classic PVD (D.-C. Wu & Tsai, 2003) methods conducted on various range tables. Similarly, the performances of proposed Tri-way-PBPVD and three directional PBPVD methods with its default/original Tri-way and three directional PVD (Chang et al., 2008; Jung & Yoo, 2014b) based methods are evaluated. Secondly, the proposed PBPVD and Tri-way PBPVD methods embedding capacities evaluated on various visual quality levels to prove the efficacy of proposed methods at different embedding rates. Third, for extensive performance evaluation, aforementioned methods evaluated over larger image datasets.

(a) ***Performance of Embedding Capacity and Visual Quality***

In this sub-experiment, a comparison of proposed PBPVD with the classic PVD (D.-C. Wu & Tsai, 2003) embedding is evaluated with different range tables, this proves that proposed method can maintain significantly high payload regardless of range levels divisions as shown in Table 5.6. We employed the two general range tables denoted as RT1 and RT2, where the range levels of RT1= (8,8,16,32,64,128) and RT2 = (8,16,32,64,128,8). In RT1 range table division, the proposed PBPVD method gained up to +31.69% higher average embedding capacity against (D.-C. Wu & Tsai, 2003)'s method (from 412,724 to 543,506). Furthermore, it retained the similar PSNR ≈40 dB values. Meanwhile, in RT2 range table divisions based evaluation; the proposed PBPVD methods also gained +29.79% higher embedding capacity (from 438,808 to 569,514) at PSNR ≈38 dB level. Similar to PSNR, proposed method has almost the identical universal quality index (Q) values against classic PVD method. The efficacy of proposed PBPVD approach with existing PVD-based methods is shown in Table 5.7. The proposed Tri-way-PBPVD method improved the average embedding capacity (627,120 to 691,959) up to 10.34% against original Tri-way PVD (Chang et al., 2008) method. Similarly, the proposed three-directional-PBPVD method improved the 9.93% average payload (653,257 to 718,095) against (Jung & Yoo, 2014b) original three-directional method, while retaining the similar visual quality statistics.

The reason behind this extensive improvement in embedding capacity and maintaining of visual quality of stego-image explained or discussed as follows. Let a cover image with the resolution of 512x512 pixels, where the number of classic PVD based blocks are 131,072. The PVD block consists of two non-overlapped pixels computed as 2x1 = 512x256 = 131,072 total number of blocks. However, the proposed PBPVD method can embed one extra secret bit inside each pixel pair of a block. Therefore, it shows that up to 131,072 extra secret bits can be accommodated in the PVD method. Furthermore, the proposed recursive readjustment process maintains the visual quality of stego-image with satisfying the boundary and inverse calculation conditions.

In conclusion of this section, From Table 5.6 and Table 5.7 results analysis, proposed PBPVD-based methods showed the improvement in the embedding payloads, while maintained the visual quality regardless of range tables divisions, and further proved its efficacy at various PVD-based methods.

Table 5.6: Performance Comparison of Proposed and Existing Singular Classic PVD Steganography Methods

Images	**(D.-C. Wu & Tsai, 2003)** **Classic PVD**						**PBPVD Method**					
	R1=[8,8,16,32,64,128]			**R2=[8,16,32,64,128,8]**			**R1=[8,8,16,32,64,128]**			**R2=[8,16,32,64,128,8]**		
	Capacity	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**	**Capacity**	**PSNR**	**Q**
Lena	409,779	41.21	0.9989	432,152	39.38	0.9984	540,850	40.69	0.9988	563,221	39.06	0.9983
Baboon	456,953	36.95	0.9963	500,778	35.18	0.9946	587,971	36.81	0.9963	631,783	35.04	0.9944
Pepper	405,425	41.51	0.9992	431,866	39.60	0.9988	536,210	41.12	0.9992	562,573	39.26	0.9987
Jet	409,531	40.44	0.9986	423,021	39.26	0.9982	540,562	40.05	0.9986	553,929	38.92	0.9981
Tank	403,990	42.40	0.9974	433,400	40.04	0.9956	535,062	41.84	0.9972	564,469	39.73	0.9955
Airplane	397,904	42.22	0.9960	402,665	41.67	0.9955	528,975	41.67	0.9957	533,735	41.17	0.9952
Truck	400,504	42.90	0.9977	423,753	40.88	0.9964	531,573	42.33	0.9976	554,817	40.54	0.9962
Elaine	408,582	41.90	0.9990	445,535	39.45	0.9983	539,652	41.34	0.9989	576,602	39.15	0.9982
Couple	419,901	39.78	0.9982	447,266	37.94	0.9974	550,541	39.45	0.9982	577,711	37.73	0.9973
Boat	419,317	39.57	0.9983	454,294	37.64	0.9974	550,105	39.24	0.9983	585,040	37.36	0.9973
Tiffany	398,980	41.48	0.9973	414,535	40.23	0.9964	527,799	41.05	0.9972	542,906	39.87	0.9963
Lake	421,819	39.73	0.9992	456,425	37.74	0.9987	552,773	39.41	0.9992	587,377	37.53	0.9987
Average	412,724	40.84	0.9980	438,808	39.08	0.9971	**543,506**	40.42	0.9979	**569,514**	38.78	0.9970

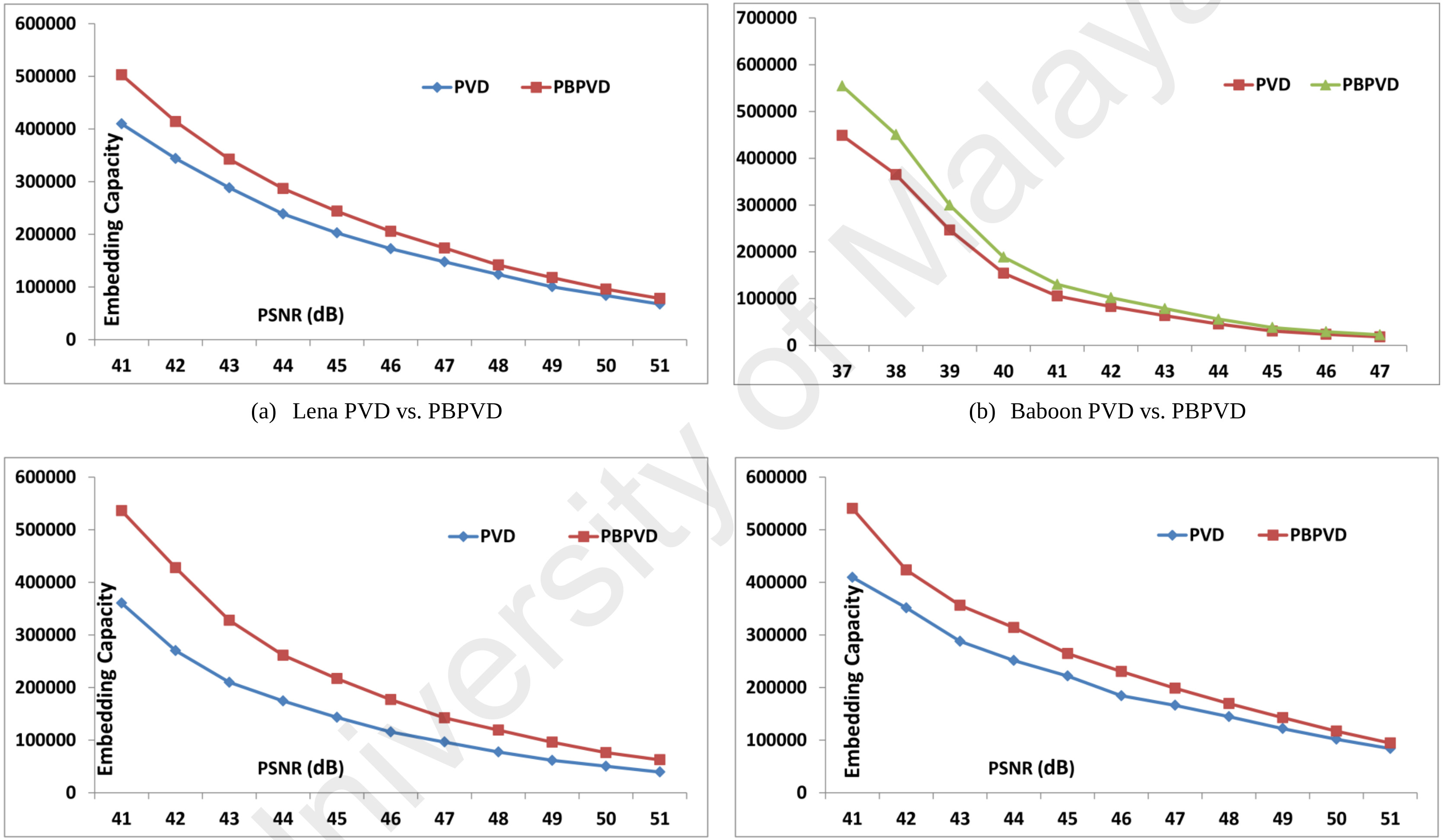
Table 5.7: Performance Comparison of Proposed Tri-Way-PBPVD and Three-Directional-PBPVD with Original Tri-Way and Three-Directional PVD-based Methods

Images	**Tri-way PVD (Chang et al., 2008)**		**Tri-way PBPVD**			**Three-Directional PVD (Jung & Yoo, 2014b)**		**Three-Directional PBPVD**		
	Capacity	**PSNR**	**Capacity**	**PSNR**	**Improvement**	**Capacity**	**PSNR**	**Capacity**	**PSNR**	**Improvement**
Lena	614,002	37.59	679,400	37.42	10.65%	622,759	38.04	688,157	37.87	10.50%
Baboon	714,211	31.70	778,165	31.59	8.95%	791,886	33.40	855,840	33.29	8.08%
Pepper	613,070	36.98	678,150	36.92	10.62%	621,134	34.35	686,214	34.29	10.48%
Jet	620,913	36.11	686,247	35.93	10.52%	634,926	36.54	700,260	36.36	10.29%
Tank	614,147	38.14	679,656	37.98	10.67%	621,203	38.35	686,712	38.19	10.55%
Airplane	598,900	38.57	664,302	38.46	10.92%	602,956	38.75	668,358	38.64	10.85%
Truck	613,629	38.27	679,077	38.06	10.67%	616,089	38.05	681,537	37.84	10.62%
Elaine	615,694	38.08	681,171	37.89	10.63%	617,225	38.20	682,702	38.01	10.61%
Couple	637,818	35.73	702,320	35.59	10.11%	644,874	35.59	709,376	35.45	10.00%
Boat	631,279	35.84	696,444	35.81	10.32%	653,453	35.61	718,618	35.58	9.97%
Tiffany	610,970	37.59	672,383	37.41	10.05%	619,924	37.40	681,337	37.22	9.91%
Lake	640,807	35.16	706,191	35.07	10.20%	645,703	35.23	711,087	35.14	10.13%
Average	627,120	36.65	**691,959**	36.51	**10.34%**	653,257	36.59	**718,095**	36.45	**9.93%**

(b) ***Performance of Embedding Capacity at Various Visual Quality (PSNR) Levels***

The purpose of this experiment is to evaluate the performance of embedding capacity at various PSNR levels. In Figure 5.3 (a-h), the x-axis and y-axis represent the PSNR levels and corresponding embedding capacity in number of bits, respectively. From Table 5.6, the maximum embedding capacity of PVD method is at around 41 dB PSNR. Similarly, in Tri-way PVD, the maximum embedding capacity can be achieve at around 37 dB PSNR as shown in Table 5.7. Therefore, in Figure 5.3, both PVD and Tri-way PVD starting points of PSNR are different to each other's. However, we will evaluate the performance of embedding capacity at various PSNR levels between PVD and PBPVD. Similarly, the PSNR of Tri-way PVD vs. Tri-way PBPVD evaluated in Figure 5.3 at various embedding capacity rates.

From Lena graphs Figure 5.3 (a), proposed PBPVD shows the higher embedding bits at each PSNR level as compared to corresponding classic PVD method. Similarly, for another proposed Tri-way PBPVD based embedding technique which throughout retains the higher embedding bit rate at various PSNR dB levels with respect to original Tri-way PVD method. This indicates that the proposed PBPVD-based methods are able to retain the high embedding capacity at various visual quality levels. Therefore, proposed methods are ideal for high capacity based applications with the highest visual quality levels.



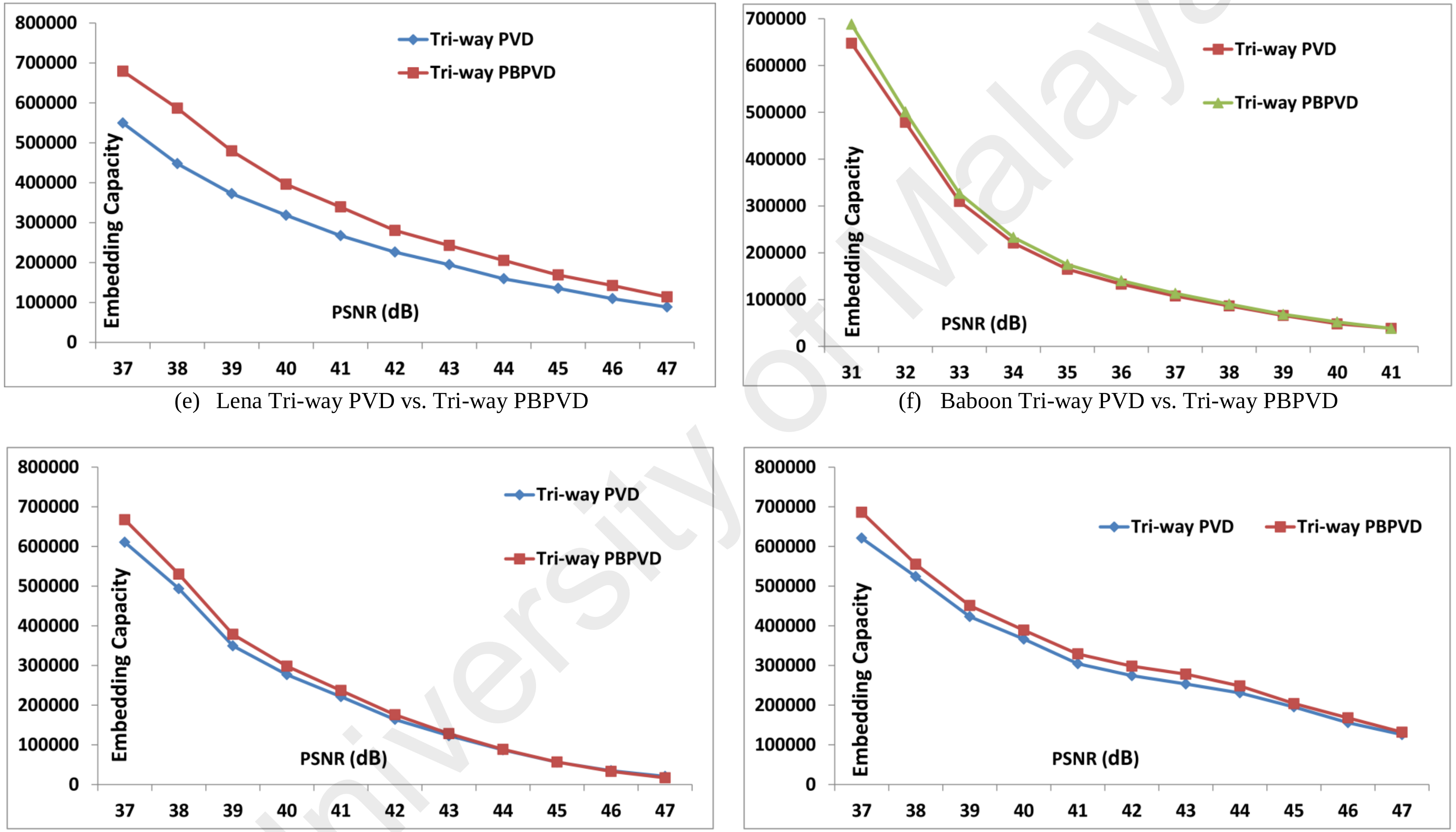
(a) Lena PVD vs. PBPVD

(b) Baboon PVD vs. PBPVD

(c) Pepper PVD vs. PBPVD

(d) Jet PVD vs. PBPVD

Figure 5.3, Continued



(e) Lena Tri-way PVD vs. Tri-way PBPVD

(f) Baboon Tri-way PVD vs. Tri-way PBPVD

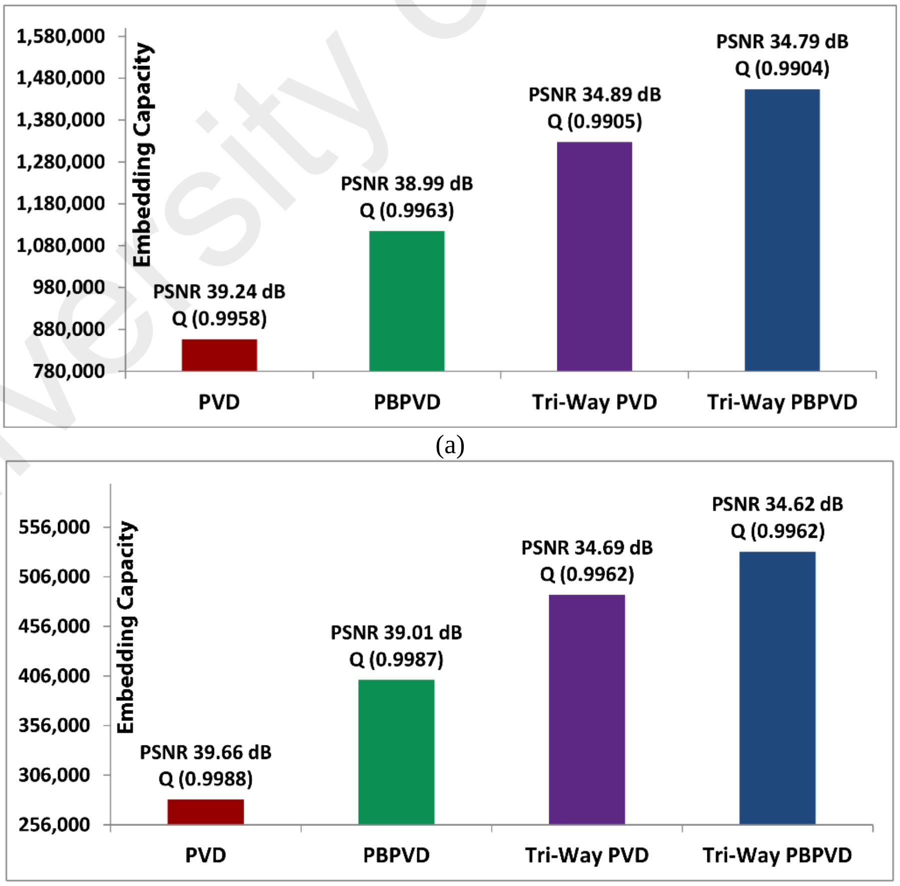
(g) Pepper Tri-way PVD vs. Tri-way PBPVD

(h) Jet Tri-way PVD vs. Tri-way PBPVD

Figure 5.3: Embedding Capacity Graph at Various PSNR Levels of Proposed PBPVD-based Methods

(c) ***Performance over UCID and USC-SIPI Image Datasets***

For in-depth performance evaluation of embedding capacity and visual quality of proposed methods, we employed the complete UCID (Schaefer & Stich, 2004) and SIPI (USC-SIPI, 2016) image datasets. Figure 5.4 (a) depicts the performance of proposed and compared steganography techniques over SIPI (144 images) dataset. Similarly, the Figure 5.4 (b) shows the embedding capacity and visual quality performance for complete UCID (1338) images. In Figure 5.4 (a-b), the x-axis and y-axis represent the embedding methods and embedding bits respectively. As results, proposed PBPVD-based methods outperformed the compared methods in order to achieve embedding capacity and visual quality for both SIPI and UCID datasets. These graphs depict that proposed PBPVD-based methods retain the higher embedding capacities and similar visual quality in terms of PSNR dB and Q values.



(a)

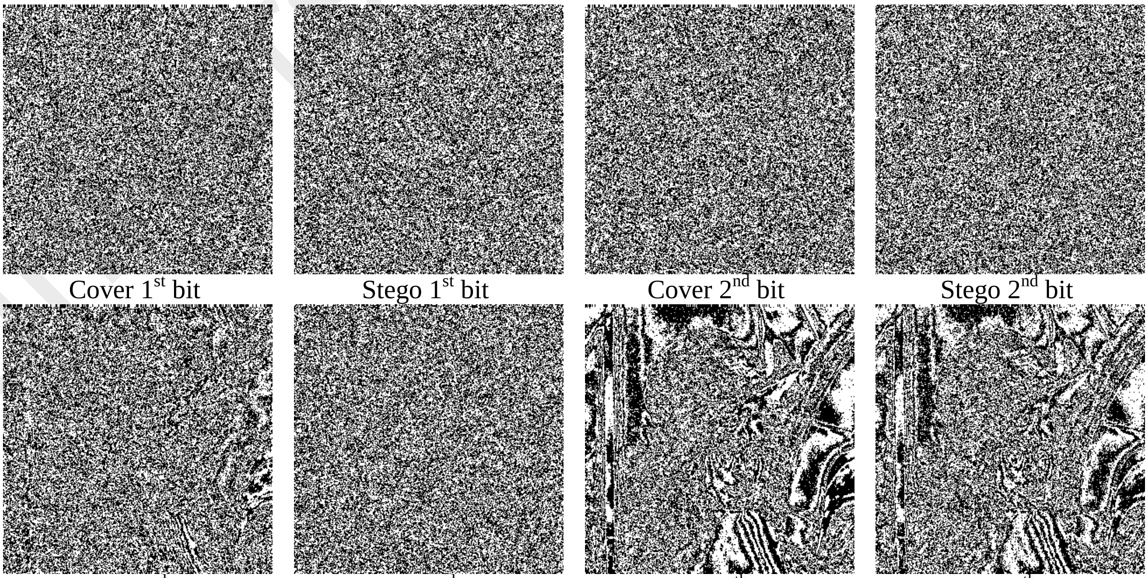
(b)

Figure 5.4: Embedding Capacity with PSNR Performance for (a) SIPI (USC-SIPI, 2016) (b) UCID (Schaefer & Stich, 2004) Datasets.

5.2.3.3 Security/Undetectability Evaluation

(a) ***Bit-plane Analysis***

In this section, we present the bit-plane analysis of PBPVD and Tri-way PBPVD techniques. The visual representation of PBPVD based Lena and Baboon bit-planes analyses are shown in Figure 5.5 and Figure 5.6, respectively. Similarly, the proposed Tri-way PBPVD embedding bit-plane analysis are shown in Figure 5.7 and Figure 5.8 for Lena and Baboon stego-images, respectively. Each bit plane of stego-images separately represented in sub-images. For example, Figure 5.5 shows the Lena cover and respective stego-images for all 1 to 8 bit planes. From Figure 5.5 to Figure 5.8, the visual representation of each bit plane between the cover and respective stego-images are almost similar to each other. This concludes that proposed PBPVD and Tri-way PBPVD stego-images can resist the visual bit-plane detection analysis. The main reason of robustness against bit planes analysis detections is that the proposed methods employed the direct pixels values and adjust the differences with secret data instead of direct bit planes modifications.



Cover 1st bit

Stego 1st bit

Cover 2nd bit

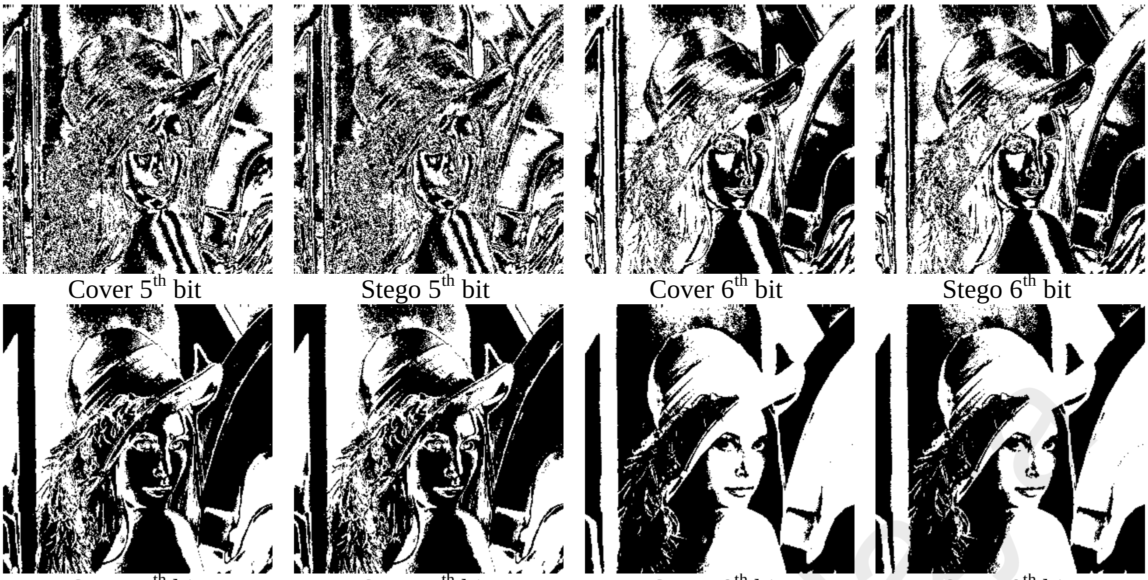
Stego 2nd bit

Cover 3rd bit

Stego 3rd bit

Cover 4th bit

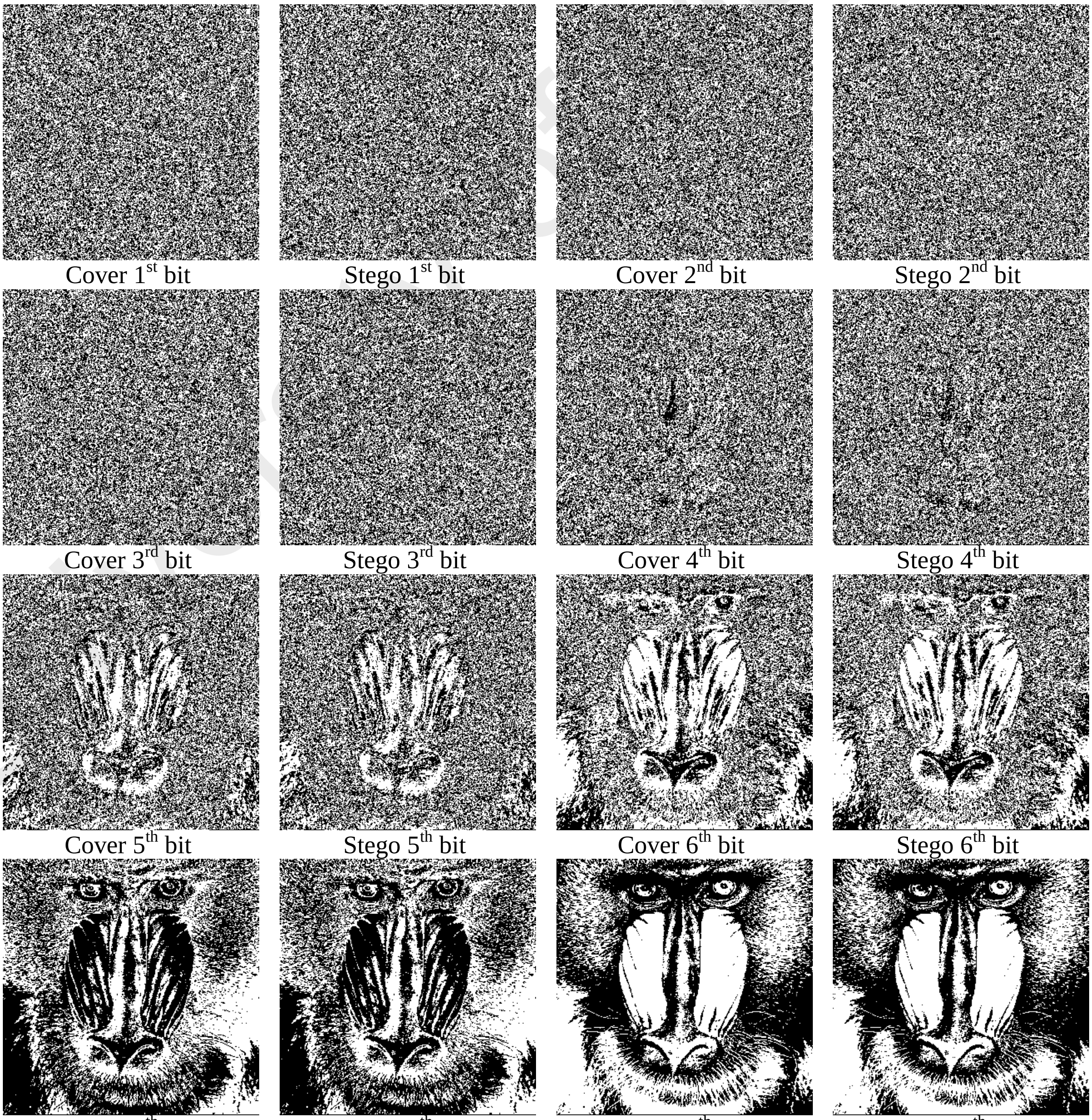
Stego 4th bit



Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 5.5: Bit-plane Analysis of Proposed PBPVD Stego-image (Lena)



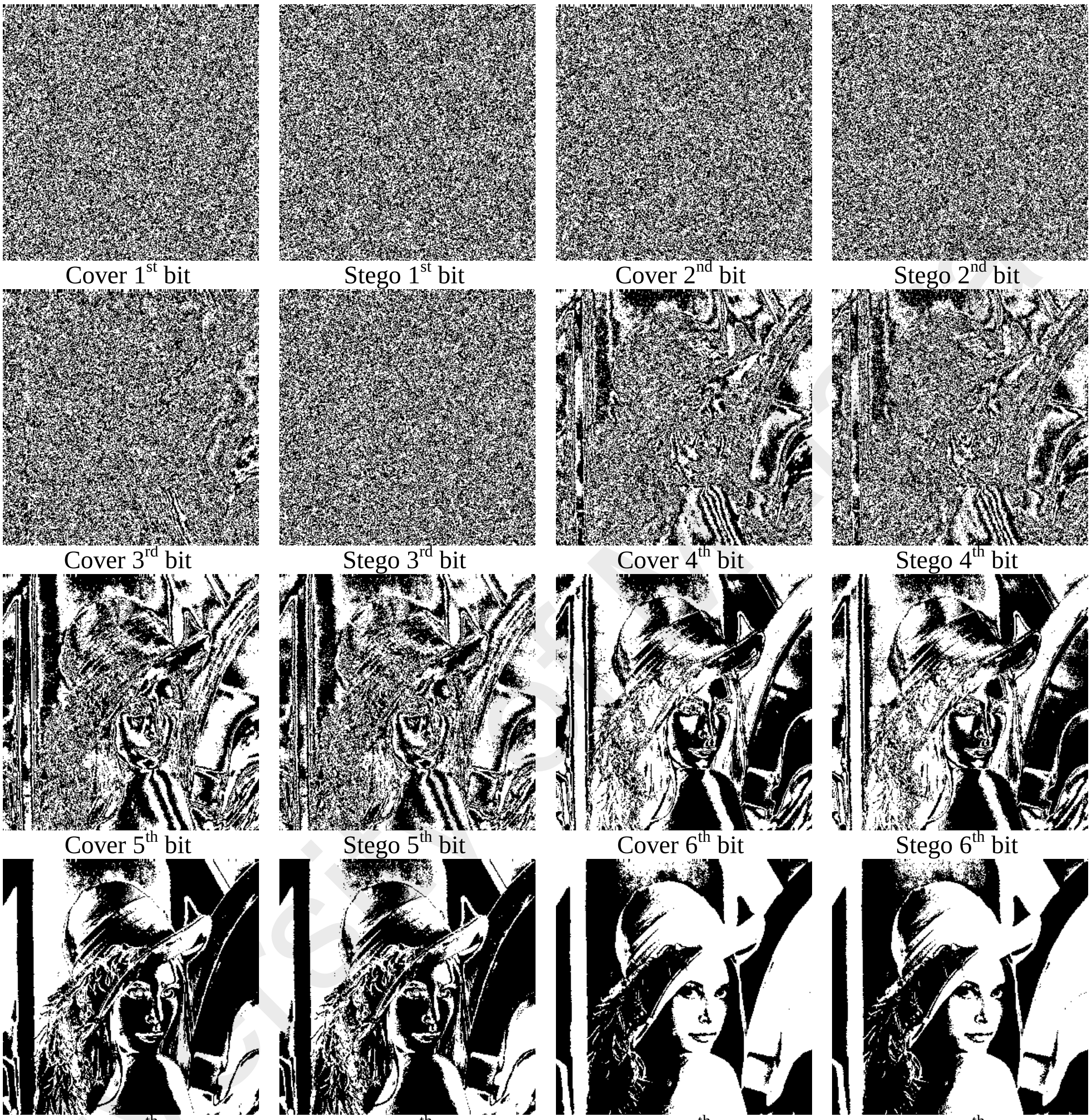
Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit

Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 5.6: Bit-plane Analysis of Proposed PBPVD Stego-image (Baboon)



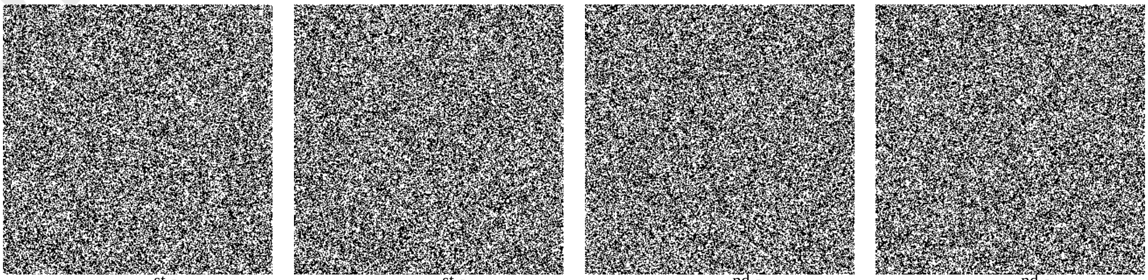
Cover 1st bit | Stego 1st bit | Cover 2nd bit | Stego 2nd bit

Cover 3rd bit | Stego 3rd bit | Cover 4th bit | Stego 4th bit

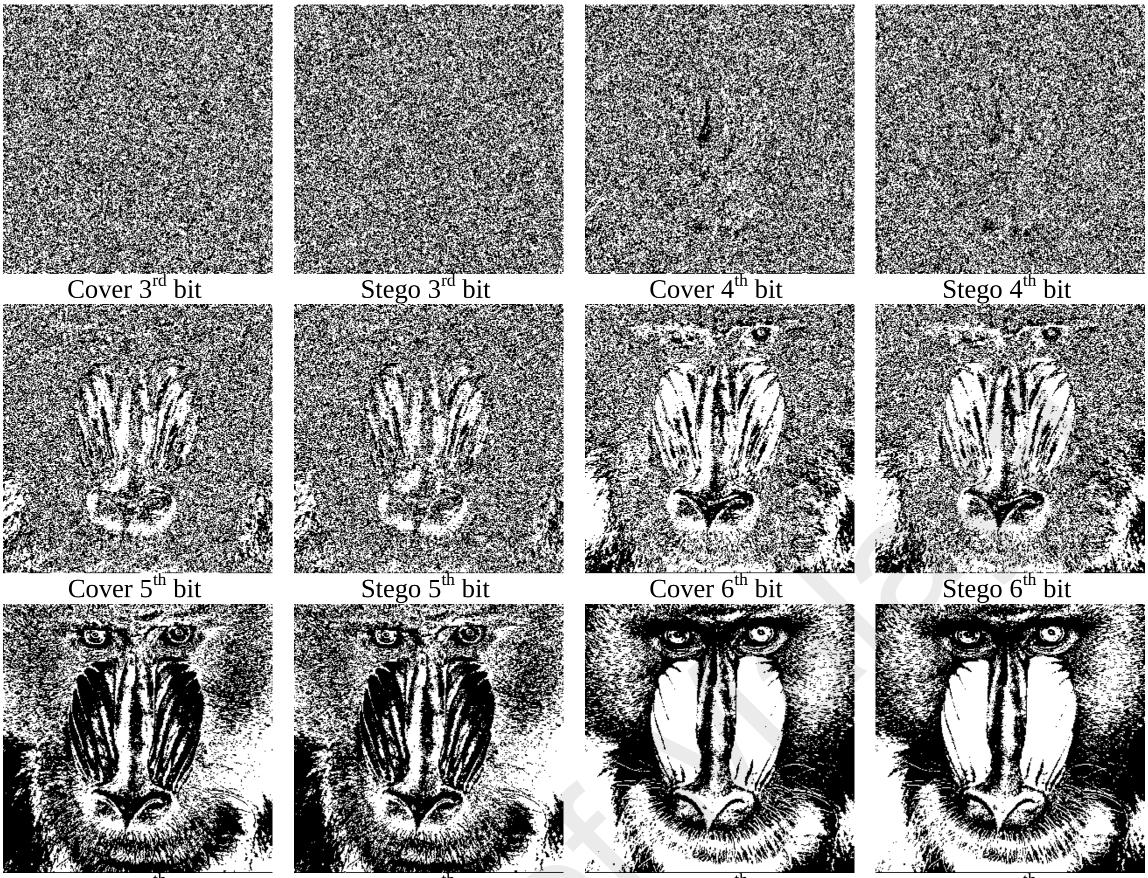
Cover 5th bit | Stego 5th bit | Cover 6th bit | Stego 6th bit

Cover 7th bit | Stego 7th bit | Cover 8th bit | Stego 8th bit

Figure 5.7: Bit-plane Analysis of Proposed Tri-way PBPVD Stego-image (Lena)



Cover 1st bit | Stego 1st bit | Cover 2nd bit | Stego 2nd bit



Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

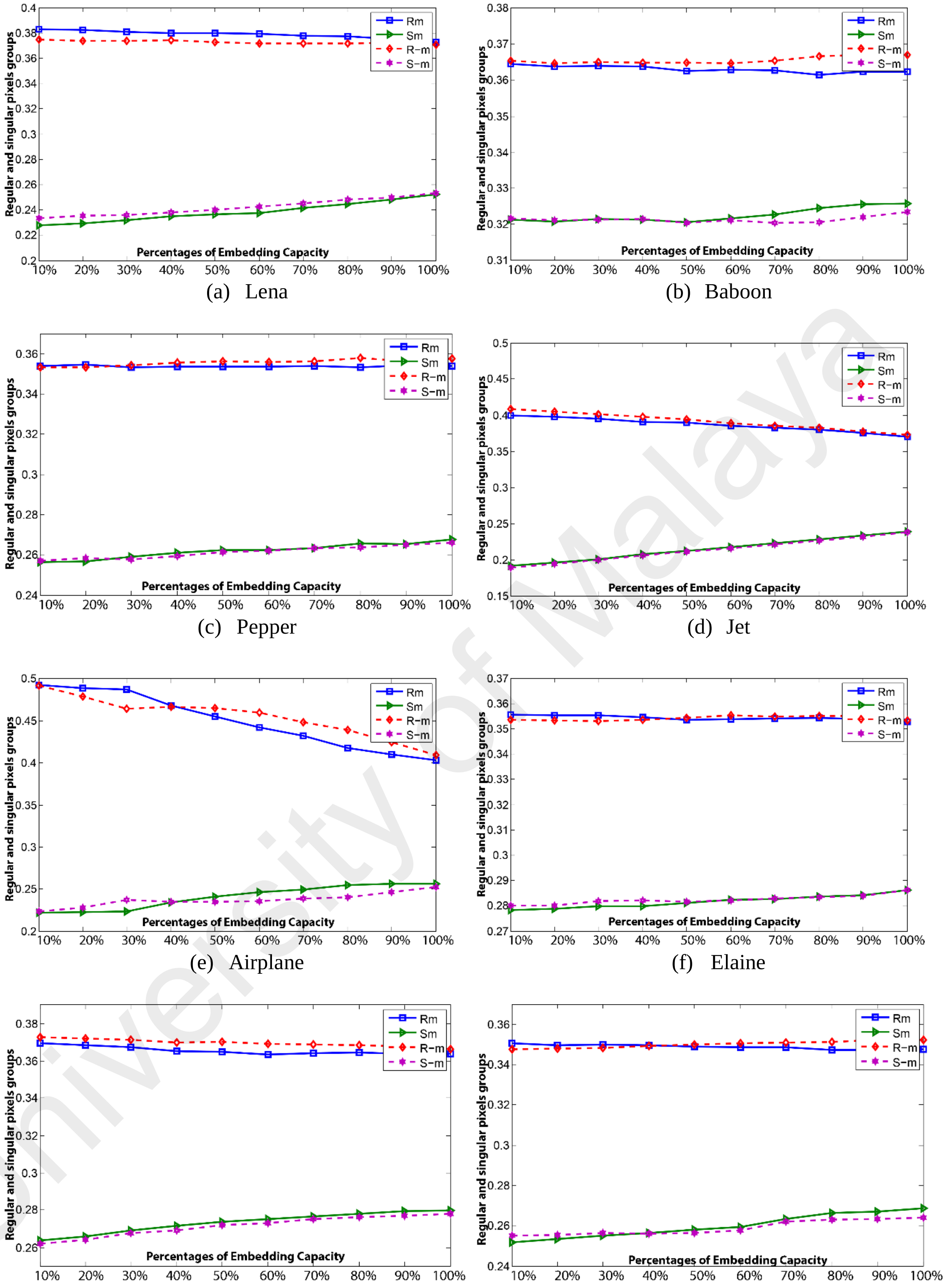
Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 5.8: Bit-plane Analysis of Proposed Tri-way PBPVD Stego-image (Baboon)

(b) ***Security under RS detection analysis***

In this analysis, Figure 5.9 presents the RS diagram of proposed PBPVD embedding. The x-axes and y-axes represent the percentage of hiding capacity and percentage of regular and singular pixels groups, respectively. Figure 5.9 (a-h) illustrate the all graphs. It is clearly noticeable that proposed PBPVD method maintained the identical curve between RM and R-M, SM and S-M parameters for all stego-images. Similarly, for Tri-way PBPVD based stego-images in Figure 5.10 (a-h) also retain the closest differences between RM and R-M, SM and S-M curves. Therefore, the overall results from Figure 5.9 to Figure 5.10 show that PBPVD and Tri-way PBPVD methods have robustness against RS detection analysis attacks. The main reason is that the proposed methods employ the pixel difference adjustment with secret data instead of substitution of secret data inside the pixels and this evades the risk of RS detection attacks.



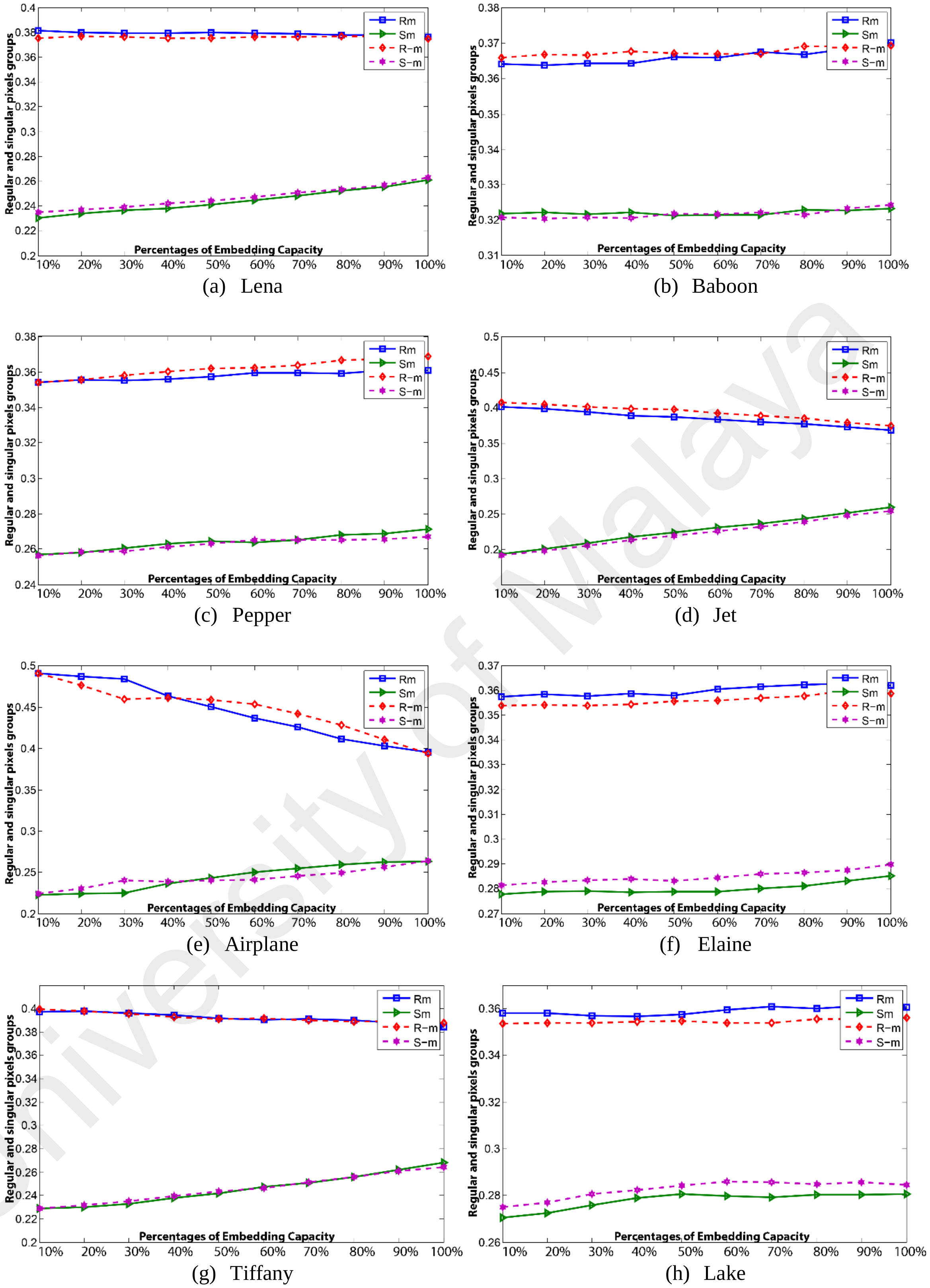
(a) Lena (b) Baboon

(c) Pepper (d) Jet

(e) Airplane (f) Elaine

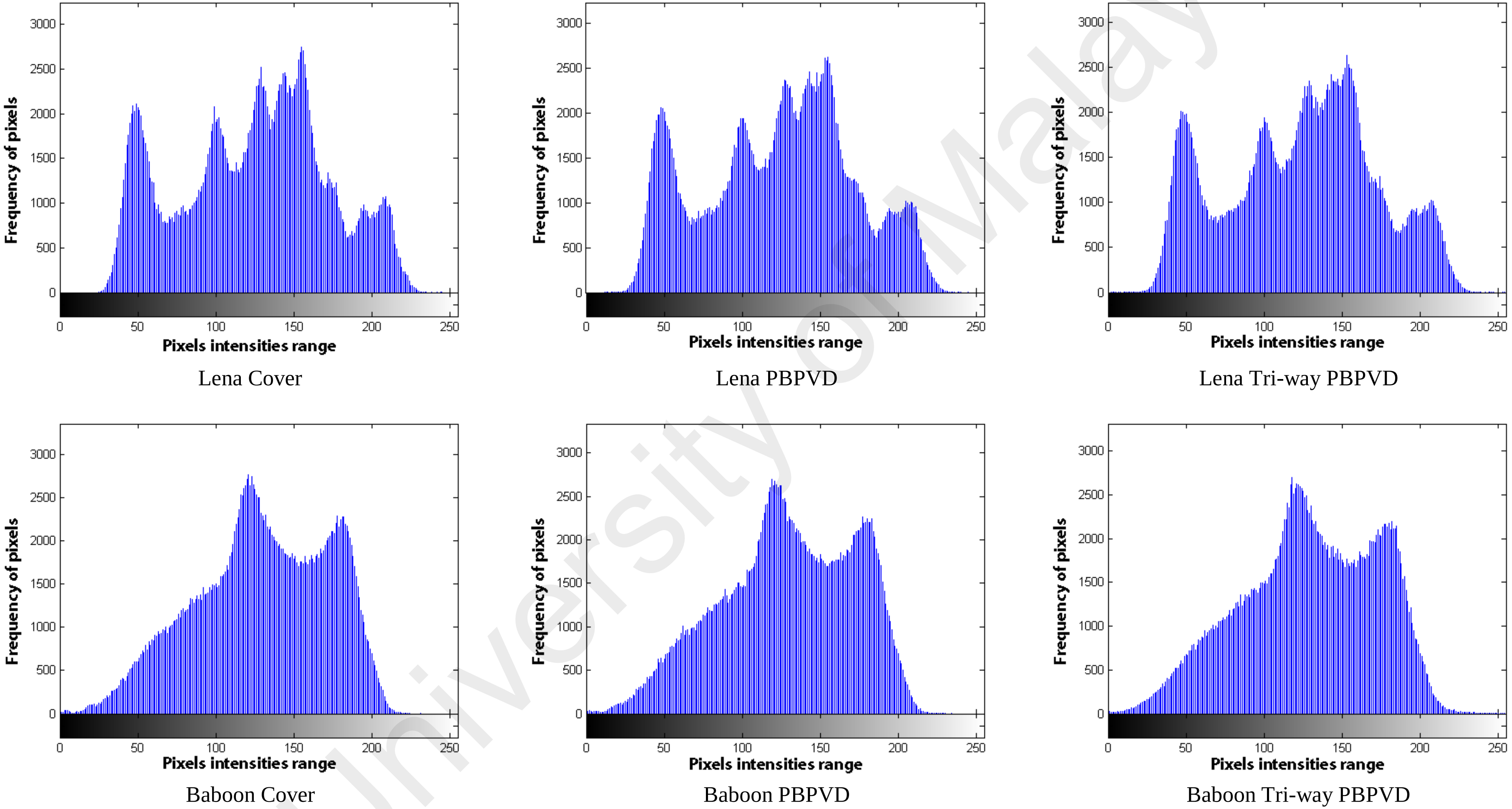
(g) Couple (h) Boat

Figure 5.9: RS Analysis Diagram for Proposed PBPVD Method



(a) Lena (b) Baboon (c) Pepper (d) Jet (e) Airplane (f) Elaine (g) Tiffany (h) Lake

Figure 5.10: RS Analysis Diagram for Proposed Tri-Way PBPVD Method



Lena Cover

Lena PBPVD

Lena Tri-way PBPVD

Baboon Cover

Baboon PBPVD

Baboon Tri-way PBPVD

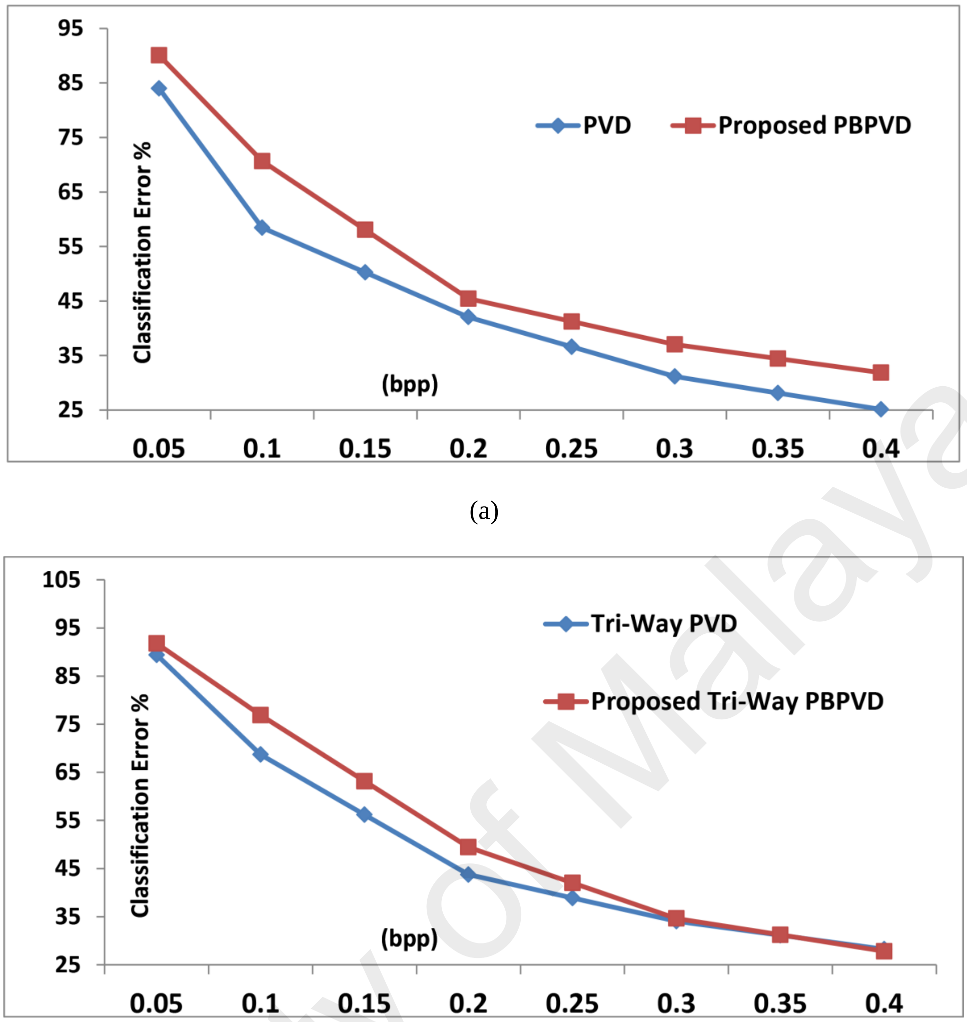
Figure 5.11: Pixel Histogram Analysis of Proposed PBPVD and Tri-Way PBPVD Methods

(c) *Pixel Histogram Analysis*

The pixel difference histogram graphs presented in Figure 5.11 for both PBPVD and Tri-way PBPVD based methods. The x-axis and y-axis represent the pixel intensity and frequency of pixels, respectively. In Figure 5.11 shows that the cover and stego-images histograms that are almost identical for both proposed PBPVD and Tri-way PBPVD based methods and also follow the similar pattern of pixels level, which indirectly to some extent evades the risk of histogram detection attacks.

(d) *Security under Ensemble Classifier using SPAM*

In this section, the security of proposed PBPVD and Tri-way PBPVD steganography methods are evaluated under SPAM based ensemble classifier for all UCID image dataset (Schaefer & Stich, 2004). Figure 5.12 illustrates the classification error of each method with 10-folded cross-validation process using WEKA tool. The 10-folded cross-validation process divides the cover and stego-images into 10 subsets, where it randomly employ each subset in training and testing process using specified classifier. In our case, we utilize the ensemble classifier using SPAM features sets of cover and stego-images to differentiate the stego-and cover images. In this experiment, the actual performance comparisons evaluated between PVD and proposed PBPVD Figure 5.12 (a), and similarly, another comparison between Tri-way PVD with proposed Tri-way PBPVD methods are shown in Figure 5.12 (b).



(a)

(b)

Figure 5.12: SPAM feature based Classification Error Rate Graph for (a) PVD vs PBPVD and (b) Tri-Way PVD vs Tri-Way PBPVD

From a critical analysis of Figure 5.12 (a), this depicts that proposed PBPVD classification error (■) curve is throughout higher than PVD based classification error (◆) curve. As mentioned before, the higher classification error rate means the higher robustness against steganalysis attacks. Similarly, Figure 5.12 (b) also depicts that the proposed Tri-way PBPVD classification error (■) curve is higher than the traditional Tri-way PVD (◆) curve. From the above results, it proved that proposed PBPVD-based embedding techniques showed the better robustness against PVD-based methods. This is because of employing the efficient adjustment process in proposed PBPVD-based methods.

5.3 PBPVD-based Adaptive Hybrid Steganography Method

In this section, we present a PBPVD-based hybrid embedding method that achieves the optimal embedding capacity, imperceptibility and improve the robustness against steganalysis detection attacks. This section contains the proposed hybrid embedding and extracting algorithms. It also evaluates the performances between proposed and existing PVD-based hybrid methods.

The proposed hybrid method exploits the basic texture features to embed the secret data using PBPVD (section 5.2) and RMDR (section 4.2) methods. To the best of our knowledge, this is the first demonstration of combining the digit substitutions based technique with the pixel differencing method in image steganography domain. The proposed hybrid method is expected to simultaneously improve the embedding capacity and imperceptibility, as well as to maintain the basic structural and statistical steganalysis security against existing PVD-based hybrid methods. The proposed method consists of two main embedding and extracting phases, which are described in the subsections below.

5.3.1 PBPVD-based Adaptive Hybrid Embedding Method

The proposed PBPVD-based hybrid embedding method partitioned the cover image into two consecutive non-overlapped pixels blocks. Similar to our previously proposed hybrid method (in section 4.2), the current PBPVD-hybrid technique also utilized the pixels differences of blocks to determine the region levels (with sub-range of Table 5.8). When the difference value of the block exists in the level of region-1, proposed hybrid technique employs the RMDR (section 4.1.1) embedding method on respective block. Conversely, for region-2, the PBPVD (section 5.2.1) technique is employed for embedding the secret data. The overall process of the proposed hybrid embedding method is illustrated in Figure 5.13 and the embedding steps are listed in Table 5.9.

Table 5.8: Proposed PBPVD-based Hybrid Method Range Table Divisions as Region-1 and Region-2 Levels

Regions	**Region-1 Level**	**Region-2 Level**		
Lower-Upper bound of *Rk*	$R_1 \in [0, 31]$	$R_2 \in [32, 63]$	$R_3 \in [64, 127]$	$R_4 \in [128, 255]$
Secret bits	6	6	7	8

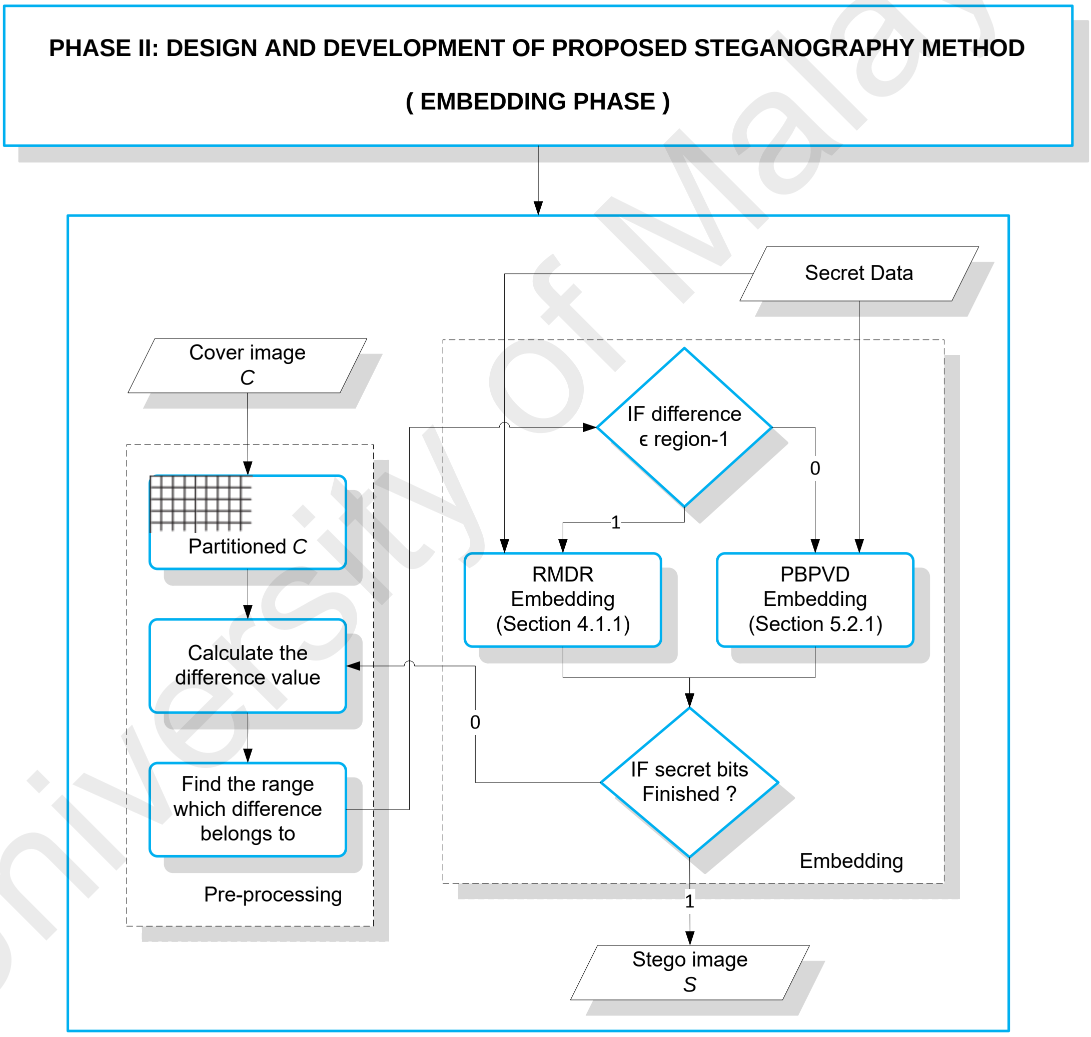
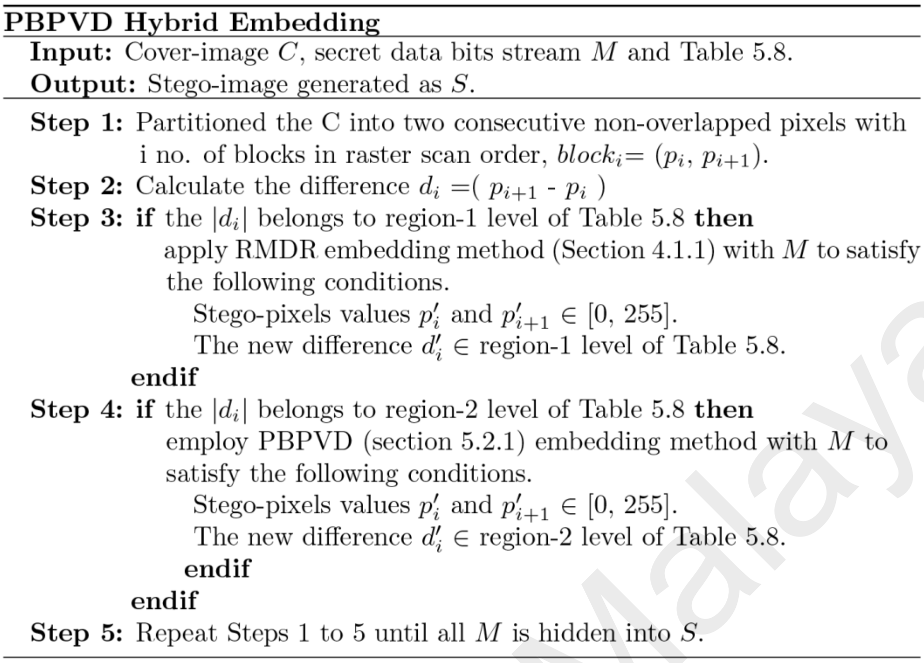


Figure 5.13: A Basic Flowchart of Proposed PBPVD-based Hybrid Embedding Method

Table 5.9: Proposed PBPVD-based Hybrid Embedding Steps



```
PBPVD Hybrid Embedding
  Input: Cover-image $C$, secret data bits stream $M$ and Table 5.8.
  Output: Stego-image generated as $S$.
  Step 1: Partitioned the C into two consecutive non-overlapped pixels with
          i no. of blocks in raster scan order, $block_i$= ($p_i$, $p_{i+1}$).
  Step 2: Calculate the difference $d_i$ =( $p_{i+1}$ - $p_i$ )
  Step 3: if the $|d_i|$ belongs to region-1 level of Table 5.8 then
            apply RMDR embedding method (Section 4.1.1) with $M$ to satisfy
            the following conditions.
              Stego-pixels values $p'_i$ and $p'_{i+1} \in [0, 255]$.
              The new difference $d'_i \in$ region-1 level of Table 5.8.
          endif
  Step 4: if the $|d_i|$ belongs to region-2 level of Table 5.8 then
            employ PBPVD (section 5.2.1) embedding method with $M$ to
            satisfy the following conditions.
              Stego-pixels values $p'_i$ and $p'_{i+1} \in [0, 255]$.
              The new difference $d'_i \in$ region-2 level of Table 5.8.
            endif
          endif
  Step 5: Repeat Steps 1 to 5 until all $M$ is hidden into $S$.
```

5.3.2 PBPVD-based Adaptive Hybrid Extracting Method

This PBPVD-based hybrid extraction method requires the stego-image as input and the range table division as listed in Table 5.8. Similar to above embedding process, this hybrid extraction process partitioned the stego-image into two non-overlapped pixels block. If the difference of these non-overlapped pixels block belong to region-1 levels (of Table 5.8), the RMDR (section 4.1.2) extraction method employed to recover the secret data. Conversely, the PBPVD (section 5.2.2) extraction process used to recover the secret bits from selected block. The complete extraction steps of PBPVD-based hybrid method are presented in Table 5.10, and the basic flow chart is illustrated in Figure 5.14.

Table 5.10: Proposed PBPVD-based Hybrid Extracting Steps

```
PBPVD Hybrid Extracting
  Input:  Stego-image $S$ and Table 5.8.
  Output: Secret recovered data bits stream $M$.
  Step 1: Partitioned the $S$ into i no. of blocks with two consecutive pixels in
          raster scan order, where $block_i$ =($p'_i, p'_{i+1}$ ).
  Step 2: Compute the difference $d'_i$= ($p'_{i+}$ $- p'_i$ ).
  Step 3: If the $|d'_i|$ belongs to region-1 of Table 5.8 then
             Apply RMDR extraction (section 4.1.2)
          else
             Apply PBPVD extraction (section 5.2.2)
          endif
  Step 4: Repeat the Step 1 to 4 until the all secret data is extracted from $S$.
```

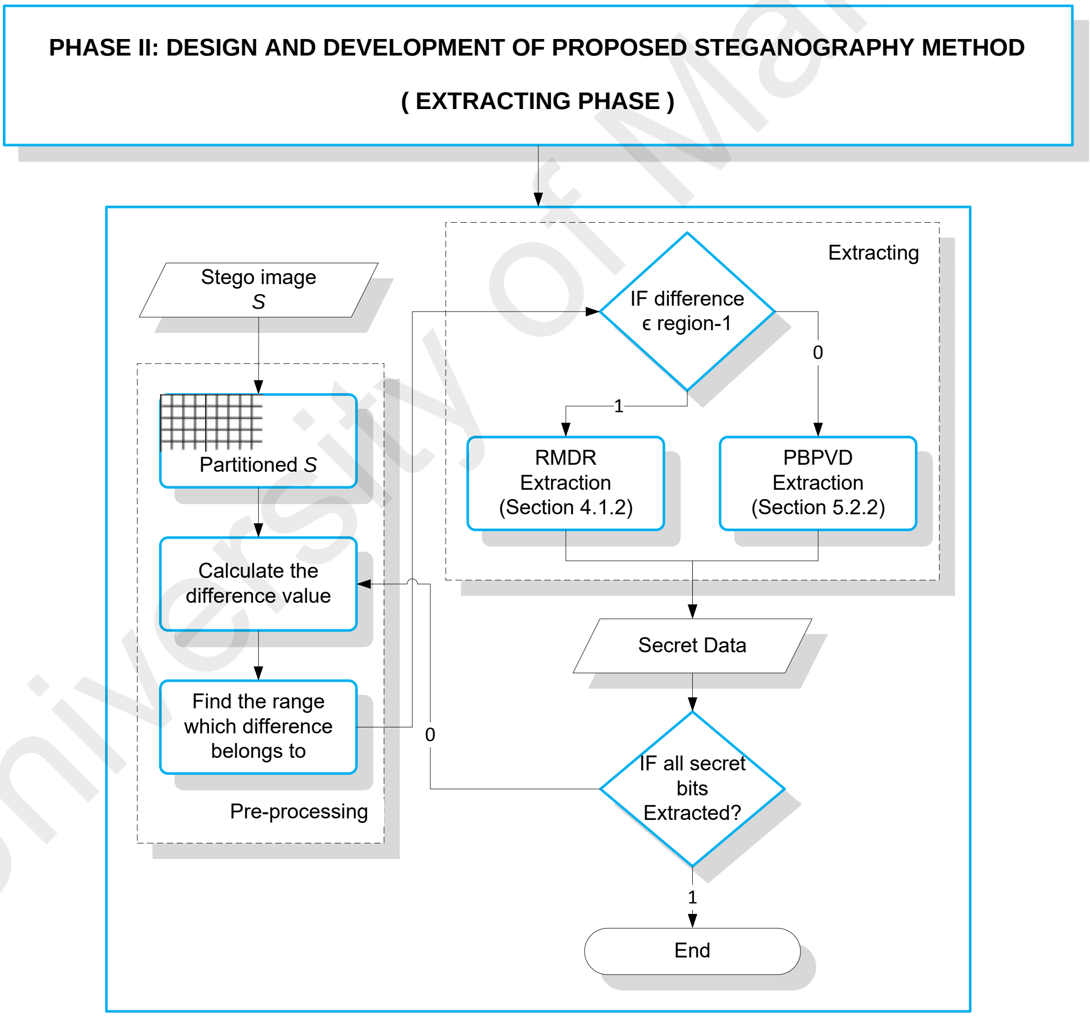

PHASE II: DESIGN AND DEVELOPMENT OF PROPOSED STEGANOGRAPHY METHOD
(EXTRACTING PHASE)
Stego image
S
Partitioned S
Calculate the difference value
Find the range which difference belongs to
Pre-processing
Extracting
IF difference ϵ region-1
1
0
RMDR Extraction (Section 4.1.2)
PBPVD Extraction (Section 5.2.2)
Secret Data
IF all secret bits Extracted?
0
1
End

Figure 5.14: A Basic Flowchart of Proposed PBPVD-based Hybrid Extracting Method

5.3.3 Experimental Results and Analysis

In this section, the experimental results of the proposed PBPVD-based hybrid embedding method are presented. Similar to previous experiments (section 5.2.3), we performed various types of tests to evaluate the performance of the proposed hybrid method with respect to all general evaluation criteria i.e., visual quality, embedding capacity, undetectability/security.

5.3.3.1 Dataset and Setup

For extensive experiments, we employed both UCID (Schaefer & Stich, 2004) and USC-SIPI (USC-SIPI, 2016) image datasets. We followed the similar evaluation methods as in section 5.2.3 to measure the performance regarding embedding capacity, visual quality and security. This section also divided into two sets of experiments, first analyzes or evaluates the embedding capacity and visual quality. Secondly, evaluate the security/undetectability against steganalysis of proposed hybrid method. Meanwhile, the security performance of proposed method is also evaluated by modern SPAM feature based steganalysis using ensemble classification.

5.3.3.2 Embedding Capacity and Visual Quality Evaluation

This section analyzes the performance of proposed PBPVD-based hybrid embedding method regarding capacity and visual quality in two aspects. First, it compared the performance with well-known existing PVD-based hybrid methods i.e., PVD+LSB and PVD+ALSB (M Khodaei & Faez, 2012; H-C Wu et al., 2005; C.-H. Yang, Weng, et al., 2010). Secondly, proposed PBPVD-based hybrid method compared with recent pixel pair difference based steganography methods with respect to capacity and visual quality i.e. (J. Chen, 2014; Jung & Yoo, 2015a; S.-Y. Shen & Huang, 2015; Xin, Qiaoyan, & Zhang, 2012). In the end of this section, for extensive performance evaluation, aforementioned methods are evaluated over larger image datasets.

(a) ***Performance of Embedding Capacity and Visual Quality***

In this experiment, proposed PBPVD-based hybrid method is compared with existing PVD-based hybrid methods as shown in Table 5.11. From the analysis, proposed hybrid method gained the highest average PSNR value (+38.84), while the embedding capacity is ranked second after the (M Khodaei & Faez, 2012) method. As compared to (M Khodaei & Faez, 2012), proposed method gained the average PSNR up to +1.84%, while bpp reduces up to -0.02. Although the (M Khodaei & Faez, 2012) method has higher capacity, it leaves the distortion artifacts on the stego-images and becomes vulnerable to histogram detection see section 5.3.3.3 (c).

Table 5.11: Performance Comparison of Proposed PBPVD-based Hybrid Method with Existing PVD-based Hybrid Methods

Images	**Methods**	**Capacity (bits)**	**PSNR (dB)**	**Bits/pixel (bpp)**	**Q**
Lena	(H-C Wu et al., 2005)	765,968	37.11	2.92	0.9973
	(C.-H. Yang, Weng, et al., 2010)	765,968	38.74	2.92	0.9981
	(M Khodaei & Faez, 2012)	791,443	37.56	3.02	0.9975
	Hybrid PBPVD	787,234	39.09	3.00	0.9983
Baboon	(H-C Wu et al., 2005)	717,752	35.27	2.74	0.9947
	(C.-H. Yang, Weng, et al., 2010)	717,752	35.87	2.74	0.9955
	(M Khodaei & Faez, 2012)	809,435	34.85	3.09	0.9940
	Hybrid PBPVD	790,552	36.90	3.02	0.9963
Pepper	(H-C Wu et al., 2005)	768,456	37.23	2.93	0.9979
	(C.-H. Yang, Weng, et al., 2010)	768,456	38.91	2.93	0.9985
	(M Khodaei & Faez, 2012)	790,299	35.88	3.01	0.9971
	Hybrid PBPVD	785,544	39.11	3.00	0.9986
Jet	(H-C Wu et al., 2005)	770,176	37.00	2.94	0.9970
	(C.-H. Yang, Weng, et al., 2010)	770,176	38.55	2.94	0.9979
	(M Khodaei & Faez, 2012)	792,443	36.29	3.02	0.9965
	Hybrid PBPVD	786,823	38.55	3.00	0.9979

Table 5.11, continued.

Images	Methods	Capacity (bits)	PSNR (dB)	Bits/pixel (bpp)	Q
Tank	(H-C Wu et al., 2005)	768,712	37.40	2.93	0.9920
	(C.-H. Yang, Weng, et al., 2010)	768,712	39.24	2.93	0.9947
	(M Khodaei & Faez, 2012)	788,107	38.36	3.01	0.9936
	Hybrid PBPVD	786,522	39.60	3.00	0.9951
Airplane	(H-C Wu et al., 2005)	782,312	37.40	2.98	0.9881
	(C.-H. Yang, Weng, et al., 2010)	782,312	39.70	2.98	0.9929
	(M Khodaei & Faez, 2012)	788,227	38.29	3.01	0.9903
	Hybrid PBPVD	786,969	39.29	3.00	0.9923
Truck	(H-C Wu et al., 2005)	773,408	37.54	2.95	0.9923
	(C.-H. Yang, Weng, et al., 2010)	773,408	39.57	2.95	0.9951
	(M Khodaei & Faez, 2012)	787,157	38.61	3.00	0.9939
	Hybrid PBPVD	786,434	39.71	3.00	0.9953
Elaine	(H-C Wu et al., 2005)	760,168	37.29	2.90	0.9971
	(C.-H. Yang, Weng, et al., 2010)	760,168	38.90	2.90	0.9980
	(M Khodaei & Faez, 2012)	788,356	38.17	3.01	0.9977
	Hybrid PBPVD	786,619	39.58	3.00	0.9983
Couple	(H-C Wu et al., 2005)	762,056	36.86	2.91	0.9964
	(C.-H. Yang, Weng, et al., 2010)	762,056	38.33	2.91	0.9973
	(M Khodaei & Faez, 2012)	795,729	36.63	3.04	0.9964
	Hybrid PBPVD	787,221	38.48	3.00	0.9977
Boat	(H-C Wu et al., 2005)	755,000	36.45	2.88	0.9967
	(C.-H. Yang, Weng, et al., 2010)	755,000	37.61	2.88	0.9975
	(M Khodaei & Faez, 2012)	795,458	34.93	3.03	0.9952
	Hybrid PBPVD	786,887	38.16	3.00	0.9977
Tiffany	(H-C Wu et al., 2005)	766,664	37.27	2.92	0.9929
	(C.-H. Yang, Weng, et al., 2010)	766,664	38.96	2.92	0.9952
	(M Khodaei & Faez, 2012)	790,503	37.78	3.02	0.9937
	Hybrid PBPVD	784,411	39.15	2.99	0.9954
Lake	(H-C Wu et al., 2005)	750,312	36.60	2.82	0.9984
	(C.-H. Yang, Weng, et al., 2010)	750,312	37.84	2.86	0.9988
	(M Khodaei & Faez, 2012)	795,471	36.36	3.02	0.9983
	Hybrid PBPVD	787,220	38.47	3.00	0.9989
Average	(H-C Wu et al., 2005)	761,749	36.95	2.91	0.9951
	(C.-H. Yang, Weng, et al., 2010)	761,749	38.51	2.91	0.9965
	(M Khodaei & Faez, 2012)	**792,719**	36.98	**3.02**	0.9954
	Hybrid PBPVD	786,870	**38.84**	3.00	0.9968

Table 5.12: Comparisons of Proposed PBPVD-based Hybrid with other Recent Pixels Pair-Based Embedding Methods

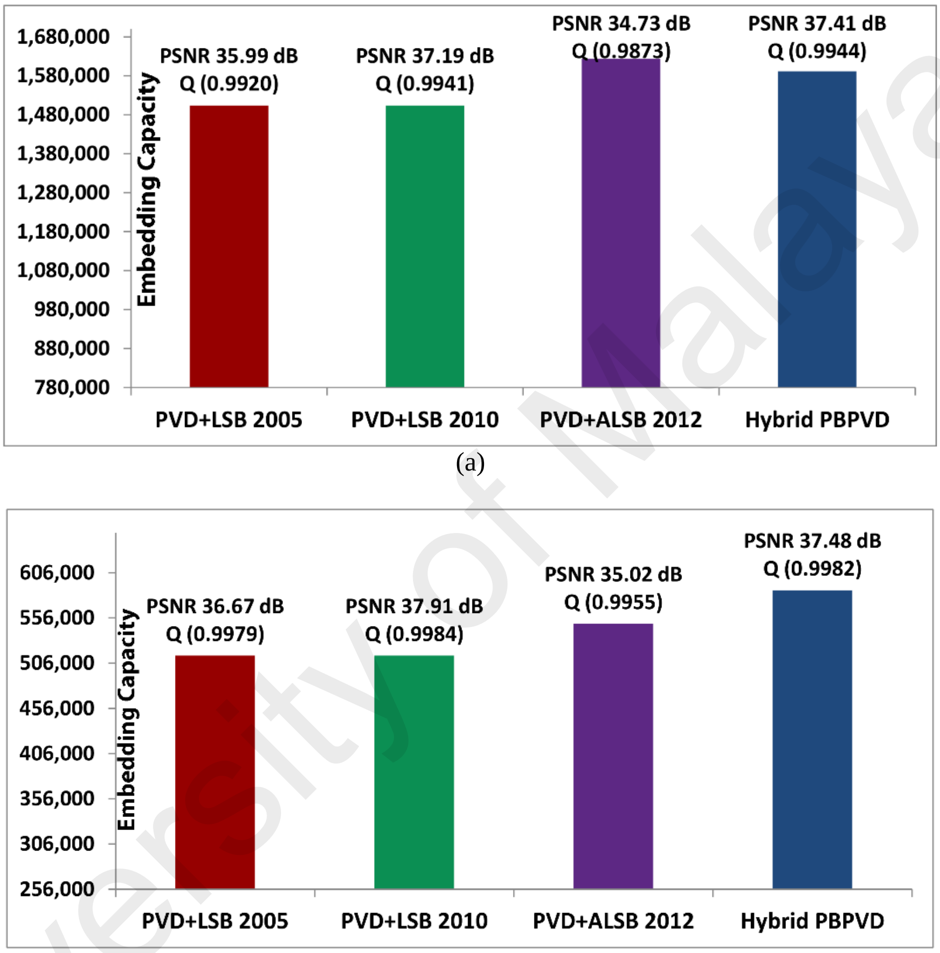
Images	**Methods**	**Capacity (bits)**	**PSNR (dB)**	**Bits/pixel (bpp)**
Lena	(S.-Y. Shen & Huang, 2015)	402,485	42.46	1.54
	(J. Chen, 2014)	650,408	42.30	2.48
	(Xin et al., 2012)	561,740	41.18	2.14
	(Jung & Yoo, 2015a)	614,799	31.94	2.35
	(Grajeda-Marín et al., 2016)	616,038	39.34	2.35
	PBPVD-based Hybrid	787,234	39.09	3.00
Baboon	(S.-Y. Shen & Huang, 2015)	443,472	38.88	1.69
	(J. Chen, 2014)	735,080	41.20	2.80
	(Xin et al., 2012)	691,735	35.61	2.64
	(Jung & Yoo, 2015a)	686,220	25.96	2.62
	(Grajeda-Marín et al., 2016)	685,845	36.38	2.61
	PBPVD-based Hybrid	790,552	36.90	3.02
Pepper	(S.-Y. Shen & Huang, 2015)	401,088	42.68	1.53
	(J. Chen, 2014)	674,804	41.97	2.57
	(Xin et al., 2012)	562,249	41.28	2.14
	(Jung & Yoo, 2015a)	611,394	30.42	2.33
	(Grajeda-Marín et al., 2016)	613,495	39.14	2.34
	PBPVD-based Hybrid	785,544	39.11	3.00
Jet	(S.-Y. Shen & Huang, 2015)	404,945	42.17	1.54
	(J. Chen, 2014)	622,200	43.00	2.37
	(Xin et al., 2012)	589,595	40.10	2.25
	(Jung & Yoo, 2015a)	614,826	30.66	2.35
	(Grajeda-Marín et al., 2016)	616,038	38.59	2.35
	PBPVD-based Hybrid	786,823	38.55	3.00
Average	(S.-Y. Shen & Huang, 2015)	412,998	41.55	1.58
	(J. Chen, 2014)	670,623	**42.12**	2.56
	(Xin et al., 2012)	601,329	39.54	2.29
	(Jung & Yoo, 2015a)	631,810	29.74	2.41
	(Grajeda-Marín et al., 2016)	632,854	38.36	2.41
	PBPVD-based Hybrid	**787,538**	38.41	**3.00**

Furthermore, the performance of proposed PBPVD-based hybrid method evaluated with recent pixels pair-based differencing approaches (J. Chen, 2014; Grajeda-Marín et al., 2016; Jung & Yoo, 2015a; S.-Y. Shen & Huang, 2015; Xin et al., 2012) as shown in Table 5.12. The embedding capacity and PSNR values for comparison directly obtained from the aforementioned studies. The proposed method outperforms the compared methods in term of embedding capacity, while maintaining the acceptable (+38 dB) PSNR value. Although the method by (J. Chen, 2014) has higher PSNR, while the proposed hybrid method significantly gained/improved the (17.43%) +116,915 secret bits in terms of embedding capacity.

In conclusion, the proposed hybrid method achieved the balance in steganography objectives and considered as an optimal steganography solution. It proves more robustness (see section 5.3.3.3) against steganalysis detection attacks while retaining higher embedding capacity and acceptable PSNR as compared to existing PVD-based and pixel pair-based steganography methods (J. Chen, 2014; M Khodaei & Faez, 2012; S.-Y. Shen & Huang, 2015; H-C Wu et al., 2005; C.-H. Yang, Weng, et al., 2010).

(b) ***Performance over UCID and USC-SIPI Image Datasets***

For extensive performance evaluation of capacity and visual quality of proposed method, we employed the complete UCID (Schaefer & Stich, 2004) and SIPI (USC-SIPI, 2016) image datasets as shown in Figure 5.15, where the x-axis and y-axis represent the embedding methods and embedding bits, respectively. In this test, proposed method is compared with existing hybrid PVD+LSB (H-C Wu et al., 2005), PVD+LSB (C.-H. Yang, Weng, et al., 2010), and PVD+ALSB (M Khodaei & Faez, 2012) embedding methods. From Figure 5.15 (a) graph, the proposed method gained the higher visual quality (PSNR and Q statistics) against all compared methods over SIPI images. Although the embedding capacity of PVD+ALSB (M Khodaei & Faez, 2012) method is higher than proposed technique, but the security of PVD+ALSB method is lower than proposed method. Furthermore, in Figure 5.15 (b), graph shows that the proposed method is able to retain the higher steganography objectives as compared to all other methods over UCID image dataset. In conclusion, the proposed hybrid method proved the better results in term of capacity and visual quality on both types of SIPI and UCID image datasets.



(a)

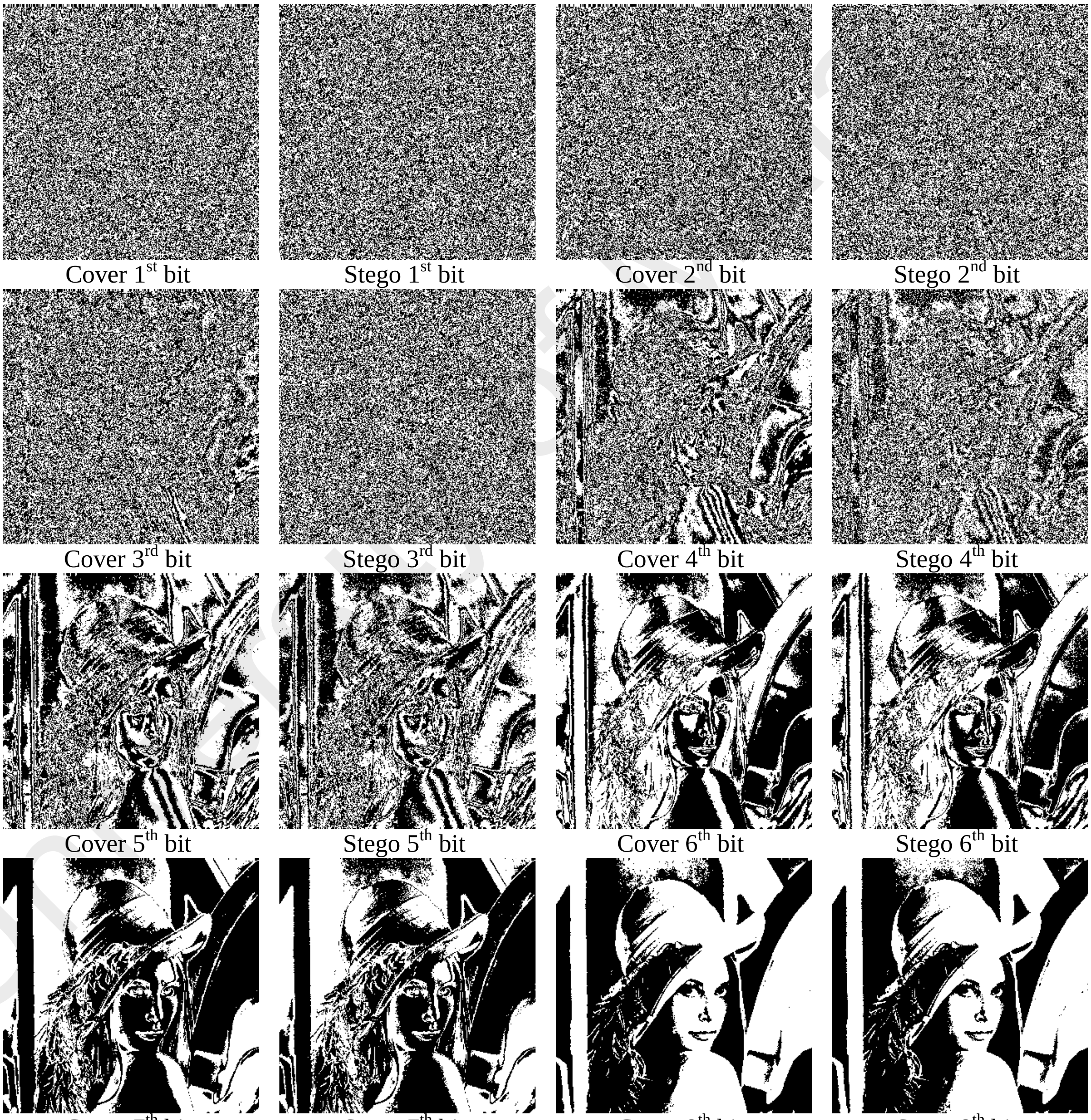
(b)

Figure 5.15: Performance Comparison of Proposed PBPVD-based Hybrid Method over (a) SIPI (USC-SIPI, 2016) (b) UCID (Schaefer & Stich, 2004) Datasets.

5.3.3.3 Security/Un-detectability Evaluation

(a) ***Bit-plane Analysis***

In this section, we evaluate the performance of proposed PBPVD-based hybrid method against bit-plane analysis, where the bit-plane of Lena and Baboon stego-images are shown in Figure 5.16 and Figure 5.17, respectively. Both figures illustrated that the visual quality of each bit plane between the cover and respective stego-images are similar to each other. The reason is that, proposed hybrid technique takes the advantage of efficient employing of RMDR and PBPVD techniques based on image textures, which indirectly modifies the pixels in adaptive manners instead of constant rate of embedding. This concludes that proposed PBPVD-based hybrid stego-images can also resist the visual bit-plane analysis detection attacks.



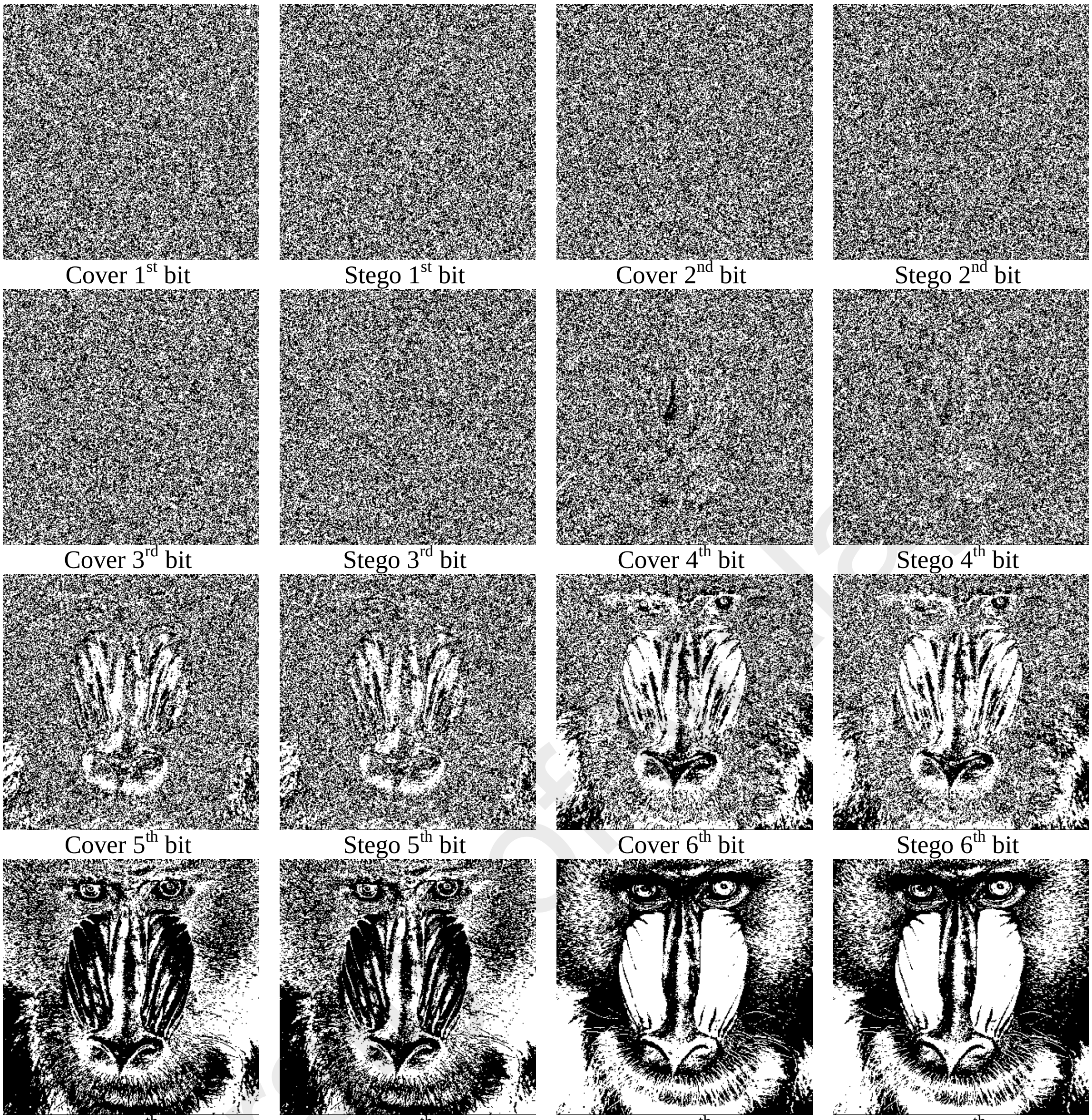
Cover 1st bit Stego 1st bit Cover 2nd bit Stego 2nd bit

Cover 3rd bit Stego 3rd bit Cover 4th bit Stego 4th bit

Cover 5th bit Stego 5th bit Cover 6th bit Stego 6th bit

Cover 7th bit Stego 7th bit Cover 8th bit Stego 8th bit

Figure 5.16: Bit-plane Analysis of Proposed PBPVD-based Hybrid Stego-image (Lena)



Cover 1st bit | Stego 1st bit | Cover 2nd bit | Stego 2nd bit

Cover 3rd bit | Stego 3rd bit | Cover 4th bit | Stego 4th bit

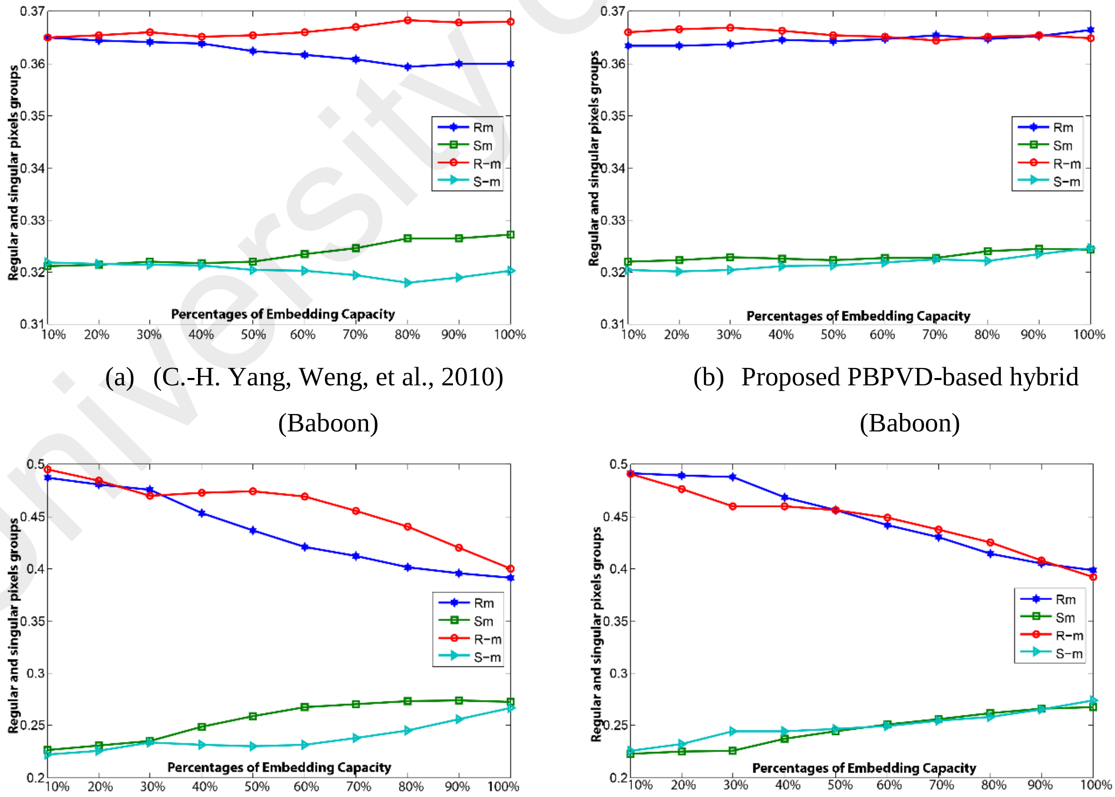
Cover 5th bit | Stego 5th bit | Cover 6th bit | Stego 6th bit

Cover 7th bit | Stego 7th bit | Cover 8th bit | Stego 8th bit

Figure 5.17: Bit-plane Analysis of Proposed PBPVD-based Hybrid Stego-image (Baboon)

(b) ***Security under RS detection analysis***

In this section, we present the RS detection analysis of proposed PBPVD-based hybrid and existing hybrid PVD+LSB (C.-H. Yang, Weng, et al., 2010) methods. The RS analysis graphs are shown in Figure 5.18. It is clearly observable from the resultant graphs that both techniques are able to resist the RS steganalysis attacks. However, in proposed method, the RS detection parameters/groups (i.e. Rm with R-m and Sm with S-m) differences curves are extremely close to each other that considered a high security. Conversely, the Yang et al. approach has the higher differences in Rm and Rm, Sm and S-m (C.-H. Yang, Weng, et al., 2010) curves that depicts the lower resistance against RS detection attacks. Furthermore, Table 5.13 presents the *maximum differences* of Rm and R-m, Sm and S-m values for proposed and (M Khodaei & Faez, 2012; C.-H. Yang, Weng, et al., 2010) steganography methods. As observed from graphs results that the smallest differences in these parameters/groups considered a highest security of a steganography method. From Table 5.13, the statistical analysis proved that the proposed PBPVD-based hybrid and (M Khodaei & Faez, 2012) methods retain the minimum differences in both regular (0.18%) and singular groups (0.14%) for all images. On the other side, (C.-H. Yang, Weng, et al., 2010) has a slightly higher differences for both regular (0.26%) and singular (0.22%) groups. As a result, the proposed PBPVD-based hybrid method has the smallest differences, thereby indicating the fewer detection artifacts that increase the capability to resist the RS-steganalysis.



(a) (C.-H. Yang, Weng, et al., 2010) (Baboon)

(b) Proposed PBPVD-based hybrid (Baboon)

(c) (C.-H. Yang, Weng, et al., 2010) (Airplane)

(d) Proposed PBPVD-based hybrid (Airplane)

Figure 5.18: RS-Analysis Graphs for Proposed PBPVD-based Hybrid vs. (C.-H. Yang, Weng, et al., 2010) (a-d).

Table 5.13: Maximum Differences between RS Analysis Groups

Images	(C.-H. Yang, Weng, et al., 2010)		(M Khodaei & Faez, 2012)		Proposed hybrid PBPVD	
	$\lvert R_M - R_{-M} \rvert$	$\lvert S_M - S_{-M} \rvert$	$\lvert R_M - R_{-M} \rvert$	$\lvert S_M - S_{-M} \rvert$	$\lvert R_M - R_{-M} \rvert$	$\lvert S_M - S_{-M} \rvert$
Lena	0.2074	0.1604	0.0716	0.0579	0.0743	0.0539
Baboon	0.0879	0.0864	0.0294	0.0174	0.0255	0.0230
Pepper	0.1176	0.1105	0.0423	0.0617	0.0539	0.0235
Jet	0.1492	0.1256	0.0699	0.0356	0.0967	0.0615
Tank	0.6906	0.5647	0.6988	0.5762	0.6998	0.5801
Airplane	0.4579	0.3394	0.2576	0.1661	0.2837	0.1860
Truck	0.1376	0.1199	0.8131	0.6532	0.8080	0.6487
Elaine	0.1553	0.1236	0.0378	0.0295	0.0447	0.0644
Couple	0.1491	0.1405	0.0713	0.0438	0.0523	0.0302
Boat	0.7857	0.6390	0.0312	0.0275	0.0357	0.0427
Tiffany	0.1407	0.1228	0.0698	0.0576	0.0461	0.0383
Lake	0.0995	0.1068	0.0408	0.0386	0.0261	0.0429
Average	0.2649	0.2200	0.1861	0.1471	0.1872	0.1496

(c) ***Pixel Difference Histogram Analysis***

In this section, we presented the pixel difference histogram of proposed PBPVD-based hybrid and existing hybrid (M Khodaei & Faez, 2012; C.-H. Yang, Weng, et al., 2010) steganography techniques as shown in Figure 5.19. The pixel difference histogram is computed by taking the differences of neighboring pixels with fall-off (±5) ranges between cover and stego-image. From keenly observation, the proposed and existing (M Khodaei & Faez, 2012; C.-H. Yang, Weng, et al., 2010) methods followed the similar to cover histogram curves as shown in Figure 5.19. However, the proposed hybrid method can retain the almost identical histogram curves between cover and its stego-images. For detail view, the visual asymmetry of the curves can be seen in the top left corner of each graph.

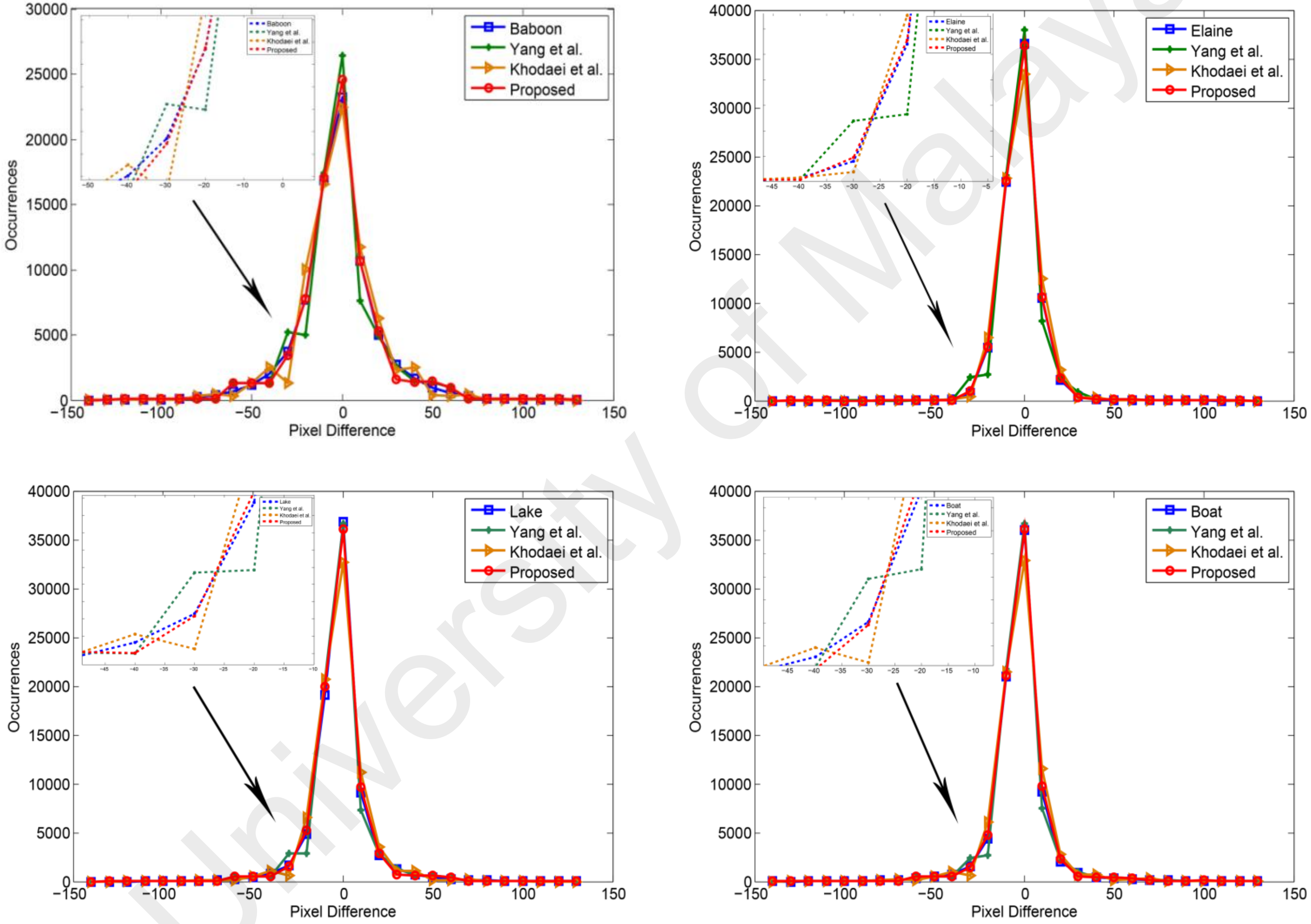


Figure 5.19: Pixel Difference Histograms of PBPVD-based Hybrid, (C.-H. Yang, Weng, et al., 2010) and (M Khodaei & Faez, 2012) Methods (a-d).

Furthermore, Table 5.14 presents the statistics of each image that exhibits the maximum displacement/variation of the pixel differences between the cover and respective stego-image. The variation of the average pixel difference histogram in the proposed method retained the lowest (5573) value as compared to (C.-H. Yang, Weng, et al., 2010) (6739) and (M Khodaei & Faez, 2012) (9586) values. Therefore, the proposed method can be considered the more secure than the other methods, because it maintains the symmetry of the pixel difference histogram and further reduces the detectable artifacts for histogram steganalysis detection attacks.

Table 5.14: Maximum Displacement of Pixel Difference Histograms between Proposed PBPVD-based Hybrid and Compared Methods

Images	(C.-H. Yang, Weng, et al., 2010)	(M Khodaei & Faez, 2012)	Proposed hybrid PBPVD
	|Cover-histogram – Stego-histogram|	|Cover-histogram – Stego-histogram|	|Cover-histogram – Stego-histogram|
Lena	5154	9000	4652
Baboon	3249	2387	1390
Pepper	1875	5501	1401
Jet	10573	14914	9083
Tank	5089	9299	5149
Airplane	30303	33989	26867
Truck	6663	10858	6001
Elaine	2737	3127	172
Couple	3792	6915	3677
Boat	1734	3147	568
Tiffany	7729	11800	6894
Lake	1965	4095	848
Average	6739	9586	**5559**

(d) ***Security under Ensemble Classifier using SPAM***

This section evaluates the security of proposed PBPVD-based hybrid, PVD+LSB (C.-H. Yang, Weng, et al., 2010), and PVD+ALSB (M Khodaei & Faez, 2012) steganography methods. Similar to earlier sections 5.2.3.3 (d), the performance of proposed hybrid method is evaluated using modern steganalysis by employing the SPAM features using ensemble-based classification. In Figure 5.20, the classification error is evaluated by 10-folded cross-validation approach in WEKA tool. This 10-folded cross-validation randomly divides the cover and stego-images into 10 sub-sets for training and testing purpose using the SPAM feature based analysis. From Figure 5.20, this depicts that proposed PBPVD-based hybrid classification error (—×—) curve is throughout higher than the compared (—◆—, —■—) methods. As mentioned earlier, the higher classification error rate means the higher robustness against steganalysis detection attacks. Therefore, through above analysis, this shows that proposed method is able to maintain the highest robustness against (C.-H. Yang, Weng, et al., 2010) and (M Khodaei & Faez, 2012) methods and prove its security at low embedding rate.

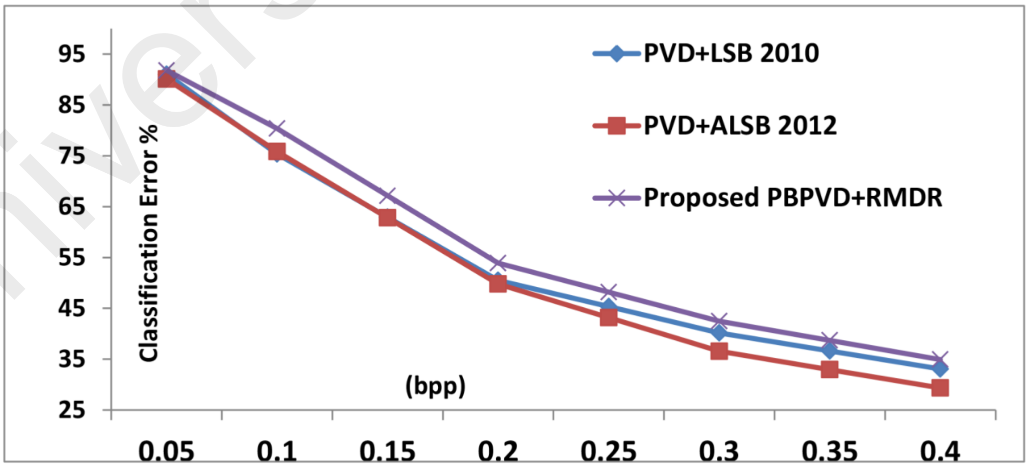


Figure 5.20: SPAM feature based Classification Error Rate Graph for PBPVD-based Hybrid, PVD+LSB (C.-H. Yang, Weng, et al., 2010), and PVD+ALSB (M Khodaei & Faez, 2012) Methods

5.4 Discussion

In this chapter, we designed two rather simple steganographic methods and tested its performances in terms of embedding capacity, visual quality and robustness against structural, statistical, and modern machine learning based steganalysis. The first method PBPVD extends the existing PVD-based methods by efficiently adjusting the pixels differences with extra secret data bits. Compared to existing PVD-based methods, this proposed solution enhanced the embedding capacity of classic and existing PVD-based methods. In addition, proposed method maintains the acceptable visual quality and reduces the steganalysis detection artifacts. In the second method, a PBPVD-based hybrid steganography is proposed, the cover image is divided into two higher and lower textures based regions that are further efficiently utilized by PBPVD and RMDR methods. The proposed solution employed the PBPVD for higher textures based areas, while RMDR employed for lower texture areas. Unlike the original hybrid, PVD+LSB based methods; proposed hybrid technique follows the HVS principle, where a higher texture area of images can embeds larger number of secret bits than lower textures. Furthermore, a newly designed range table is proposed, where the lower texture region increased from 15 to 32 without degrading the visual quality of stego-images. Consequently, both techniques record the high performance in terms of visual quality, embedding capacity and security for statistical and modern steganalysis over various types of texture based images.

5.5 Chapter Summary

In this chapter, two spatial domain image steganography methods are introduced with the aim of increasing capacity and security without degrading the visual quality. The experimental section demonstrates that both singular PBPVD and adaptive mannered hybrid (PBPVD with RMDR) embedding does also meet the stated objectives i.e. embedding capacity and visual imperceptibility. Meanwhile, the robustness of both

PBPVD and hybrid embedding methods are evaluated against well-known targeted RS, histogram and SPAM features based machine-learning steganalysis. In the light of the outcomes in this study, a parity bit adjustment process is introduced that can be employed on existing PVD-based methods to enhance their embedding capacity without degrading the visual quality and security. Meanwhile, the hybrid solution also meets the steganography objectives i.e. enhanced capacity, visual quality and reduced the steganalysis detection artifacts in stego-images. These solutions can be valuable for providing a balanced steganography as compared to existing PVD-based techniques.

CHAPTER 6: CONCLUSION AND FUTURE WORK

This chapter is concluded by a reconsideration of the objectives presented in chapter one. The goal of this chapter is to provide an important summarize contribution of this research and also presents a platform for the direction of future research.

6.1 Conclusion

Nowadays, the digital world is overwhelmed with digital multimedia content i.e. images, audios, and videos. The digital images are now everywhere due to low-cost devices (i.e. smart phones, digital camera) and also extensively used in social media applications even with limited network bandwidth. It also becomes the most favorite medium and carrier for securing data (or secret communication) by employing image steganography. This study is devoted to an investigation of existing spatial domain based image steganography techniques. It was initially motivated by protecting sensitive communication application by intelligence and law enforcing agencies. Similarly, military forces required various types of secret data exchanging through steganography. Furthermore, bank and financial sectors can employ this technology for remote authentication with certain level of secret log or key sharing protocol etc.

The main objectives of research work conducted in this thesis were the design, development and testing the performance of optimal steganography methods, where a high payload with acceptable visual quality and security was focused. In literature, many steganography methods have been proposed to achieve the general steganographic objectives by manipulating different embedding strategies, i.e. LSB, PVD, and different hybrid mechanism. However, these methods are directly or indirectly modifies the pixels intensities during the embedding process. Although, human eyes may not perceive the changes in stego-images, but the presence of secret data can be exposed by steganalysis techniques. Generally, high capacity based steganography methods led the visual distortion artifacts or produced some specific dissimilarity correlation among pixels. Therefore, steganalysis methods exploit these types of uneven statistical/structural correlations or find some variation in local characteristics of stego-image to expose the steganography techniques.

Having conducted a literature review of image steganography (in Chapter 2), several challenges were identified that faced by researchers. Apart from that, success criteria of image steganography methods were also discovered. To provide a larger embedding payload while maintaining the visual quality and security of stego-image is an immense challenge. Another demanding issue is to provide high visual quality by reducing the dissimilarity characteristics among stego-pixels. In fact, high visual quality indirectly helps to maintain security against statistical steganalysis detection attacks. However, this research aims to tackle the above challenges while achieving the optimal performance in terms of embedding capacity, visual quality, and security.

In existing spatial domain based image steganography techniques, substitution and pixel differencing methods are found to be the most popular techniques that aims the high performances in general steganography objectives. We also designed two steganography techniques based on substitution and pixel differencing namely as rightmost digit replacement (RMDR) and parity bit pixel value differencing (PBPVD) methods, respectively. In addition, we proposed their hybrid flavors to achieve the optimal performance of steganographic objectives as well.

The first RMDR steganography method (in Chapter 4) provided the high embedding capacity while enhancing the visual quality and security. The notion of RMDR embedding based on digits substitution, where the closest digits selection process improved the similarity between the cover and stego-pixels, which indirectly increases the visual quality. Compared to existing classic LSB and adaptive LSB-based methods, the RMDR embedding provides up to 3 bpp of capacity while improves (+1.85 dB PSNR) visual quality and robustness against steganalysis i.e. RS, bit-plane, pixel difference histogram and SPAM based analysis. Furthermore, RMDR-based hybrid embedding (section 4.3) achieved the optimal performance in all steganography objectives. Compared to classic LSB and adaptive LSB, the proposed hybrid method resulted in improving the payload to +13,622 and +33,593 bits, respectively. Similarly, enhanced +1.43 dB PSNR and proved the robustness against RS, bit-plane, SPAM feature based steganalysis.

The second proposed steganography (in Chapter 5) extended the PVD-based methods using an efficient parity bit adjustment process. Unlike the original PVD, proposed method mapped the secret bits with a secret selective order to accommodate the extra secret data bits in stego-image. Consequently, this method is able to improve the embedding capacity not even in classical PVD; it can also be employed in other existing PVD-based methods as proved in experimental Sections 5.2.3. Furthermore, the proposed method can maintain the original visual quality and resist the steganalysis detection attacks i.e. RS, bit-plane, histogram and SPAM steganalysis. Next, a PBPVD-based hybrid embedding solution was proposed (in Section 5.3) to achieve the optimal steganography objectives. From experimental results, PBPVD-based hybrid method maintained a high embedding capacity rate without degrading the visual quality. In addition, it can also resist the RS, bit-plane, histogram, and SPAM feature based steganalysis detection attacks. In conclusion, the proposed singular and hybrid embedding methods have succeeded in achieving the required criteria of steganography.

6.2 Reappraisal of the Research Objective

The first main objective of this study was to develop a digit substitution based spatial domain image steganography. Furthermore, sub-objective was to investigate the strength and limitations of existing LSB-based substitution techniques that were critically analyzed in Chapter 2. Another sub-objective was to develop a digits substitution based singular and hybrid steganography methods, as explained in Chapter 4 (Section 4.1 and 4.2). The RMDR method employed rightmost digit replacement with pre-processed secret digits, where the closest selection process that improved the similarity between cover and stego-pixels. Consequently, the RMDR method has improved the visual quality and security while maintained the larger embedding capacity (Section 4.1). Similarly, RMDR-based hybrid steganography proposed in Chapter 4 (Section 4.2), where it was an integration of RMDR with adaptive LSB approach. This exploited the image textures features; where the cover image was divided into two regions, i.e. higher and lower textures. Lower texture regions were efficiently employed by RMDR while higher texture embedded by adaptive LSB technique. The proposed hybrid embedding outperformed the existing LSB-based hybrid methods in order to achieve larger embedding capacity, visual quality and security over various types of image datasets such as UCID and SIPI.

The second main objective of this study was to develop a parity bit differencing spatial domain image steganography. Furthermore, the sub-objective was to investigate the strengths and limitations of existing PVD-based steganography as critically analyzed in Chapter 2. Another sub-objective was to develop parity bit pixel value difference (PBPVD) based singular and hybrid steganography methods, as explained in Chapter 5. PBPVD steganography exploited the pixels difference adjustment strategies with the correlation of secret bits in existing PVD-based methods (Section 5.2). Consequently, the PBPVD method improved the embedding capacity and security of original PVD-based methods without degrading the visual quality. Similarly, PBPVD-based hybrid steganography technique was presented by integrating PBPVD with previously proposed RMDR method in Chapter 5 (Section 5.3). This hybrid method also exploited the image textures, the higher textures based pixels groups followed the PBPVD embedding while the lower textures based pixels group employed by RMDR method. Meanwhile, this hybrid method followed the human vision principle based range table for regions division, where the higher texture (edgy) pixels group embedded more secret data instead of lower texture (less edge/smooth). The PBPVD-based hybrid approach also revealed the improvement in embedding capacity, visual quality, and security as compared to existing PVD-based hybrid methods over larger image datasets such as UCID and SIPI.

6.3 Future Research Directions

The works reported in this thesis have not only demonstrated the high embedding capacity, acceptable visual quality, and robustness of basic steganalysis methods but also highlights several potential research direction to be explored in future work. Some of them are listed as follows to improve the current methods.

6.3.1 Cover Image Selection

The fact that some performances measures are on average over a larger number of cover images. This has prompt to an incentive to adopt a credible cover-image selection process to overcome the marginal limitation on stego-images. Therefore, the investigation is required to make the more precise relationship between secret data and cover image texture, where the most suitable cover image would be chosen for embedding with respect to secret data.

6.3.2 Texture Adaptable Similarity between Cover and Stego-pixels

To improve the similarity between cover and stego-pixels in some or all of our proposed methods, we need to investigate our post-processing phase to come up with another layer of adaptable closest mapping between cover and stego-pixels on texture criteria. However, this would require an investigation on texture elasticity. For example, how much texture of cover and stego-pixels can accommodate the secret data without degrading certain levels of visual quality? This may exploit the local texture based adaptable mapping models to increase the similarity between cover and stego-pixels.

6.3.3 Robustness over Modern Steganalysis

To improve the robustness of proposed methods against machine learning based classifier for larger payload, we will investigate and improvise the location sensitive embedding of the proposed methods. This texture identification mechanism should be investigated and improved from 2 non-overlapped consecutive pixels blocks to multiple pixels with multiple directions.

REFERENCES

Abdulla, A. A., Sellahewa, H., & Jassim, S. A. (2014). Steganography based on pixel intensity value decomposition. *In Proc. of SPIE Mobile Multimedia/Image Processing, Security, and Applications, 9120*, Baltimore, Maryland, United States, (pp. 912005). doi:10.1117/12.2050518

Abdulla, A. A., Sellahewa, H., & Jassim, S. A. (2014). Stego quality enhancement by message size reduction and fibonacci bit-plane mapping. *In Proc. of International Conference on Research in Security Standardisation*, London, UK, (pp. 151-166). doi:https://doi.org/10.1007/978-3-319-14054-4_10

Afrakhteh, M., & Ibrahim, S. (2010). Adaptive steganography scheme using more surrounding pixels. *In Proc. of International Conference on Computer Design and Applications (ICCDA), 2010, 1*, Qinhuangdao, China, (pp. V1-225). doi:10.1109/ICCDA.2010.5541442

Al-Dmour, H., & Al-Ani, A. (2016). A steganography embedding method based on edge identification and XOR coding. *Expert systems with Applications*, *46*, 293-306.

Al-Husainy, M. A. (2009). Image steganography by mapping pixels to letters. *Journal of Computer science*, *5*(1), 33.

Alattar, A. M., & Alattar, O. M. (2004). Watermarking electronic text documents containing justified paragraphs and irregular line spacing. *In Proc. of SPIE, 5306*, San Jose, California, United States, (pp. 685-695). doi:10.1117/12.527147

Amirtharajan, R., & Rayappan, J. B. B. (2009). Tri-layer stego for enhanced security-a keyless random approach. *In Proc. of IEEE Internet Multimedia Services Architecture and Applications (IMSAA), 2009*, Bangalore, India, (pp. 1-6). doi:10.1109/IMSAA.2009.5439438

Balasubramanian, C., Selvakumar, S., & Geetha, S. (2014). High payload image steganography with reduced distortion using octonary pixel pairing scheme. *Multimedia Tools and Applications*, *73*(3), 2223-2245.

Bhattacharyya, D., Dutta, J., Das, P., Bandyopadhyay, R., Bandyopadhyay, S. K., & Kim, T.-h. (2009). Discrete Fourier transformation based image authentication technique. *In Proc. of 8th IEEE International Conference on Cognitive Informatics, 2009. ICCI'09.*, Kowloon, Hong Kong, China, (pp. 196-200). doi:10.1109/COGINF.2009.5250756

Chan, C.-K., & Cheng, L.-M. (2004). Hiding data in images by simple LSB substitution. *Pattern recognition*, *37*(3), 469-474.

Chang, K.-C., Chang, C.-P., Huang, P. S., & Tu, T.-M. (2008). A novel image steganographic method using tri-way pixel-value differencing. *Journal of multimedia*, *3*(2), 37-44.

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing, 90*(3), 727-752.

Chen, J. (2014). A PVD-based data hiding method with histogram preserving using pixel pair matching. *Signal Processing: Image Communication, 29*(3), 375-384.

Chen, N.-K., Su, C.-Y., Shih, C.-Y., & Chen, Y.-T. (2016). Reversible watermarking for medical images using histogram shifting with location map reduction. *In Proc. of IEEE International Conference on Industrial Technology (ICIT), 2016*, 792-797. doi:10.1109/ICIT.2016.7474852

Chen, P.-Y., & Lin, H.-J. (2006). A DWT based approach for image steganography. *International Journal of Applied Science and Engineering, 4*(3), 275-290.

Chen, W.-J., Chang, C.-C., & Le, T. H. N. (2010). High payload steganography mechanism using hybrid edge detector. *Expert systems with Applications, 37*(4), 3292-3301.

Chen, W.-S., Liao, Y.-K., Lin, Y.-T., & Wang, C.-M. (2016). A novel general multiple-base data embedding algorithm. *Information Sciences, 358*, 164-190.

Choudhury, B., Das, R., & Baruah, A. (2015). A Novel Steganalysis Method Based on Histogram Analysis. *Advanced Computer and Communication Engineering Technology*, 779-789. doi:https://doi.org/10.1007/978-3-319-07674-4_73

Cogranne, R., Zitzmann, C., Retraint, F., Nikiforov, I. V., Cornu, P., & Fillatre, L. (2014). A local adaptive model of natural images for almost optimal detection of hidden data. *Signal Processing, 100*, 169-185.

Das, P., & Kar, N. (2015). ILSB: Indicator-Based LSB Steganography *Intelligent Computing, Communication and Devices* (pp. 489-495): Springer.

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing, 2012*(1), 1-16.

Doğan, Ş. (2016). A new data hiding method based on chaos embedded genetic algorithm for color image. *Artificial Intelligence Review, 46*(1), 129-143.

El-Emam, N. N. (2015). New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization. *Computers & Security, 55*, 21-45.

El-Emam, N. N., & Al-Diabat, M. (2015). A novel algorithm for colour image steganography using a new intelligent technique based on three phases. *Applied Soft Computing, 37*, 830-846.

Fillatre, L. (2012). Adaptive steganalysis of least significant bit replacement in grayscale natural images. *IEEE Transactions on Signal Processing, 60*(2), 556-569.

Fridrich, J. (1999). Applications of data hiding in digital images. *In Proc. of Fifth International Symposium on Signal Processing and Its Applications, 1999. ISSPA'99. , 1*, Brisbane, Queensland, Australia, (9 vol. pp. 1). doi:10.1109/ISSPA.1999.818099

Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. *IEEE multimedia, 8*(4), 22-28.

Geetha, S., Kabilan, V., Chockalingam, S., & Kamaraj, N. (2011). Varying radix numeral system based adaptive image steganography. *Information Processing Letters, 111*(16), 792-797.

Gonzalez, R. C., & Woods, R. E. (2007). Image processing. *Digital image processing, 2*.

Grajeda-Marín, I. R., Montes-Venegas, H. A., Marcial-Romero, J. R., Hernández-Servín, J., & De Ita, G. (2016). An Optimization Approach to the TWPVD Method for Digital Image Steganography. *In Proc. of Mexican Conference on Pattern Recognition*, Guanajuato, Mexico, (pp. 125-134). doi:https://doi.org/10.1007/978-3-319-39393-3_13

Grover, N., & Mohapatra, A. (2013). Digital image authentication model based on edge adaptive steganography. *In Proc. of 2nd International Conference on Advanced Computing, Networking and Security (ADCONS), 2013*, Mangalore, India, (pp. 238-242). doi:10.1109/ADCONS.2013.45

Gutub, A. A.-A. (2010). Pixel indicator technique for RGB image steganography. *Journal of Emerging Technologies in Web Intelligence, 2*(1), 56-64.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA data mining software: an update. *ACM SIGKDD explorations newsletter, 11*(1), 10-18.

Hernández-Servin, J., Marcial-Romero, J. R., Jiménez, V. M., & Montes-Venegas, H. (2015). A modification of the TPVD algorithm for data embedding. *In Proc. of Mexican Conference on Pattern Recognition*, Mexico City, Mexico (pp. 74-83). doi:https://doi.org/10.1007/978-3-319-19264-2_8

Holub, V., Fridrich, J., & Denemark, T. (2014). Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security, 2014*(1), 1.

Hong, W. (2013). Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique. *Information Sciences, 221*, 473-489.

Hong, W., & Chen, T.-S. (2012). A novel data embedding method using adaptive pixel pair matching. *IEEE Transactions on Information Forensics and Security*, *7*(1), 176-184.

Hong, W., Chen, T.-S., & Luo, C.-W. (2012). Data embedding using pixel value differencing and diamond encoding with multiple-base notational system. *Journal of Systems and Software, 85*(5), 1166-1175.

Hong, W., Chen, T.-S., & Shiu, C.-W. (2009). Reversible data hiding for high quality images using modification of prediction errors. *Journal of Systems and Software, 82*(11), 1833-1842.

Huang, H.-S. (2015). A combined image steganographic method using multi-way pixel-value differencing. *In Proc. of 6th International Conference on Graphic and Image Processing (ICGIP 2014)*, Beijing, China (pp. 944319). doi:10.1117/12.2179107

Ioannidou, A., Halkidis, S. T., & Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. *Expert systems with Applications, 39*(14), 11517-11524.

Iranpour, M. (2013). LSB-based steganography using Hamiltonian paths. *In Proc. of 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013*, Beijing, China, (pp. 586-589). doi:10.1109/IIH-MSP.2013.151

Jafar, I. F., Darabkh, K. A., Al-Zubi, R. T., & Al Na'mneh, R. A. (2015). Efficient reversible data hiding using multiple predictors. *The Computer Journal, 59*(3), 423-438.

Jenifer, K. S., Yogaraj, G., & Rajalakshmi, K. (2014). LSB approach for video steganography to embed images. *International Journal of Computer Science and Information Technologies, 5*(1), 319-322.

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26-34.

Jung, K.-H. (2010). High-capacity steganographic method based on pixel-value differencing and LSB replacement methods. *The Imaging Science Journal, 58*(4), 213-221.

Jung, K.-H., & Yoo, K.-Y. (2014a). Data hiding using edge detector for scalable images. *Multimedia Tools and Applications*, *71*(3), 1455-1468.

Jung, K.-H., & Yoo, K.-Y. (2014b). Three-Directional Data Hiding Method for Digital Images. *Cryptologia, 38*(2), 178-191.

Jung, K.-H., & Yoo, K.-Y. (2015a). High-capacity index based data hiding method. *Multimedia Tools and Applications, 74*(6), 2179-2193.

Jung, K.-H., & Yoo, K.-Y. (2015b). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications, 74*(6), 2143-2155.

Kanan, H. R., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert systems with Applications, 41*(14), 6123-6130.

Katzenbeisser, S., & Petitcolas, F. (2000). *Information hiding techniques for steganography and digital watermarking*: Artech house: Boston, MA, USA.

Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. *Ieee Signal Processing Letters, 12*(6), 441-444.

Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., . . . Pevný, T. (2013). Moving steganography and steganalysis from the laboratory into the real world. *In Proc. o 1st ACM workshop on Information hiding and multimedia security*, Montpellier, France, (pp. 45-58). doi:10.1145/2482513.2482965

Khodaei, M., & Faez, K. (2010). Image hiding by using genetic algorithm and LSB substitution. *Image and Signal Processing*, 404-411.

Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least significant-bit substitution and pixel-value differencing. *IET Image processing, 6*(6), 677-686.

Khodaei, M., Sadeghi Bigham, B., & Faez, K. (2016). Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution. *Cybernetics and Systems*, 1-12.

Kieu, T. D., & Chang, C.-C. (2011). A steganographic scheme by fully exploiting modification directions. *Expert systems with Applications*, *38*(8), 10648-10657.

Kodovsky, J., Fridrich, J., & Holub, V. (2012). Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security, 7*(2), 432-444.

Kuo, W.-C., Kuo, S.-H., & Huang, Y.-C. (2013). Data hiding schemes based on the formal improved exploiting modification direction method. *Applied Mathematics & Information Sciences Letters, 1*(3), 1-8.

Kuo, W.-C., Kuo, S.-H., Wang, C.-C., & Wuu, L.-C. (2016). High capacity data hiding scheme based on multi-bit encoding function. *Optik-International Journal for Light and Electron Optics, 127*(4), 1762-1769.

Kuo, W.-C., Wang, C.-C., & Hou, H.-C. (2016). Signed digit data hiding scheme. *Information Processing Letters, 116*(2), 183-191.

Lee, Y.-P., Lee, J.-C., Chen, W.-K., Chang, K.-C., Su, J., & Chang, C.-P. (2012). High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Information Sciences, 191*, 214-225.

Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*(2), 142-172.

Li, X., Zhang, W., Gui, X., & Yang, B. (2013). A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. *IEEE Transactions on Information Forensics and Security*, *8*(7), 1091-1100.

Liao, X., Wen, Q.-y., & Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. *Journal of Visual Communication and Image Representation, 22*(1), 1-8.

Liu, J., Tang, G., & Sun, Y. (2013). A secure steganography for privacy protection in healthcare system. *Journal of medical systems, 37*(2), 1-10.

Liu, Y., Yang, T., & Xin, G. (2015). Text Steganography in Chat Based on Emoticons and Interjections. *Journal of Computational and Theoretical Nanoscience, 12*(9), 2091-2094.

Lu, T.-C., Chang, C.-C., & Huang, Y.-H. (2014). High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting. *multimedia tools and applications, 72*(1), 417-435.

Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security, 5*(2), 201-214.

Mahimah, P., & Kurinji, R. (2013). Zigzag pixel indicator based secret data hiding method. *In Proc. of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013*, Enathi, India, (pp. 1-5). doi:10.1109/ICCIC.2013.6724286

Mandal, J., & Das, D. (2012). Steganography using adaptive pixel value differencing (APVD) of gray images through exclusion of overflow/underflow. *In Proc. of 2nd International Conference on Computer Science, engineering and Applications (CCSEA-2012)*, Delhi, India (pp. 10). doi:10.5121/csit.20122201-10.5121/csit.2012.2243

Mazurczyk, W., Smolarczyk, M., & Szczypiorski, K. (2011). Retransmission steganography and its detection. *Soft Computing, 15*(3), 505-515.

Modi, M. R., Islam, S., & Gupta, P. (2013). Edge based steganography on colored images. *In Proc. of International Conference on Intelligent Computing*, Nanning, China (pp. 593-600). doi:https://doi.org/10.1007/978-3-642-39479-9_69

Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W. (2015). A secure method for color image steganography using gray-level modification and multi-level encryption. *KSII Transactions on Internet and Information Systems (TIIS), 9*, 1938-1962.

Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. (2016). CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*, 1-30.

Murdoch, S. J., & Lewis, S. (2005). *Embedding covert channels into TCP/IP* (Vol. 3727): Springer.

Nag, A., Ghosh, S., Biswas, S., Sarkar, D., & Sarkar, P. P. (2012). An image steganography technique using X-box mapping. *In Proc. of IEEE Advances in Engineering, Science and Management (ICAESM), 2012*, Nagapattinam, Tamil Nadu, India, (pp. 709-713).

Nguyen, T. D., Arch-int, S., & Arch-int, N. (2015). An adaptive multi bit-plane image steganography using block data-hiding. *Multimedia Tools and Applications*, 1-27.

Pan, F., Li, J., & Yang, X. (2011). Image steganography method based on PVD and modulus function. *In Proc. of IEEE Electronics, Communications and Control (ICECC), 2011*, Ningbo, China, (pp. 282-284). doi:10.1109/ICECC.2011.6067590

Pan, Z., Hu, S., Ma, X., & Wang, L. (2015). Reversible data hiding based on local histogram shifting with multilayer embedding. *Journal of Visual Communication and Image Representation, 31*, 64-74.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE, 87*(7), 1062-1078.

Pevny, T., Bas, P., & Fridrich, J. (2010). Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security, 5*(2), 215-224.

Pevný, T., Filler, T., & Bas, P. (2010). Using high-dimensional image models to perform highly undetectable steganography. *In Proc. of International Workshop on Information Hiding*, Calgary, AB, Canada, (pp. 161-177). doi:https://doi.org/10.1007/978-3-642-16435-4_13

Qazanfari, K., & Safabakhsh, R. (2014). A new steganography method which preserves histogram: Generalization of LSB++. *Information Sciences, 277*, 90-101.

Roy, R., & Changder, S. (2014). Image realization steganography with LCS based mapping. *In Proc. of 7th International Conference on Contemporary Computing (IC3), 2014*, Noida, India, (pp. 218-223). doi:10.1109/IC3.2014.6897176

Roy, R., Sarkar, A., & Changder, S. (2013). Chaos based edge adaptive image steganography. *Procedia Technology, 10*, 138-146.

Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. (2015). Video steganography: a comprehensive review. *Multimedia Tools and Applications, 74*(17), 7063-7094.

Santoso, K. N., Suk-Hwan, L., Hwang, W.-J., & Ki-Ryong, K. (2015). Information Hiding in Noncoding DNA for DNA Steganography. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 98*(7), 1529-1536.

Sarreshtedari, S., & Akhaee, M. A. (2014). One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme. *IET Image processing, 8*(2), 78-89.

Schaefer, G., & Stich, M. (2004). UCID: An uncompressed color image database. *Storage and retrieval methods and applications for multimedia, 5307*, 472-480.

Sedighi, V., Cogranne, R., & Fridrich, J. (2016). Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security, 11*(2), 221-234.

Shen, S.-Y., & Huang, L.-H. (2015). A data hiding scheme using pixel value differencing and improving exploiting modification directions. *Computers & Security, 48*, 131-141.

Shen, S., Huang, L., & Tian, Q. (2015). A novel data hiding for color images based on pixel value difference and modulus function. *Multimedia Tools and Applications, 74*(3), 707-728.

Stoica, A., Vertan, C., & Fernandez-Maloigne, C. (2003). Objective and subjective color image quality evaluation for JPEG 2000 compressed images. *In Proc. of International Symposium on Signals, Circuits and Systems, 2003. SCS 2003., 1*, Iasi, Romania, Romania (pp. 137-140). doi:10.1109/SCS.2003.1226967

Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. *Computer science review, 13*, 95-113.

Sun, H.-M., Weng, C.-Y., Lee, C.-F., & Yang, C.-H. (2011). Anti-forensics with steganographic data embedding in digital images. *IEEE Journal on Selected areas in Communications, 29*(7), 1392-1403.

Sun, S. (2016). A novel edge based image steganography with 2 k correction and Huffman encoding. *Information Processing Letters, 116*(2), 93-99.

Swain, G. (2015). Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimedia Tools and Applications*, 1-16.

Swain, G. (2016). A Steganographic Method Combining LSB Substitution and PVD in a Block. *Procedia Computer Science, 85*, 39-44.

Swain, G., & Lenka, S. K. (2012). A better RGB channel based image steganography technique *Global Trends in Information Systems and Software Applications* (pp. 470-478): Springer.

Tang, M., Song, W., Chen, X., & Hu, J. (2015). An image information hiding using adaptation and radix. *Optik-International Journal for Light and Electron Optics, 126*(23), 4136-4141.

Tavares, J. R. C., & Junior, F. M. B. (2016). Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel. *IEEE Latin America Transactions, 14*(2), 1058-1064.

Thanikaiselvan, V., Subashanthini, S., & Amirtharajan, R. (2014). PVD based steganography on scrambled RGB cover images with pixel indicator. *Journal of Artificial Intelligence, 7*(2), 54.

Tiwari, N., & Shandilya, M. (2010). Secure RGB image steganography from pixel indicator to triple algorithm-an incremental growth. *International Journal of Security and Its Applications, 4*(4), 53-62.

Tsai, P., Hu, Y.-C., & Yeh, H.-L. (2009). Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Processing, 89*(6), 1129-1143.

Tsai, Y.-Y., Chen, J.-T., & Chan, C.-S. (2014). Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding. *IJ Network Security, 16*(5), 363-368.

Tseng, H.-W., & Leng, H.-S. (2014). High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion. *IET Image processing, 8*(11), 647-654.

Tseng, L.-Y., Chan, Y.-K., Ho, Y.-A., & Chu, Y.-P. (2008). Image hiding with an improved genetic algorithm and an optimal pixel adjustment process. *In Proc. of 8th International Conference on Intelligent Systems Design and Applications, 2008. ISDA'08., 3*, Kaohsiung, Taiwan, (pp. 320-325). doi:10.1109/ISDA.2008.235

USC-SIPI. (2016, Accessed 1st January 2016). http://sipi.usc.edu/database/.

Wang, Z.-H., Chang, C.-C., & Li, M.-C. (2012). Optimizing least-significant-bit substitution using cat swarm optimization strategy. *Information Sciences, 192*, 98-108.

Wang, Z., & Bovik, A. C. (2002). A universal image quality index. *IEEE Signal Processing Letters, 9*(3), 81-84.

Wen-Chung, K., & Ming-Chih, K. (2013). A steganographic scheme based on formula fully exploiting modification directions. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 96*(11), 2235-2243.

Westfeld, A. (2001). F5—a steganographic algorithm. *In Proc. of 4th International Workshop on Information hiding*, Pittsburgh, PA, USA, (pp. 289-302).

Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems. *In Proc. of International Workshop on Information Hiding*, Dresden, Germany, (pp. 61-76). doi:https://doi.org/10.1007/10719724_5

Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24*(9), 1613-1626.

Wu, H.-C., Wang, H.-C., Tsai, C.-S., & Wang, C.-M. (2010). Reversible image steganographic scheme via predictive coding. *Displays, 31*(1), 35-43.

Wu, H.-C., Wu, N.-I., Tsai, C.-S., & Hwang, M.-S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proceedings-Vision, Image and Signal Processing, 152*(5), 611-615.

Wu, K., Liao, W., Lin, C., & Chen, T. (2015). A high payload hybrid data hiding scheme with LSB, EMD and MPE. *The Imaging Science Journal, 63*(3), 174-181.

Wu, N.-I., & Hwang, M.-S. (2007). Data hiding: current status and key issues. *IJ Network Security, 4*(1), 1-9.

Xin, L., Qiaoyan, W., & Zhang, J. (2012). A novel steganographic method with four-pixel differencing and exploiting modification direction. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 95*(7), 1189-1192.

Xu, W.-L., Chang, C.-C., Chen, T.-S., & Wang, L.-M. (2016). An improved least-significant-bit substitution method using the modulo three strategy. *Displays, 42*, 36-42.

Yang, C.-H., Wang, S.-J., & Weng, C.-Y. (2010). Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations. *Fundamenta Informaticae, 98*(2-3), 321-336.

Yang, C.-H., Weng, C.-Y., Tso, H.-K., & Wang, S.-J. (2011). A data hiding scheme using the varieties of pixel-value differencing in multimedia images. *Journal of Systems and Software, 84*(4), 669-678.

Yang, C.-H., Weng, C.-Y., Wang, S.-J., & Sun, H.-M. (2010). Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. *Journal of Systems and Software, 83*(10), 1635-1643.

Yang, H., Sun, X., & Sun, G. (2009). A high-capacity image data hiding scheme using adaptive LSB substitution. *Radioengineering, 18*(4), 509-516.

Yu, Y.-H., Chang, C.-C., & Hu, Y.-C. (2005). Hiding secret data in images via predictive coding. *Pattern Recognition, 38*(5), 691-705.

Yuan, H.-D. (2014). Secret sharing with multi-cover adaptive steganography. *Information Sciences, 254*, 197-212.

Zaker, N., & Hamzeh, A. (2012). A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram. *Multimedia Tools and Applications, 58*(1), 147-166.

Zhang, H., Ping, X., Xu, M., & Wang, R. (2014). Steganalysis by subtractive pixel adjacency matrix and dimensionality reduction. *Science China Information Sciences, 57*(4), 1-7.

Zhang, T., & Ping, X. (2003). Reliable detection of LSB steganography based on the difference image histogram. *In Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003, 3*, Hong Kong, China, (pp. III-545). doi:10.1109/ICASSP.2003.1199532

Zhang, X., & Wang, S. (2006). Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters, 10*(11), 781-783.

Zhao, Z., & Luo, H. (2012). Reversible data hiding based on Hilbert curve scan and histogram modification. *Information Technology Journal, 11*(2), 209.

Zielińska, E., Mazurczyk, W., & Szczypiorski, K. (2014). Trends in steganography. *Communications of the ACM, 57*(3), 86-95.

LIST OF PUBLICATIONS AND PAPERS PRESENTED

Articles on Research Topic:

1. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Anthony T. S. Ho, Noman Javed, Ki-Hyun Jung. (2017). A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Processing: Image Communication, 50, 44-57. (**ISI-Cited Publication**), **IF 2.244, Q2** (**Published**).

2. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Noman Javed, Ki-Hyun Jung. (2016). Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. Symmetry, 8(6), 41**.** (**ISI-Cited Publication**), **IF 1.547, Q2** (**Published**).

3. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Noman Javed, Ki-Hyun Jung. (2016). Recursive Information Hiding Scheme Through LSB, PVD, and MPE. IETE Technical Review, 1-11. (**ISI-Cited Publication**), **IF 1.330, Q2** (**Published**).

4. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, Anthony T. S. Ho, Ki-Hyun Jung. (2017). Image Steganography in Spatial Domain: A Survey. Signal Processing: Image Communication, (**ISI-Cited Publication**), **IF 2.244, Q2** (**Under Review**).

5. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Ishrat Batool. (2015). Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography. Vol, 9, 179-188. (**SCOPUS-Cited Publication**) (**Published**).

Conference Proceedings on Research Topic:

1. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Nor Badrul Anuar, Rosli Salleh, Rafidah Md Noor. (2015, June). Pixel value differencing steganography techniques: Analysis and open challenge. In Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on (pp. 21-22). **IEEE. Taiwan**.

2. Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, Noman Javed, Rosli Salleh. (2016). High capacity data embedding method with LSB and PVD Proceedings of the 5th International Cryptology and Information Security Conference 2016 (**CRYPTOLOGY** 2016), Kota Kinabalu, Sabah **Malaysia**.

Seminars:

1. Postgraduate Research Excellence Symposium (PGRes) Held in Faculty of Computer Science and Information Technology, Universiti Malaya. Malaysia. June, 2015.