THESIS

ENHANCING THE PERFORMANCE OF DIGITAL IMAGE DATA HIDING USING REDUCED DIFFERENCE EXPANSION TECHNIQUE AND CONSTANT BASE POINT

NAME: PASCAL MANIRIHO
NRP : 5116201701

SUPERVISOR
TOHARI AHMAD, S. Kom.,MIT., Ph.D

MASTER PROGRAM
NET CENTRIC COMPUTING
DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND COMMUNICATION
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2018

A thesis submitted in fulfilment of the requirements to be admitted to the degree of

Master of Computer Science

at
Institut Teknologi Sepuluh Nopember

By

Pascal Maniriho
Registration Number: 5116201701

With the topic:

Enhancing the Performance of Digital Image Data Hiding Using Reduced Difference Expansion Technique and Constant Base Point

Examination Date: January 03, 2018
Graduation Period: March 2018

Approved by:

Tohari Ahmad, S.Kom, MIT, Ph.D
NIP: 197505252003121002 (Supervisor) .....

Waskitho Wibisono, S.Kom, M.Eng, Ph.D
NIP: 197410222000031001 (Examiner) .....

Dr.Eng. Radityo Anggoro, S.Kom, M.Sc
NIP: 198410162008121002 (Examiner) .....

Royyana Muslim I, S.Kom, M.Kom, Ph.D
NIP: 197708242006041001 (Examiner) .....

Director of Graduate Programs

Dr. Agus Zainal Arifin, S.Kom, M.Kom
NIP: 197208091995121001

[This page intentionally left blank]

ENHANCING THE PERFORMANCE OF DIGITAL IMAGE DATA HIDING USING REDUCED DIFFERENCE EXPANSION TECHNIQUE AND CONSTANT BASE POINT

Student Name : Pascal Maniriho

Registration Number : 5116201701

Supervisor : Tohari Ahmad, S.Kom., MIT., Ph.D

ABSTRACT

The last few decades have been marked by a rapid growth and significant enhancement of the internet infrastructures, i.e., the internet has become a broad network enabling many enterprises around the world to interact while sharing multimedia data. Nevertheless, this technology has brought many challenges related to securing private and sensitive information which has led to the application of cryptography technique as a mean for securing data by encrypting them. However, since the encrypted data can be seen by active and sophisticated intruders during the transmission, this may lead to its suspicion which can result in unauthorized access. Thereby**,** data hiding (which is also called information hiding) is another technique for securing commutation via the public network. Data hiding is one of the best and most challenging fields dealing with securing organizational sensitive information due to many factors such as identity theft, information phishing, user privacy, network policy violation, contents and copyright protection. It is performed by utilizing some carriers to conceal private information which is further extracted later to verify and validate the genuineness.

Digital steganography has been recognized among the recent and most popular data hiding techniques. Steganography is the practice of concealing confidential information in the codes that make up the digital files. Such digital files can be an image, audio, video, and text. Different from cryptography, however, steganography provides security by disguising the presence of communication. It originates from the concept that if the communication is visible, the suspicion or attack is obvious. Hence, the main goal is to always disguise the presence of the hidden confidential data. Recently, various data

hiding methods based on digital image steganography have been already suggested by several researchers around the globe. The main goal was to improve the security, embedding capacity and the quality of the stego image. However, research have shown that there is still a challenge to achieve a good visual quality of the stego media while preserving a good embedding capacity. In this direction, this study aims at proposing a new data hiding approach that enhances the quality of the stego image and the embedding capacity. That is, the suggested approach enhances the existing data hiding methods by utilizing pixel block, constant base point for each pixel block and the reduced difference expansion scheme (RDE-scheme) for grayscale digital images.

Accordingly, the suggested enhancement is detailed as follows. First, the existing reduced difference expansion scheme (RDE-scheme) for reducing the difference values is enhanced in order to get possible small values to be used while concealing the secret data into the cover image. The main objective behind this enhancement is to allow data to be concealed while preserving the quality of the stego image. Notice that the suggested RDE-scheme does not only enhance the quality but also it solves the problem of underflow and overflow. The underflow is encountered when the pixel value in the stego image is below 0 (Pixel value < 0) while the overflow occurs when it is greater than 255 (Pixel value > 255). Second, the new constant base point for each pixel block is chosen differently for the sake of increasing the visual quality of the stego image. Third, we have adjusted the size of the pixel block which achieves a high embedding capacity while distorting the cover media from quad of quad (4×4) to quad, block of size 2 by 2 (2×2). Besides, the effect of varying the size of the secret data with respect to the quality of the stego image is also investigated throughout this study.

Overall, based on the experimental results, good visual quality of the stego image which is evaluated by measuring the peak signal-to-noise ratio (PSNR) and good embedding capacity (measured in bits) are yielded compared to the previous approach, i.e., the proposed method is effective in terms of maintaining both visual quality of the stego image and the embedding capacity.

Index terms— Data hiding, information security, reduced difference expansion, digital steganography, cover image, stego image, confidential data

ENHANCING THE PERFORMANCE OF DIGITAL IMAGE DATA HIDING USING REDUCED DIFFERENCE EXPANSION TECHNIQUE AND CONSTANT BASE POINT

Nama Mahasiswa : Pascal Maniriho

NRP : 5116201701

Pembimbing : Tohari Ahmad, S.Kom., MIT., Ph.D

ABSTRAK

Beberapa dekade terakhir internet telah menjadi jaringan luas yang memungkinkan banyak perusahaan di seluruh dunia untuk berinteraksi sambil berbagi data multimedia. Ini merupakan tanda bahwa infrastruktur internet telah tumbuh dan berkembang secara signifikan. Namun, teknologi ini memiliki banyak tantangan dalam hal pengamanan informasi yang bersifat sensitif dan pribadi sehingga mendorong penerapan teknik kriptografi untuk mengamankan data dengan cara mengenkripsinya. Teknik kriptografi memiliki kekurangan yaitu hasil enkripsi dapat dilihat oleh penyusup *(intruders)* selama transmisi sehingga menyebabkan kecurigaan yang berakibat pada tindakan akses yang bersifat ilegal. Untuk mengurangi hal ini, *data hiding* dapat dimanfaatkan untuk mengamankan informasi tersebut. *Data hiding* adalah salah satu teknik terbaik untuk mendapatkan data tetapi memiliki banyak tantangan permasalahan seperti pencurian identitas, *phising,* pelanggaran kebijakan jaringan dan hak cipta. Untuk mendapatkan kemanan data, *data hiding* memanfaatkan beberapa media untuk menyembunyikan informasi dan dapat diekstrak untuk memverifikasi keasliannya.

Salah satu teknik *data hiding* yang paling terkenal adalah steganografi digital. Teknik ini menyembunyikan informasi rahasia kedalam *file digital* seperti citra digital, audio, video dan teks. Berbeda dengan kriptografi, steganografi memberikan keamanan informasi dengan menyamarkannya dalam *file digital*. Penyebab digunakannya tindakan ini adalah jika komunikasi terlihat maka akan mengundang kecurigaan yang mengakibatkan terjadi serangan seperti yang dijelaskan sebelumnya. Oleh karena itu, tujuan utama dari teknik ini adalah menyamarkan informasi rahasia dengan

menyembunyikannya kedalam *file* yang digunakan. Akhir-akhir ini, beberapa teknik data hiding dengan menggunakan citra digital telah banyak dikembangkan oleh beberapa peneliti di seluruh dunia. Tujuan utama mereka adalah untuk meningkatkan keamanan, kapasitas penyisipan dan kualitas dari citra stego. Sampai saat ini, banyak penelitian yang menunjukkan bahwa masih menjadi tantangan untuk mendapatkan kualitas media *stego* yang baik dengan kapasitas penyisipan yang tinggi. Dengan maksud yang sama, penelitian ini mengusulkan konsep pendekatan baru dalam hal *data hiding* yang dapat meningkatkan kualitas dan kapasitas dari citra *stego*.

Pendekatan tersebut dilakukan dengan cara meningkatkan metode *data hiding* yang sudah ada dengan memanfaatkan blok piksel, penentuan *base point* yang konsisten untuk masing-masing blok dan mereduksi *difference expansion* untuk citra abu-abu. Rincian dari pendekatan tersebut adalah sebagai berikut. Pertama, skema reduksi *difference expansion* (RDE) ditingkatkan untuk mendapatkan nilai terkecil yang akan digunakan dalam penyembunyian data kedalam citra *carrier*. Tujuannya adalah memungkinkan data dapat disisipkan dengan tetap menjaga kualitas citra stego tetap baik. Perlu diketahui bahwa usulan skema RDE tidak hanya meningkatkan kualitas tetapi juga menyelesaikan masalah *overflow* dan *underflow*. *Underfow* merupakan kondisi piksel dalam citra *stego* bernilai kurang dari 0 sedangkan overflow terjadi ketika nilai piksel melebihi 255. Kedua, *base-point* yang bersifat konstan untuk masing-masing blok piksel akan dipilih secara berbeda untuk dapat meningkatkan kualitas visual dari citra stego. Ketiga, kami mengatur ukuran blok dari *quad of quad* (4x4) yang memiliki kualitas citra *stego* kurang baik menjadi 2x2.

Hal lain yang kami lakukan adalah mengetahui efek dari besar ukuran data yang digunakan dalam proses penyisipan. Secara keseluruhan, berdasarkan hasil eksperimen, usulan pendekatan ini memiliki kemampuan yang lebih baik dibandingkan dengan penelitian sebelumnya yang ditandai dengan kapasitas penyisipan yang lebih tinggi dan kualitas visual citra *stego* yang baik yang diukur menggunakan metode signal-to-noise ratio (PSNR).

Kata Kunci: *Data hiding*, kemanan Infomasi, reduksi *error expansion*, *digital steganography*, citra *cover*, citra *stego*, penyembunyian *data*

Acknowledgement

After an intensive period full of struggles of almost 3 years, today is my great pleasure to write this thankful note as finishing touch on my thesis. First of all, I would like to dedicate this hard work to the Almighty God who by grace gave me strengths and wisdom to fulfill and accomplish it. Writing this thesis has been a period of intense learning not only in the scientific arena, but also on a personal level and international cooperation. Besides, working on this thesis has had a significant impact on my career development. Therein, I would like to take this moment to reflect on the people and different partners who have supported and helped me to reach this grand achievement.

My sincere gratitude goes to the Indonesian Ministry of Research, Technology and Higher Education for offering me a full scholarship to pursue my master studies at Institut Teknologi Sepuluh Nopember (ITS Surabaya), in the Department of Informatics, Faculty of Information Technology and Communication.

Most importantly, I would like thank my supervisor, Tohari Ahmad, S.Kom., MIT., Ph.D, for accepting me to carry out my research under his supervision. During my tenure, he contributed a lot to my projects by giving me brilliant ideas, friendly and cooperative atmosphere, intellectual freedom in my work, supporting my attendance at various meetings, engaging me in new ideas, useful feedback and demanding a high quality of work in all my endeavors.

In addition, my special thanks goes to the rest of my thesis examination committee: Head of Postgraduate Studies Waskitho Wibisono, S.Kom., M.Eng, Ph.D, Royyana Muslim Ijtihadie, S.Kom.,M.Kom.,Ph.D, and Dr. Eng. Radityo Anggoro, S.Kom.,M.Sc. for their valuable guidance, encouragement, insightful comments, hard questions and interest on my work. I would also like to thank my academic advisor Dr. Agus Zainal Arifin, S.Kom., M.Kom for his valuable daily advices during my studies. Moreover, I was fortunate to meet with Prof. Ir. Supeno Djanali, M.Sc.,Ph.D, who patiently taught me three interesting courses. With his great motivation, I got relevant knowledge which in turn helped me to choose my right career path. Being taught by him was such an amazing opportunity. I am also indebted to the Head of ITS International Office, Dr. Maria Anityasari. You definitely provided me with the tools and support that

I needed to successfully complete my studies. As well as that, as early mentioned every result described in this thesis was accomplished with the help and support of fellow labmates and collaborators. Hence, I thank my fellow classmates and labmates in the department of informatics, NCC, Pascasarjana and AJK labs: Hendro, Thiar, Effendi, Rozita, Dinial, Dewi, Amelia, Nahya, Depandi, Maurice, Mustofa, Rarasmaya, Hernawati, and others, for their support, knowledgeable discussions, and sleepless nights we were working together before the deadlines, and for all the fun we have had over the entire period at ITS. I would be remiss if I do not thank Ibu Eva Mursidah and Ibu Lina, who deserve credit for providing much needed assistance with administrative issues and tasks which kept my work running smoothly. Moreover, I am grateful for the funding sources that allowed me to publish my research articles especially, the Indonesia Ministry of Research, Technology and Higher Education Research Project N^{o} 010/SP2H/LT/DRPM/IV/2017.

Finally, I would like to acknowledge my family and friends who supported me over the years of my studies. First and foremost, I would like to thank my lovely mom Ziporah, my brothers and their wives, my sisters Jacqueline and Magdalene for their constant love and support. I also thank my brothers' sons and daughters especially, Umurerwa, for their love, good wishes and willingness to always know how I feel.

Last but not least, In the name of our Almighty God, I thank you all!

Pascal Maniriho

5116201701

ITS Surabaya, Indonesia

January 16, 2018

Credits

List of the publications mentioned in this page have been accomplished throughout this study.

Journal article

- Pascal Maniriho and Tohari Ahmad. Enhancing the capability of data hiding method based on reduced difference expansion. Engineering Letters, IAENG, 2017. [accepted].
- Pascal Maniriho and Tohari Ahmad. Information hiding scheme for digital images using difference expansion and modulus function. Journal of King Saud University-Computer and Information Sciences, JKSUCIS, 2018. [revision]
- Pascal Maniriho and Tohari Ahmad. Survey on digital image information hiding methods implemented using difference expansion and pixel value modification techniques. Journal of King Saud University-Engineering Sciences, 2018. [Submitted].

Conference based paper

- Pascal Maniriho and Tohari Ahmad. A data hiding approach using enhanced-RDE in grayscale images. In the 2nd International Conference on Advanced Mechatronics, Intelligent Manufacture, and Industrial Automation (ICAMIMIA 2017), 2017. [presented].
- Aurélien Laffont, Pascal Maniriho, Anaïs Ramsi, Guillaume Guerteau, Tohari Ahmad. Enhanced Pixel Value Modification based on Modulus Function for RGB Image Steganography. In the 11th International Conference on Information and Communication Technology and System (ICTS 2017), 2017. [presented].

[This page intentionally left blank]

Table of Contents

[This page intentionally left blank]

Table of Figures

[This page intentionally left blank]

List of Tables

[This page intentionally left blank]

CHAPTER 1
INTRODUCTION

This chapter elaborates the background study on digital image steganography thereafter the problem formulation, main objectives of this study, hypotheses, research questions, problem scope, research contribution, benefits, and contents layout are presented.

1.1 Research Background

Owing to the advancement of the internet in the recent years, it has become very easy for people to access and share multimedia data without being worried about their physical locations. That is, data can be shared through the internet from anywhere in world. Nevertheless, the internet which was first developed to be safe is often being hijacked by expert intruders which makes the security of multimedia data to be the utmost matter of concern. Additionally, the illegitimate users can easily intercept and alter the sensitive information while being transmitted to the intended recipients via the internet.

Thus, this problem has brought the need for securing sensitive information which can be easily available for intruders intending to violate user rights and communication policies. Recently, various data hiding research dealing with protecting information being shared between individuals via the internet channel have been already carried out. Data hiding aims at protecting privacy, intellectual property rights, and content authentication by concealing sensitive information (also called secret data) into multimedia objects, i.e. it does play a significant role in multimedia security (Tsai et al., 2013). For these reasons, steganography which is one of the data hiding techniques has been adopted among the best security countermeasures to address data security issues.

Besides, cryptography is another well-known security technique in the paradigm of information security. Steganography and cryptography have been around for several years. However, even though both technologies aim at protecting confidential data, they do possess different concepts. Cryptography involves protecting communication by encrypting data before being sent or shared without hiding the communication existence, i.e., the third party (intruders or unauthorized party) can see the encrypted data while being transmitted to the destination which may lead to its suspicion and interception. In contrast to the cryptography,

steganography is the practice of hiding information in the codes that make up digital files while preventing unwanted sources from discovering the communication presence. That is, data transmission is kept confidential between the intended communicating parties. This ensures that the data protection is well maintained which is a necessity in any types of communication.

In steganography, secret information can be embedded in various digital cover media such as image, text, audio and video without causing substantial alteration. Digital image steganography has proven its ability for securing the exchange of information between private communicating parties which is a necessity in today's application (Subhedar & Mankar, 2014). Spatial domain (SD) and transform domain (TD) are two main approaches that are used in digital image steganography. In spatial domain, there is no transformation done before hiding the secret message in the cover image. That is, the secret data are directly hidden in the pixel values.

Different from the spatial domain, however, in the transform domain approach before embedding the secret message the cover image is first transformed from spatial to frequency domain by utilizing some of the transform schemes such as discrete wavelet transform (DWT), discrete cosine transform (DCT), double density dual tree (DD DT), Hadamard transform (HT), curvelet transform (CT), etc. After the transformation, the secret message is then embedded in the transform coefficients, i.e., the information is concealed in the regions of the image that are less exposed to image processing operations such as compression or cropping and this demonstrates its advantage over the spatial domain (Subhedar & Mankar, 2014) and (El-sayed et al., 2016). However, the capacity of the secret message can be a problem. The main goal of any digital image steganographic approach is to simultaneously enhance the security, visual quality of the stego image, and embedding capacity (Hussain et al., 2017).

Recently, different data hiding methods have been already implemented by researchers using any of the aforementioned cover media. Secret data were hidden into the expanded difference obtained by computing the difference expansion (DE) between adjacent pixel pairs (Tian, 2003). This method was further enhanced by (Alattar, 2004) and (Lou et al., 2009) by introducing new methods developed based on DE and the reduced difference expansion (RDE). The RDE aims at reducing the difference so that the secret data can be concealed into small difference values which significantly improves the embedding capacity as well as maintaining

the quality of the cover media (Lou et al., 2009). The enhanced RDE was employed to developed the information hiding scheme presented by (Maniriho & Ahmad, 2017). A new reversible method that conceals the secret data into digital images by utilizing binary-block was proposed by (Lu & Lyu, 2015). Being reversible means that it is possible to reconstruct both the original cover image and the secret message. To achieve a high payload capacity a new technique that utilizes prediction of quad of quad smoothness was applied to control the embedding order (Lin et al., 2010). The work presented by (Wang et al., 2008), introduced a new technique that uses the pixel value differencing (PVD) and the modulo function to hide secret data in a digital image. The number of bits to be embedded in the color image was improved (Nagaraj et al., 2013a). Their method has the capability of hiding one bit of the secret data in each pixel after being modified using a modulo function which results in a good visual quality. Nonetheless, the payload capacity is relatively low since only one bit of the secret message can be concealed in a pair of pixel.

The lossless method that utilizes one statistical global parameter to conceal and recover the secret data was implemented by (Han et al., 2006). The data were hidden by modifying some pixel values as well as leaving others unchanged. Besides, all pixel values can be easily kept after concealing data and both payload capacity and the quality of the stego-image can be controlled as well. To allow more than one bit to be hidden in each pixel of the colored image using the new scheme implemented in (El-sayed et al., 2016), the digital image was first split up into overlapping blocks thereafter the adaptive difference expansion was computed. Moreover, their implemented scheme has also the capability to employ three global parameters to determine the embedding capacity. In our previous work confidential data were concealed into the difference values after reduction performed using the reduced difference expansion scheme (Maniriho & Ahmad, 2017).

The work presented by (Wang et al., 2013) suggested another method that hides data in JPEG image by first modifying the quantized DCT and the quantization table coefficients. In 2013, (Lahiri et al., 2013) introduced an approach that allows secret data to be embedded in the edge of the colored image pixels in the discrete cosine transform domain. The encryption was performed in DCT coefficients so as to improve the efficiency as well as preventing the unintended recipients to decrypt the message. With reference to the concept behind JPEG

encoder and DCT statistical characteristics, basic procedures stating how to choose DCT coefficient for reversible data hiding (RDH) was introduced by (Huang et al., 2016), thereafter a new RDH approach based on histogram shifting was further developed. Moreover, secret bits were only concealed in the coefficients whose values are 1 or -1 while zero coefficients remained unchanged. With this approach, good quality (good PNSR) was achieved but high embedding capacity can deform the stego image, which can result in suspecting the existence of the hidden data.

In the existing approaches, however, the number of the secret bits which can be embedded in the cover and its respective quality of the stego image are still among the severe challenges. Thus, in this research, we suggest a new data hiding technique to deal with those early mentioned problems while hiding data into digital grayscale images. The proposed method is based on the spatial domain approach and it is able to hide 3 bits in one block of pixel in accordance with the predefined criteria which control the embedding process. The cover image is divided into non-overlapping blocks of size 2 by 2 (2×2), i.e., four pixels are defined in each block. Moreover, with this proposed method the embedding capacity and the visual quality can be controlled in order to achieve good quality and good embedding capacity.

1.2 Problem Formulation

With regard to the above background study, several data hiding approaches have been recently suggested in the literature. However, there is still a severe challenge to achieve a good quality of the stego image and good embedding capacity. Furthermore, one of the most challenges which make digital image steganography to be among the research areas attracted by many researchers interested in the paradigm information hiding, is to protect sensitive data by concealing them while preserving the visual quality of the stego media**.** That is, the size of the cover media should not be greatly increased by the embedded data since it could be easy for some experienced attackers (also known as intruders) who have seen the original cover media before to doubt or suspect the existence of confidential data.

Therefore, a well-designed image steganographic approach should conceal data without greatly changing the statistical properties of the cover media. If these two factors i.e. the visual quality and the embedding capacity are met, it ensures that the designed data hiding approach is robust and less perceptible. Thereby, this research aims at addressing the aforementioned

problems by suggesting a new data hiding approach that enhances the work presented by (Ali AL_Huti et al., 2015). Specifically, our main concerns and motivations are elucidated as follows. The quality of the stego image is ameliorated by adjusting the size of the pixel's block and enhancing the reduced difference expansion scheme (RDE-scheme) presented in the previous work (Ali AL_Huti et al., 2015).

Furthermore, the new basepoint (also called the base pixel) is also suggested. Adjusting the size of the pixel's block is ideal since the previously defined large pixel's block had greatly decreased the PSNR value (quality of the stego image) which is measured in order to evaluate and analyze the variations or changes that occur in the statistical properties of the cover media after concealing data. Therein, it does make sense to adjust it since such PSNR reduction (stego image distortion) could lead to the data suspicion and interception. On the other hand, as it was proved in the work carried out by (Lou et al., 2009), concealing data in the reduced difference values can significantly improve the quality and embedding capacity as well. In this way, to ensure that the proposed method does perform well, the existing RDE-based scheme is also ameliorated to allow data to be concealed without worsening the cover media.

Additionally, as early mentioned the new constant basepoint for each pixel's block is chosen differently for increasing the quality of the stego. This suggested basepoint also reduces the number of pixels which can fall out of the gray level range, i.e., $(0 \leq \text{Pix\_value} \leq 255)$ while building the stego image since two pixel's values are not added up as it was performed in the previous research (Ali AL_Huti et al., 2015). Notice that when the value of the pixel obtained after hiding data is less than zero $(\text{Pix\_value} < 0)$, it is called underflow whereas if it is greater than 255, it is considered as overflow $(\text{Pix\_value} > 255)$. Moreover, it is worth to mention that these two types of pixel can lead to the loss of the concealed data and reduction of the embedding capacity if they are not taken into account during the design and development of the algorithm.

Nonetheless, with the proposed method they can be well controlled so as to improve its performance and make it more suitable for concealing confidential data. Thus, the suggested method is considered as a good data hiding approach since it does not only preserve and ameliorate the quality of the stego media but also it does achieve a good embedding capacity.

1.3 Research Objectives

The main goals of this study are presented as follows.

1. Enhance the previous reduced difference expansion scheme (RDE-based scheme) and adjust the pixel's block to allow data to be concealed while preserving the visual quality of the stego image.
2. Suggest a new constant basepoint that ameliorates the visual quality of the stego image and reduces underflow and overflow.
3. Evaluate and analyze the distortion level of the stego image by measuring the variation of the peak signal-to-noise ratio (PSNR) with respect to the embedding capacity.
4. Discuss and make prediction analysis on the experimental results.

1.4 Hypotheses

1. "A well-defined size of the pixel's block can enhance the visual quality of the stego image while maintaining a good embedding capacity".
2. "Defining a good basepoint (also known as base pixel) can have a positive effect on the quality of the stego image".
3. "By using the reduced difference expansion scheme, good visual quality of the stego image and the embedding capacity can be enhanced".

1.5 Research Questions

In order to address the aforementioned problem, the following research questions are essential.

1. How a good visual quality of the stego image can be preserved after concealing the secret data?
2. How the number of secret bits to be concealed in a grayscale digital image can be increased without drastically deforming it?

1.6 Problem Scope

Throughout this research, we are limited at working on the following scope.

1. To conceal data, different 8-bit grayscale images are utilized as cover media.
2. Different sizes of secret data are used in the experiment to evaluate the influence of varying the embedding capacity with respect to the visual quality of the sego image.

3. The location map is employed to keep track of information about any operations performed in each pixel's block.
4. All cover images that are used for evaluation during the experiment are public standard images of size 512×512 obtained from (Califonia, 2017) and (Microbes Digital Library, 2017).
5. The suggested data hiding approach is implemented using MATLAB.

1.7 Main Contribution

A new approach for enhancing the existing image steganographic approaches is implemented in this research. The proposed approach has the capability of preserving the visual quality of the stego image while achieving a good embedding capacity compared to the one suggested by (Ali AL_Huti et al., 2015).

1.8 Research Benefits

The benefit of this study can be highly recognized in the field of information hiding which deals with securing sensitive or private data while being shared (or transmitted) via the internet. That is, since the visual quality of the stego image and embedding capacity are enhanced, this approach minimizes the chance for unauthorized users to suspect the stego image, i.e., it is awkward for any adversaries to discover and realize that the communication between individuals is taking place. Therein, communication can be completely kept secret or unknown. Besides, the work presented in this study will be used as a new reference in the field of information hiding and information security.

1.9 Contents Layout

The remaining parts presented in this thesis are structured as follows. The second chapter introduces the general concepts behind information hiding and digital image steganography coupled with terminologies used in the literature. Thereafter, further discussion on the existing techniques developed based on digital image steganography are covered. Additionally, detailed and deep explanations demonstrating the functionality of the proposed method and the schedule for the project milestones (all research activities) that are carried out are provided in the third chapter. The experiment results and detailed analysis are presented in the fourth chapter while the fifth chapter wraps up this dissertation with conclusion and suggested future work.

[This page intentionally left blank]

CHAPTER 2

FUNDEMENTAL CONCPTS AND LITERATURE STUDY

One of the prominent research fields in information hiding is steganography. By adopting steganography, potential for private and secure communication that has become a necessity in most of the applications in today's world can be achieved (Subhedar & Mankar, 2014). While using steganography, secret data can be concealed in various multimedia carriers (also called objects) such as video, image, audio, and text that acts as cover media to keep and carry sensitive information. Fig 2.1 depicts the well-known research areas in the paradigm of information (data) hiding.

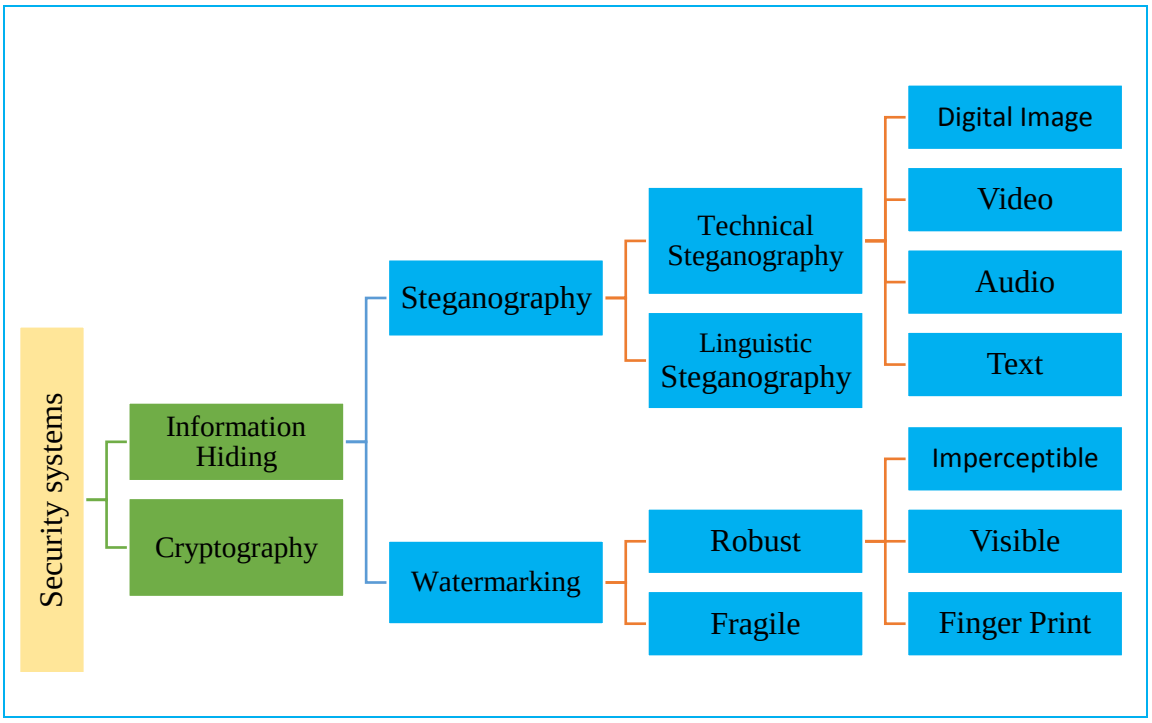

Figure 2.1 Information Hiding Disciplines (Subhedar & Mankar, 2014)

Text steganography can be achieved by modifying the text layout or by utilizing the n^{th} character from text or altering some of the rules such as spaces. Another way is to make use of codes by combining characters, lines and page numbers. Nonetheless, this approach is not secure which makes the text having secret data to be suspected by unauthorized users. On the other hand, concealing information in audio can be performed by utilizing frequencies that are inaudible to human ear.

Correspondingly, it is also possible to embed data in video files. Due to the fact that video file is all about moving streams of images (also known as frames) and sounds, any slight distortion may not be easily seen owing to the continuous flow of information. This technique is somewhat advantageous since high payload capacity can be achieved. The high degree of redundancy encountered in digital image has made it to be the most famous file format for steganography (Cheddad et al., 2010). Furthermore, various researchers have shown that with digital image steganography both the payload capacity and imperceptibility can be maintained if the algorithm is well designed.

2.1 Digital Image Steganography

2.2.1 Fundamental Concepts

This section elaborates some of the basic concepts coupled with technical terms used in digital image steganography.

- **Cover (or carrier) image:** It refers to the image that carries the hidden data.
- **Embedding capacity**: This is the number of bits that can be concealed in the cover image without causing much deformation. It can be represented in the form of bits, kilobits or bits per pixel (bpp).
- **Stego image**: Denotes the image obtained after concealing the secret data.
- **Imperceptibility**: It means that severe deformations should not occur in the cover image after concealing data. That is, embedding the secret data must not change drastically the statistical properties of the original cover image.

Furthermore, the robustness and security are also the conspicuous factors to be considered in digital image steganography (Subhedar & Mankar, 2014).

a) **Robustness**: It shows the amount of alteration that the stego image can resist before the concealed information can be intercepted or destroyed by an adversary.
b) **Security:** The inability of adversaries to detect the secret information.

Generally, as it is illustrated in Fig. 2.2, the image steganography can be broadly categorized into spatial domain, frequency domain, transform domain, spread spectrum and model based steganography approaches (Subhedar & Mankar, 2014).

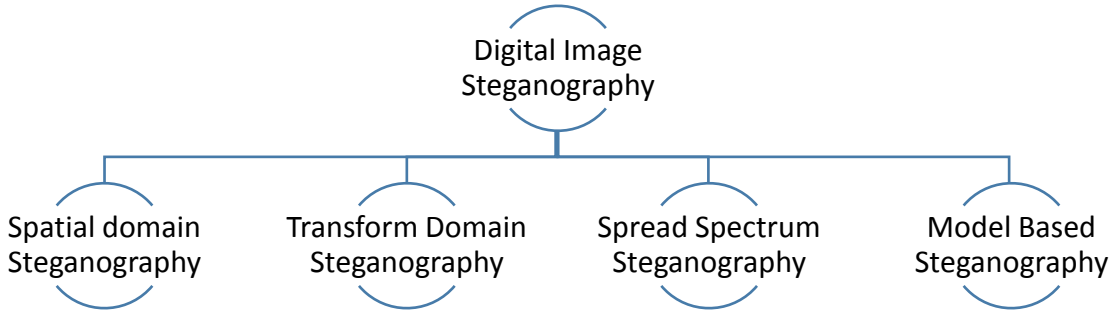

Figure 2.2 Digital Image Steganography Approaches

2.2.2 Image Steganography in the Spatial Domain

In the spatial domain the embedding is performed by immediately concealing the secret data in the image pixel's value. That is, the encoding is performed at the LSB level. The illustration of digital image steganography in the spatial domain can be viewed from Fig. 2.3 below.

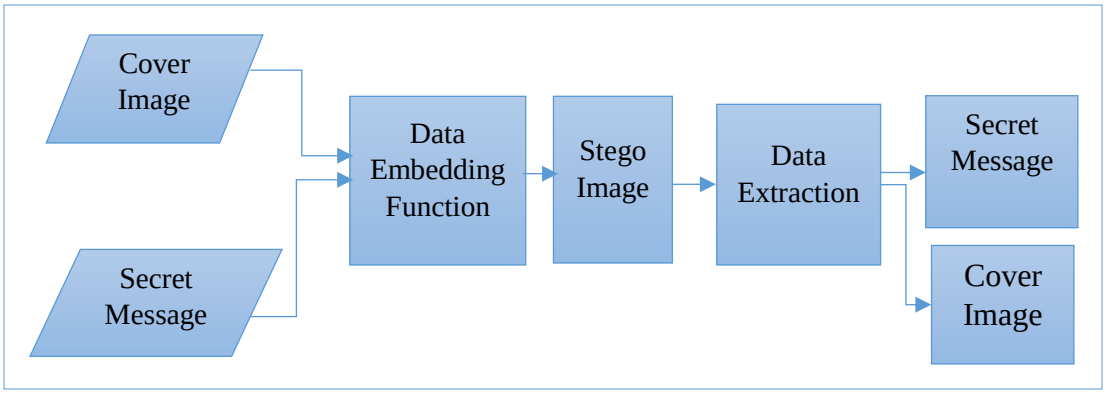

Figure 2.3 Architecture of Image Steganography in the Spatial Domain

In order to demonstrate this concept, Fig 2.4 depicts the whole process where the embedding is done by performing LSB substitution. Note that the substitution occurs only from the first till the fourth LSB. At the first stage, the embedding begins by first substituting the first LSB of the pixel value for the bit of the secret message and then the same process continues to the second, third till the forth LSB is substituted. It is also important to mention that many modified LBSs will cause a drastic distortion of the stego image and as the results, adversaries can easily suspect the existence of the message which is undesirable while sharing sensitive information through the internet.

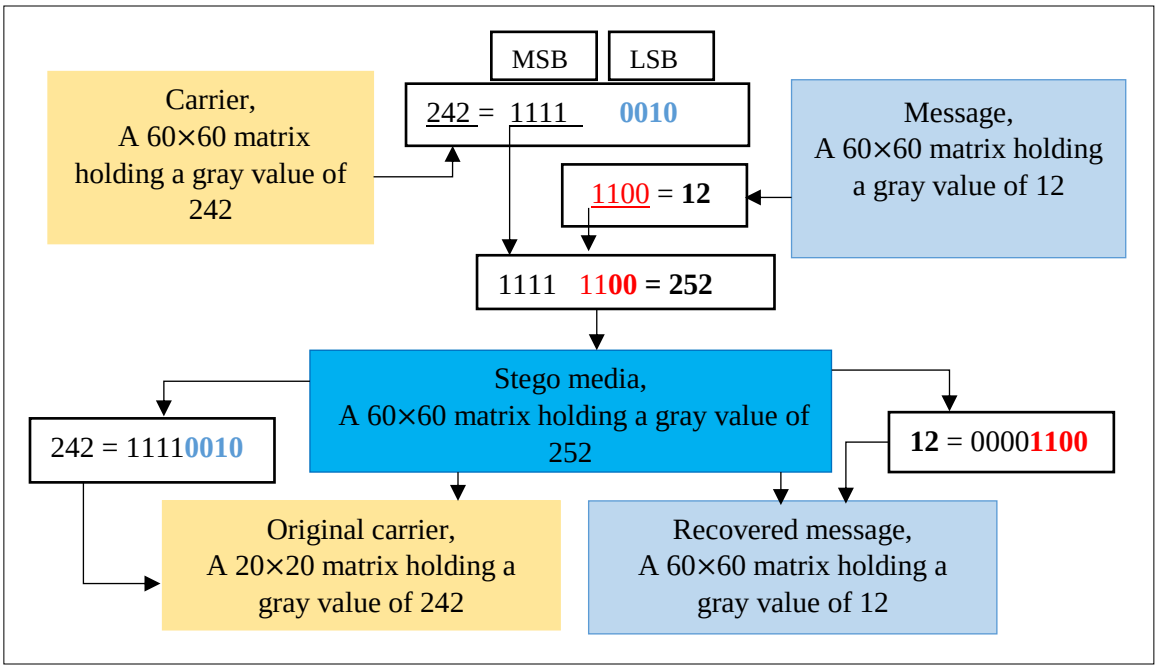

Figure 2.4 The Image Steganography in the Spatial Domain (Cheddad et al., 2010).

The models implemented based on spatial domain approach achieves a high payload capacity. Nonetheless, spatial domain approach can have major security impact compared to the other types of steganographic approaches such as frequency domain approach (Alvarez, 2004). In addition, research have shown that there is always a trade-off between the embedding capacity and the visual quality of cover media holding the secret data. That is, increasing the embedding capacity can result in downgrading the quality of the stego image while high quality will decrease the embedding capacity.

2.2 Literature Study on Digital Image Steganography

In this section, we provide the state of the art on some of the existing digital image steganographic approaches. Moreover, since the proposed approach aims at enhancing the existing methods developed based on the reduced difference expansion scheme, it is crucial to present a review on some of the previous DE and RDE based methods.

2.3.1 Current Trends on Digital Image Steganographic Methods

Digital image steganography has been around for several decades (Anderson & Petitcolas 1998). Hence, this makes it to be among the mature research fields in the paradigm of information hiding. The first example on steganography or data hiding was introduced by

(Simmons, 1883) on "the prisoner's secret message". Since then, this has attracted many researchers to implement data hiding approaches that hides data in digital images. An enhanced multi-layer data hiding method based on IRDE was implemented by (Arham et al., 2017). Their scheme was built by combining two approaches proposed by (Lou et al., 2009) and (Alattar, 2004). Lou et al.'s IRDE was applied in all layers to control the embedding capacity and the quality as well. Besides, their results show that the quality and the embedding capacity were improved. Both visual quality of the stego image and the payload capacity were enhanced by utilizing modulo function and four-pixel differencing (Liao et al., 2012). The difference between pixel pairs was calculated by first defining four neighboring pixels in each block, after that the secret data were hidden based on the obtained difference values.

The data hiding approach developed using pixel value differencing and FFEMD was further suggested by (Kuo et al., 2016). Data were concealed in digital image by utilizing mean and additive modulus (Agrawal & Kumar, 2017). Moreover, data were embedded in two layers of RGB colored images (Verma et al., 2013). The author in (Swain, 2016) proposed a scheme that utilizes correlation calculated between neighboring pixels to conceal data in digital image. The difference expansion and modulus function were combined in the data hiding approach implemented by (Maniriho & Ahmad, 2018b). The existing methods based on pixel value ordering were improved by a model suggested by (Wang et al., 2015) which utilizes a dynamic blocking technique to adaptively partition the cover image into blocks of various sizes. Two important areas ("flat and rough areas") were considered within the image. To achieve high payload capacity, small blocks were generated from flat areas and large blocks were constructed from the rough areas in order to prevent PSNR from being decreased. Their experimental results show that making the block size dynamic has advantages over blocks with fixed sizes since it can simultaneously improve the embedding capacity while achieving low degradation of the stego image. Several approaches that conceal secret data by employing spatial domain approach have been implemented (Datta et al., 2016) and (Tayel et al., 2016).

Secret data were embedded in the difference and sum computed by considering adjacent pixel pairs in non-overlapping blocks (Tyagi et al., 2015). Besides, both secret message and the cover image were fed to the algorithm as inputs. Since their algorithm makes use of two parameters to embed data, some options have been defined before embedding. For

example, if the data cannot be embedded in the difference, it can then be embedded in the sum. However, if it is possible to embed data in the sum or difference, the option that achieves more embedding bits is chosen. Moreover, if both methods are able to achieve high embedding capacity, the method that makes less changes in the value of the pixel pairs is utilized for embedding. The LSB and 8nPVD were utilized to implement the method presented by (Kalita & Tuithung, 2016). This method divides a grayscale image into blocks of size 3×3 which are non- overlapped. Different from other schemes, blocks were constructed in row major order. To obtain the number of secret bits that can be hidden in the LSBs of the difference values, the gray level was further split up into different ranges thereafter the secret bits to be concealed were computed using the generated gray level range table. The modulus function, DE and pixel block of quad were employed to build the data hiding model presented by (Kurniawan et al., 2016). A method where pixels for hiding secret data are selected randomly was suggested in (Saleema & Amarunnishad, 2016) and the hybrid fuzzy neural networks was used to perform the post processing of the stego media.

Han et al. introduced a new model aiming to incorporate steganography into cybersecurity (Han et al., 2017). The embedding positions have to be selected based on smooth and edge areas before concealing data (Li et al., 2017). The large smooth areas are one of the well-known characteristics of medical images (Arham et al., 2016). This property permits secret data to be concealed with less distortion of the cover image. That is, the stego media cannot be easily suspected by malicious users. The LSB-matching approach that uses seven rules to disguise the modification of pixels was presented in Lu et al.'s work (Lu et al., 2015). Their approach employs the technique of dual image to embed confidential data. Dual image is one of the current reversible data hiding technique which conceals data by creating two identical copies of the same original carrier image to be used for concealing data so as to increase the payload capacity. Lu et al.'s method has proven the dual image concept by yielding a high payload capacity while maintaining the quality of the stego image. A steganographic method for RGB digital images was implemented by (Laffont et al., 2017).

In 2013, (Nagaraj et al., 2013b) introduced a pixel value modification method using modulus function. Their method divides colored cover image into three planes (or components) namely, Red, Green and Blue where every pixel contains 24 bits (8 bits for each color).

Additionally, in this method, all the three components have been used for data embedding after applying modulus three function to the pixel values in each color component. Their embedding process is explained in the following steps:

Step 1: Separate the color image into three components color matrices and sequentially apply the next steps on each of them i.e. apply the next steps on the first pixel value of Red matrix, Green matrix and the first pixel of the Blue matrix. The same process continues for the second pixel value of each plane until all pixels are accessed.

Step 2: Let S be the secret digits in base 10. These digits are first converted into base 3 values after that the obtained digits are embedded in all three planes (Red, Green and Blue).

Step 3: Pixel values are grouped into different sets $\{, g_{gi}, and\ g_{bi}\}$ with these three parameters representing the set for Red, Green and Blue pixel values respectively.

Step 4: The suitable pixel to be selected for embedding should fall in the range of $0 \leq g_i \leq 250$. where g_i denotes the ith suitable pixel.

Step 5: Perform the embedding by increasing or decreasing the original pixel value by 1 or -1 respectively. Note that the decision for embedding data is taken after comparing the modulus values and the digits to be concealed. That is, having the secret digits S and the values obtained by applying modulus three function on each pixel value which is denoted by f, three criteria are considered.

1. Criterion 1: $If\ s = f$ the original pixel value is not modified.
2. Criterion 2*:* $If\ s \neq f$ and $f < s$, the original pixel value is increased by 1.
3. Criterion 3*:* $If\ s \neq f$ and $f > s$ the original pixel value is decreased by 1.

During the extraction, the stego image is divided into three planes Red, Green and Blue correspondingly after that the secret digits are obtained by applying modulus three function to each pixel value. Moreover, the extracted digits values have to be converted back to base 10 to get the original secret message.

2.3.2 Difference Expansion Method

The difference expansion is a data hiding technique that allows data to be concealed in the difference values obtained after computing the difference between pixel pairs within the image. This technique has become more popular due to its simplicity. Thereby, several DE-based

methods already exist in the literature. A data hiding method based on difference expansion was presented in the work carried out by (Tian, 2003). With this method, the embedding process begins by first dividing the image into blocks of size 2 by 1 $\rightarrow (2 \times 1)$ and then looping throughout all defined blocks to compute the average and the difference between each two adjacent pixels. Thereafter, the binary bits of the secret data are hidden into each obtained difference value. That is, each difference is expanded by adding one bit of secret data according to the predefined conditions which control the embedding process. After concealing the secret data, the stego image holding the hidden secret data have to be constructed. The details about their method is presented as follows. Given two neighboring pixels u_1 and u_2 depicted in Fig. 2.5, if we want to reversible hide one binary bit of data which can be zero or one, b $\rightarrow$\{0,1\}, the following operations are performed.

1. The Average m and the difference $\boldsymbol{v}$ are calculated using (1).

$$m = \left\lfloor \frac{u_1 + u_2}{2} \right\rfloor \quad \text{and} \quad v = u_1 - u_2 \tag{1}$$

2. The difference v is expanded by adding a secret bit using the equation (2)

$$v' = 2 \times v + b \tag{2}$$

3. After performing (2), the new pixels u'_1 and u'_2 are constructed using (3)

$$u'_1 = m + \left\lfloor \frac{v'+1}{2} \right\rfloor \quad \text{and} \quad u'_2 = m - \left\lfloor \frac{v'}{2} \right\rfloor \tag{3}$$

Where u'_1 and u'_2 represent the neighboring pixels in the stego image. Notice that the value of the pixel u'_1 and u'_2 must not be underflow or overflow since these two types of pixels result in unrecoverable data. To avoid this problem, the difference v' has to fulfill the conditions presented in (4).

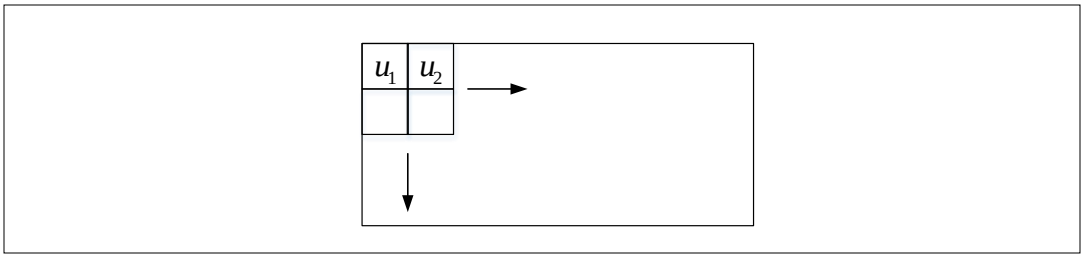

Figure 2.5 Neighboring pixels in a grayscale image

$$\begin{cases} |v'| \leq 2 \times (255 - m) & if\ 128 \leq m \leq 255 \\ |v'| \leq 2 \times m + 1 & if\ 128 \leq m \leq 127 \end{cases} \quad (4)$$

Having the above expressions, let us then take an example of a pixel's pair having values of 206 and 201, $pixel's\ pair \rightarrow (206, 201)$ to elucidate the embedding and extraction process

Step 1**:** Compute average m and difference v as shown in (5)

$$m = \left\lfloor \frac{206+201}{2} \right\rfloor = 203 \quad \text{and} \quad v = 206 - 201 = 5 \quad (5)$$

Step 2: Embed one secret bit, i.e., b →1 to the obtained difference v using (6)

$$v' = 2 \times 5 + 1 = 11 \quad (6)$$

Step 3: Use (7) to compute the new pixel to be used while constructing the stego image

$$u'_1 = 203 + \left\lfloor \frac{11+1}{2} \right\rfloor = 209 \quad \text{and} \quad u'_2 = 203 - \left\lfloor \frac{11}{2} \right\rfloor = 198 \quad (7)$$

Now the new pixel's pair holding the hidden bit becomes (209, 198). Since Tian's method is reversible, both the secret message and the original pixels are recovered as follows. As it was performed during the embedding process, the extraction begins by first computing the average and the difference between the pixel pairs from the stego image.

Step 1: Compute the average m and difference v**.** That is, for the pixel's pair **(**209, 198), m and v are computed using (8).

$$m = \left\lfloor \frac{209+198}{2} \right\rfloor = 203 \quad \text{and} \quad v = 209 - 198 = 11 \quad (8)$$

Step 2: to get the original difference v and the hidden bit, (9) and (10) are utilized.

$$v' = \left\lfloor \frac{11}{2} \right\rfloor = 5 \ \rightarrow \ b = LSB(11) = 1 \quad (9)$$

Step 3: Reconstruct the original pixel pair u_1 and u_2 by utilizing the equation in (10).

$$u_1 = 203 + \left\lfloor \frac{5+1}{2} \right\rfloor = 206 \quad \text{And} \quad u_2 = 203 - \left\lfloor \frac{5}{2} \right\rfloor = 201 \quad (10)$$

Now both the secret message and the original image are well reconstructed. However, Since this method can cause underflow or overflow for certain images, it was further improved in terms of both quality and embedding capacity by (Alattar, 2004), who proposed the data hiding scheme based on difference expansion of quad.

2.3.3 Quad Based Difference Expansion

Different from (Tian, 2003), with the method suggested by (Alattar, 2004) data can be embedded in quad without causing underflow or overflow. Alattar's scheme works as follows. The image was first divided into blocks called quad. That is, four pixels were defined in each quad. Blocks were formed from both direction, left to right and top to bottom. Furthermore, pixels in each quad were converted into a vector as it is shown in (11) and an integer transformation was further defined. Each vector v has the form of $v = (v_o, v_1, v_2, v_3)$ obtained by calculating the difference between pixels in each block having pixels arranged in a vector $p = (u_o, u_1, u_2, u_3)$.

$$\begin{cases} v_o = \left\lfloor \frac{u_o + u_1 + u_2 + u_3}{4} \right\rfloor \\ v_1 = u_1 - u_o \\ v_2 = u_2 - u_1 \\ v_3 = u_3 - u_2 \end{cases} \tag{11}$$

In order to conceal data, the difference values obtained in (11) have to be modified. Two different stages in (12) and (13) were considered.

1. Expanding the difference

$$\begin{cases} v'_1 = 2 \times v_1 + b_1 \\ v'_2 = 2 \times v_2 + b_2 \\ v'_3 = 2 \times v_3 + b_3 \end{cases} \tag{12}$$

2. LSB modification

$$\begin{cases} v'_1 = 2 \times \left\lfloor \frac{v_1}{2} \right\rfloor + b_1 \\ v'_2 = 2 \times \left\lfloor \frac{v_2}{2} \right\rfloor + b_2 \\ v'_3 = 2 \times \left\lfloor \frac{v_3}{2} \right\rfloor + b_2 \end{cases} \tag{13}$$

If the expression in (12) causes underflow or overflow, (13) is used otherwise the block is marked as non-changeable (no data is embedded to it). Notice that the bits of the secret data to be embedded are denoted by b_1, b_2, b_3 with all belonging to the set $b_n = \{0,1\}$. After embedding data, the new pixels are reconstructed by transforming the vector $v' = v'_o, v'_1, v'_2, v'_3)$ into $p' = (u'_o, u'_1, u'_2, u'_3)$ using (14). The original pixel's block p is replaced by the new one (p') containing the bits of the embedded data in the stego image.

$$\begin{cases} u'_o = v'_0 - \left\lfloor \frac{u_o + u_1 + u_2 + u_3}{4} \right\rfloor \\ u'_1 = v'_1 + u_o \\ u'_2 = v'_2 + u'_1 \\ u'_3 = v'_3 + u'_2 \end{cases} \quad (14)$$

Two criteria have to be fulfilled in order to ensure that data are well embedded. First, the block p' have to meet conditions from (12-14). Second, the resulted pixel containing the hidden data must not be underflow or overflow. If the data is embedded using (12) the block p is said to be expandable whereas if it is carried out using (13), it is said to be changeable. If neither (12) nor (13) is utilized, the block is said to be non-changeable and as the results, the value of the pixel is kept unchanged (no data in concealed to it). To be able to recover the hidden secret message, the location map was defined during the embedding process to record any operation performed in each quad. Furthermore, Fig 2.6 presents their groups of pixel blocks.

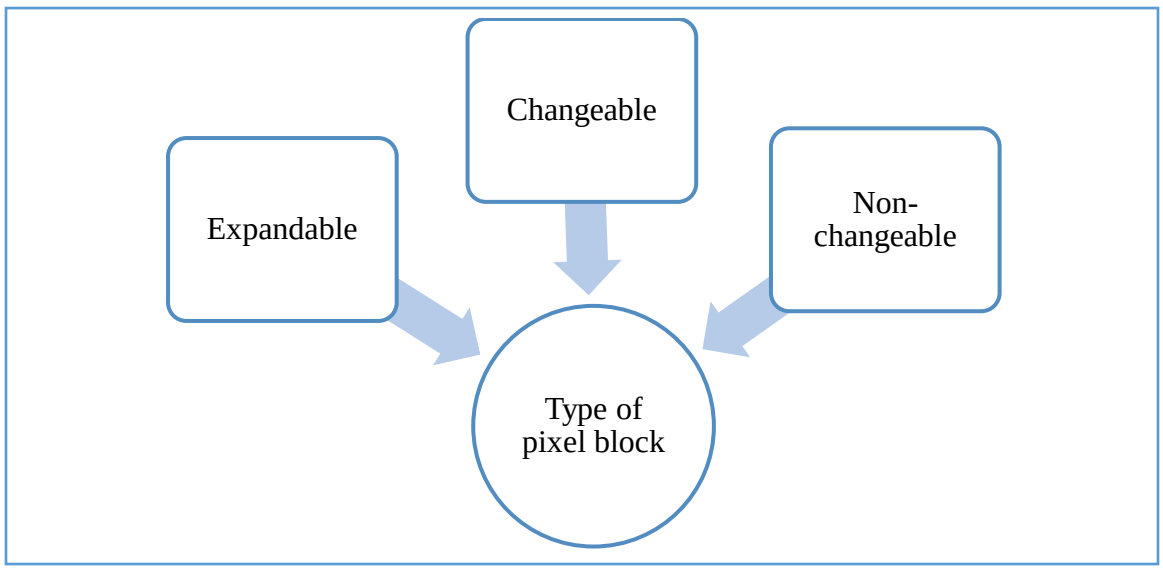

Figure 2.6 Categories of Pixel Block

2.3.4 Reduced Difference Expansion

The reduced difference expansion is another information hiding technique which was developed to improve the traditional difference expansion (DE) method. Its main goal is to allow data to be embedded into small values which greatly preserves the similarity between the stego image and its respective cover image. Hence, several RDE based algorithms have been already developed. The visual quality of the stego image and the embedding capacity were improved by the reduced difference expansion scheme proposed by (Lou et al., 2009). The RDE expression in (15) was proposed in order to reduce the difference values.

$$v'_n = \begin{cases} v_n & if\ v_n < 2 \\ v_n - 2^{\lfloor log_2 v_n \rfloor - 1} & otherwise \end{cases} \quad (15)$$

With this scheme, any difference which is equals to 1 or 0 was not changed, i.e., there is no reduction applied to it. To be able to restore the hidden data, this method uses the location map (LM) in (16) to record information about each pixel reduction. Besides, in order to restore the original cover media, the expression in (17) was given.

$$LM = \begin{cases} 0 & if\ \ 2^{\lfloor log_2 v'_n \rfloor} = 2^{\lfloor log_2 v_n \rfloor}\ or\ v'_n = v_n \\ 1 & if\ \ 2^{\lfloor log_2 v'_n \rfloor} \neq 2^{\lfloor log_2 v_n \rfloor} \end{cases} \quad (16)$$

$$v_n = \begin{cases} v'_n - 2^{\lfloor log_2 v'_n \rfloor - 1} & if\ LM = 0 \\ v'_n - 2^{\lfloor log_2 v_n \rfloor} & if\ LM = 1 \end{cases} \quad (17)$$

According to their experimental results, reducing the difference preserves good visual quality and embedding capacity as well.

2.3.5 Improved Difference Expansion-IRDE

In 2009, Lou's method (Lou et al., 2009) was further enhanced by (Yi et al., 2009), who proposed the improved reduced difference expansion (IRDE) reduction function in (18).

$$v'_n = \begin{cases} v - 2^{\lfloor log_2 v_n \rfloor - 1} & if\ 2 \times 2^{n-1} \leq v_n \leq\ 3 \times 2^{n-1} - 1 \\ v - 2^{\lfloor log_2 v_n \rfloor} & if\ 3 \times 2^{n-1} \leq v_n \leq\ 4 \times 2^{n-1} - 1 \end{cases} \quad (18)$$

Where

$$n = \lfloor log_2 |v_n| \rfloor$$

When the original difference values fall in the interval of $3 \times 2^{n-1} \leq v \leq 4 \times 2^{n-1} - 1$, small difference values are obtained. Based on the modified IRDE expression, the location map in (19) was defined in order for extracting the secret data and to recover the original difference, the equation in (20) was suggested.

$$LM = \begin{cases} 0 & if\ 2 \times 2^{n-1} \leq v_n \leq 3 \times 2^{n-1} - 1 \\ 1 & if\ 3 \times 2^{n-1} \leq v_n \leq 4 \times 2^{n-1} - 1 \end{cases} \quad (19)$$

$$v'_n = \begin{cases} v_n + 2^{\lfloor log_2 v_n \rfloor + 1} & LM = 1 \\ v_n + 2^{\lfloor log_2 v_n \rfloor} & if\ LM = 0 \end{cases} \quad (20)$$

The details about the embedding and extraction procedures of Yi et al.'s scheme can be found in (Yi et al., 2009).

2.3.6 General Smoothness Difference Expansion

The data hiding scheme based on general smoothness difference expansion was further proposed by (Holil & Ahmad, 2015). Similar to the other steganographic approaches, their method consists of two main parts, namely, data embedding and extraction. Besides, it was developed based on the quad smoothness and generalized difference expansion (GDE) and data embedding was performed as follows. Suppose U_{m0}, U_{m1}, U_{m2} *and* U_{m3} are the first pixels in the pixel blocks *A*, *B*, *C* and *D* respectively. The smoothness level was computed using (21) and (22).

$$v_a = \frac{\sum_{i=0}^{3} (u_{mi-avg})^2}{4} \quad (21)$$

$$avg = \frac{\sum_{i=0}^{3} u_{mi}}{4} \quad (22)$$

Where v_a = Variance

avg = Average

Similar to the DE presented in (Alattar, 2004), the data embedding for this method was accomplished by first calculating the difference between pixels in their respective blocks using the median as the base point (23) in each pixel block. Note that in the above expression u_m denotes the median computed in each block of pixel.

$$\begin{cases} v_1 = u_1 - u_m \\ \quad \ldots . \\ \quad \ldots . \\ \quad \ldots . \\ \quad \ldots . \\ v_{N-1=u_{N-1}-U_m} \end{cases} \tag{23}$$

The GDE in (24) was applied before embedding data by considering both negative and positive values. In addition, according to the values obtained in (24), two categories of pixel's block were defined. That is, the expandable blocks were divided into two subcategories according to the result of the equation below (24). Those are, expandable RDE if $v'_n \neq v_n$ and expandable non-RDE if $v'_n = v_n$.

$$v'_n = \begin{cases} v_n & if -2 < v_n < 2 \\ v_n + 2^{\lfloor log_2 |v_n| \rfloor} - 1\,, & if\ v_n \leq -2 \\ v_n - 2^{\lfloor log_2 |v_n| \rfloor} - 1\,, & if\ v_n \geq 2 \end{cases} \tag{24}$$

Besides, two bits of data were concealed into expandable blocks (expandable RDE and expandable non-RDE) whose $v_a = 1$ and one bit where variance is greater than one $(v_a > 1)$ using (25). Note that b belongs to the set $[1,2,3]$, where 1, 2 and 3 represent the binary which can be bits 0 or 1 respectively.

$$\begin{cases} v''_1 = 4 \times v_1 + b_1 \\ \quad \ldots . \\ v''_{N-1=4\times v_n + b_{N-1}} \end{cases} \tag{25}$$

Their method has improved the capacity and the quality of the stego image. However, it doesn't perform well for some images which results in degrading the quality of the stego image, i.e., its PSNR is lower than that of the previous methods for certain images.

2.3.7 Quad of Quad Based RDE

In the work presented by (Ali AL_Huti et al., 2015), another information hiding technique based on RDE and pixel's block was implemented. Before applying their proposed RDE-scheme the cover image was first segmented into blocks of quad of quad (4×4). Fig. 2.7, illustrates their pixel's block, where 16 pixels were defined in each block. After generating all blocks, (26) was utilized to compute the difference between pixel pairs in each block except

that the first pixel was not used to hide data. Furthermore, the RDE-scheme presented in (27) was used to reduce the difference and the pixel blocks were grouped into different groups namely, "expandable, changeable and non-changeable". Notice that these groups are similar to the ones in (Alattar, 2004) and (Ahmad et al., 2013).

$$\begin{cases} v_0 = 0 \\ v_1 = u_1 - u_0 \\ v_2 = u_2 - u_1 \\ \quad \dots\dots \\ \quad \dots\dots. \\ v_{15} = u_{15} - u_{14} \end{cases} \tag{26}$$

$$v''n = \begin{cases} v_n - (2^{\lfloor \log_2 |\, v_n \rfloor |}) + (\lfloor \log_2 v_n \rfloor) & if\ v_n > 1 \\ v_n + (2^{\lfloor \log_2 |\, v_n \rfloor |}) + (\lfloor \log_2 |\, v_n \,| \rfloor) & if\ v_n < -1 \end{cases} \tag{27}$$

After performing the reduction, the data was concealed as in (12) and (13) and the new pixels having data were computed using (28). Additionally, the hidden message was extracted using the location map defined during the embedding process and the values of the reduced difference were restored using the recovery expression in (29).

$$\begin{cases} u'_o = u_0 \\ u'_1 = v'_1 + u_o \\ u'_2 = v'_2 + u'_1 \\ \quad \dots \\ \quad \dots. \\ \quad \dots. \\ u'_{14} = v'_{14} + u'_{13} \\ u'_{15} = v'_{15} + u'_{14} \end{cases} \tag{28}$$

$$v_n = \begin{cases} v''_n + \left(2^{\lfloor \log_2 v''_n \rfloor - 1}\right) + (\lfloor \log_2 v''_n \rfloor - 1) & if\ v''_n > 1 \\ v''_n - \left(2^{\lfloor \log_2 |\, v''_n \rfloor |}\right) + (\lfloor \log_2 |\, v''_n \rfloor) & if\quad v''_n < -1 \end{cases} \tag{29}$$

Where

u = Original pixel before hiding data

v = Difference before reduction

v''_n = Reduced difference before hiding data

v'_n= Difference holding the secret data (difference obtained after hiding data)

u' = New pixel in the stego image

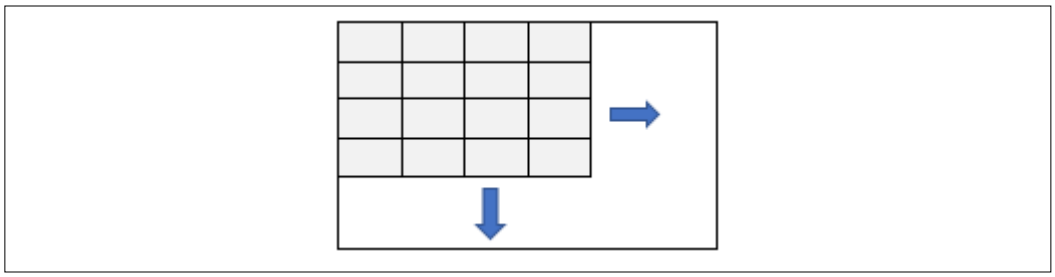

Figure 2.7. Quad of Quad Pixel's Block

v_n = Original difference after recovery

Accordingly, with this approach, the embedding capacity was improved. Nevertheless, with reference to their experimental results, the quality of the stego image was decreased due to defined large pixel's block. In addition, it is worth to mention that such degradation of the stego image is undesirable since it could lead to disclosing the communication existence.

2.3 Evaluation Metrics

2.4.1 Peak Signal-to-Noise Ratio (PSNR)

The PSNR is computed to analyze and evaluate how the stego image degrades with respect to the original cover image. If the PSNR value is high, the quality of the stego image is better. That is, the stego image is not drastically distorted. Besides, the value of the PSNR is computed using (31), where MSE is obtained using (30).

$$\text{MSE} = \left(\frac{1}{\text{WH}}\right) \sum_{i=1}^{H} \sum_{j=1}^{W} (P_{ij} - M_{ij})^2 \quad (30)$$

$$\text{PSNR} = 10\log_{10} \frac{(\text{MAX})^2}{\text{MSE}} \quad (31)$$

In (30), P_{ij} represents the pixel's value in the original image and M_{ij} corresponds to the stego image pixel's value which is located at (i, j) position and the MSE refers to the mean squared error. It gives information about how the stego image P' differs from the original image P. Moreover, regarding the equation presented in (31), MAX is used to denote the maximum pixel value while W and H denote the width and height of the image respectively.

2.4.2 Histogram Visualization

The number of occurrence of pixels with respect to a particular value of the pixel can be measured using histogram (Fridrich et al., 2003). In addition, the pixel values change throughout the embedding, thus the number of pixel values having the embedded data are different from their respective original ones. In this way, unauthorized individuals can take

advantage of these changes and interfere communication while trying to get the hidden secret message. Hence, slight changes (also known as deformation) in the histogram of the stego image are always desirable since there are less chances to detect or suspect the stego image. that is, severe changes in the cover image are always not desirable since they will greatly change its statistical properties and histogram which may arouse the suspicions.

2.4.3 Embedding Capacity

The embedding (payload) capacity is the number of bits that can be accommodated in the cover image. It can be expressed in bits, kilobits or bit per pixel (bpp).

[This page intentionally left blank]

CHAPTER 3
RESEARCH METHODOLOGY

This chapter provides a detailed discussion demonstrating the functionality of the proposed approach. Additionally, as depicted in Fig 3.1, research activities are divided in eight stages, namely, literature study, algorithm design, algorithm implementation, testing and validation, results analysis and discussion, writing final report, report presentation and finally submitting the final report after being approved by the examination committee. The full schedule for research activities accomplished in this work is presented in the next section (see Table 3.3). Considerably, a comprehensive design and discussion elucidating the functionality of the proposed method is provided.

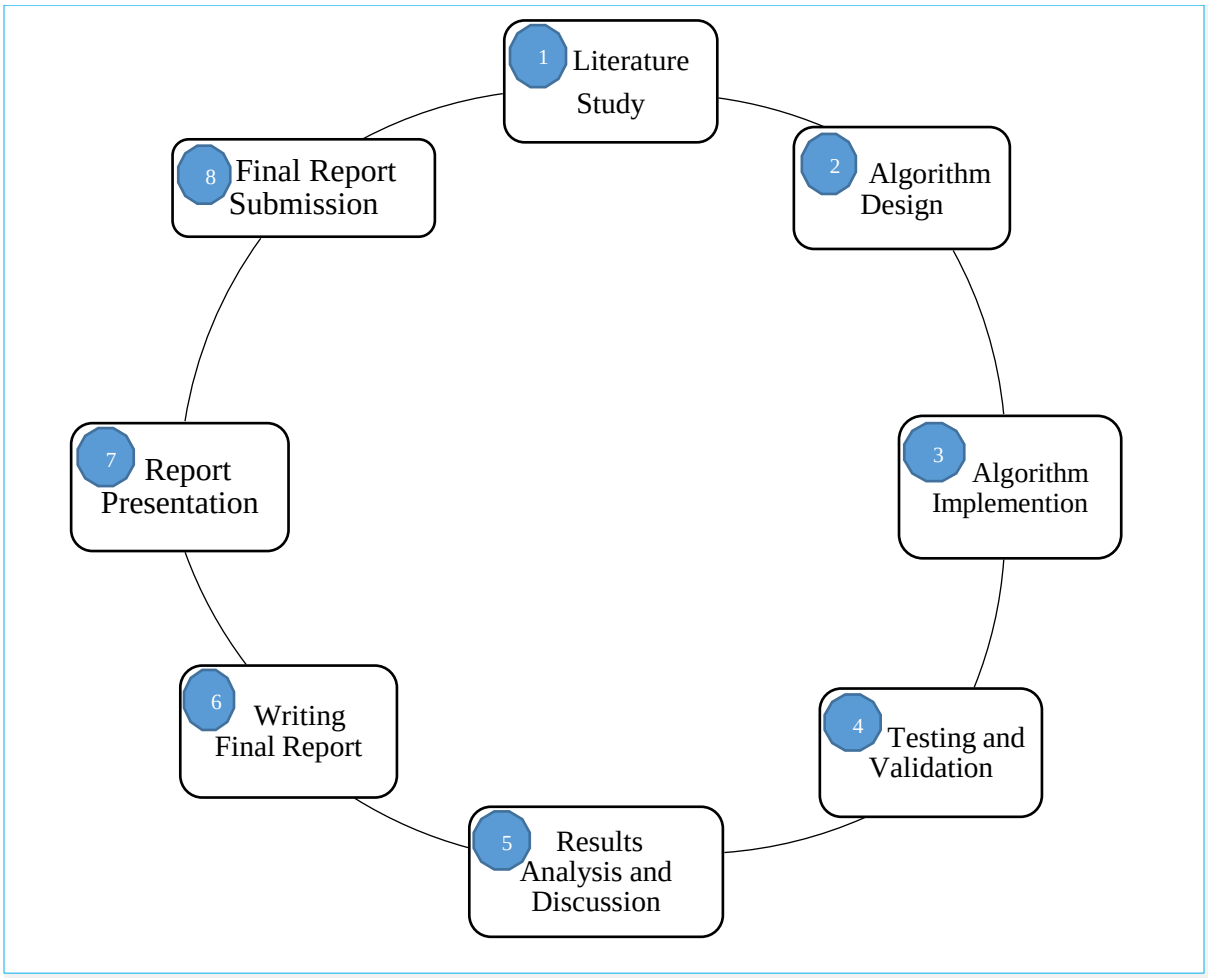

Figure 3.1 Research Methodology Steps

3.1 Exploring the Literature

Since it is highly recommended to have a strong background and knowledge on the existing information hiding approaches before going for any enhancements of other authors' work, in this research we consider various documentations such as books, journal articles, conference based papers, online blogs and portals providing relevant information related to this research. In this way, the background study was presented in chapter 1 while the fundamental concepts used in the paradigm of information hiding and the literature study detailing the operation of the existing approaches were elaborated in the second chapter.

It is also important to notice that most of the approaches previously discussed are related to this research. This is because if we look at them especially those ones implemented based on DE and RDE concepts, they have been developed in such a way that one is enhancing another. Moreover, after exploring the literature, a clear research problem and relevant solution are well formulated in this chapter. That is, this research addresses the problems encountered in the existing methods and provides better solution.

3.2 Designing the Proposed Algorithm

As mentioned in the previous sections, this research intends to enhance the previous data hiding techniques specifically the one presented by (Ali AL_Huti et al., 2015). Ideally, since the suggested approach is mainly implemented based on pixel's block, constant based point and the reduced difference expansion (RDE), we begin by first defining the pixel's block. In (Ali AL_Huti et al., 2015) the cover image was divided into blocks of quad of quad (block of size 4 by 4) which has resulted in achieving a good embedding capacity while decreasing the PSNR value which degrades the quality of the stego image.

To solve the problem of pixel's block which achieves a good embedding capacity while decreasing the quality of the stego image, the block of pixel is adjusted from size of 4×4 to 2×2, so as to allow data to be concealed without worsening the stego media. Note that the difference between these blocks can be viewed from Fig. 3.2 which is depicted below. Second, to make sure that the quality of the cover media and the embedding capacity are well preserved, the previous RDE- scheme in (29) which is used to reduce the difference is also ameliorated in order to get possible small values to be utilized while concealing the secret data. The enhanced RDE-scheme does not only ameliorate the quality of the stego image but also the

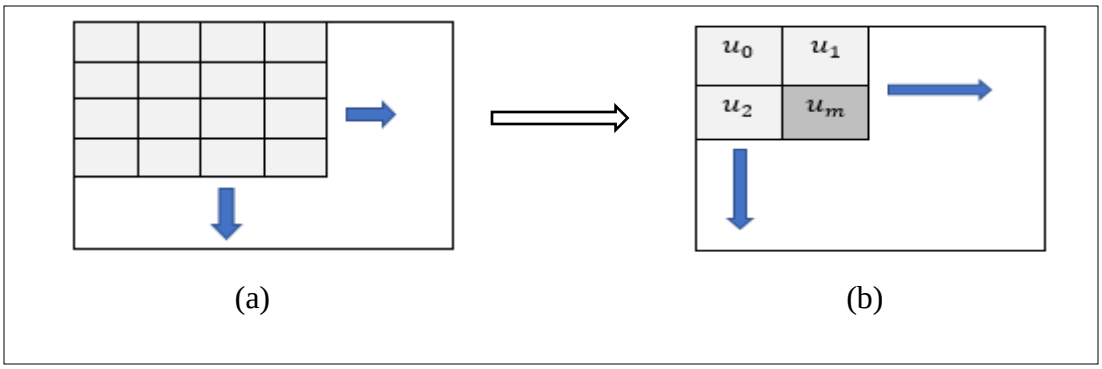

Figure 3.2 (a) Previous Pixel's block (b) Suggested Pixel's Block

embedding capacity. Additionally, the new constant base point for each pixel's block is chosen differently for increasing the quality of the stego image. This new base point also reduces the number of pixels which can be underflow or overflow, i.e., pixels whose values are out of the gray level range ($0 \leq$ Pix_value ≤ 255) since in contrast to was carried out in the previous work (Ali AL_Huti et al., 2015) two pixels values are not added up in order to get the new pixels for constructing the stego image. Hence, both the quality and capacity can be well maintained.

Overall, in order to design and implement the suggested method, two main phases, namely, embedding phase (which deals with embedding the secret data) and the extraction phase (which is about extracting the hidden data, restoring the reduced difference values and constructing the original cover image) are elaborated. These phases can be viewed in Fig. 3.3.

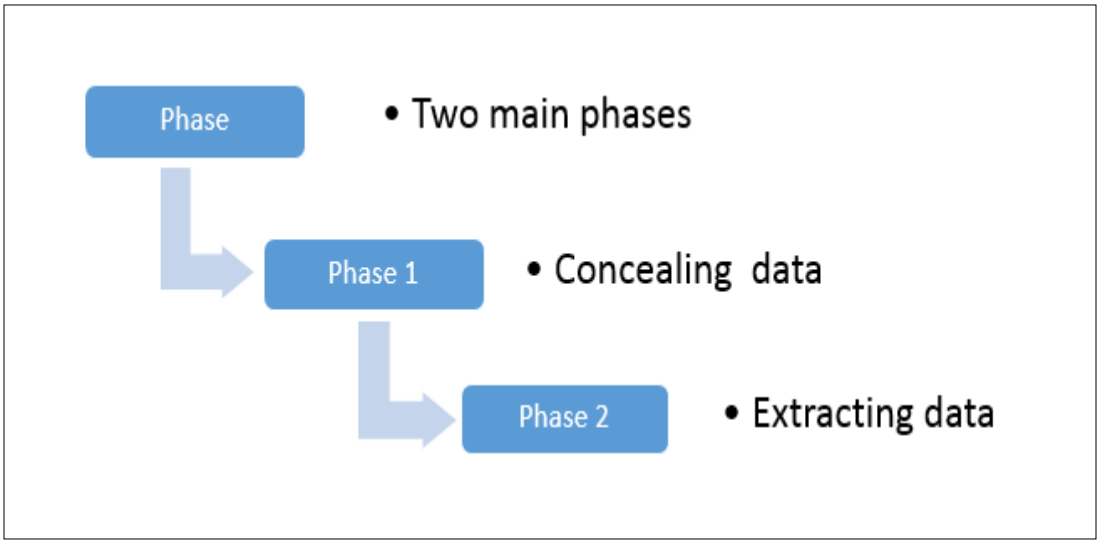

Figure 3.3 Main Phases for the Proposed Approach

3.2.1 Phase 1: Steps for Embedding Data

This section discusses the necessary steps that demonstrates how the proposed method is applied to conceal the secret data into the cover image. Given the cover image h of size f by p $(f \times p)$, the embedding process is accomplished as follows.

Step 1: It is first segmented into m blocks or structures of size 2×2. That is, with this proposed method each block has 4 pixels. From Fig. 3.2 (b), a block of pixel is represented by u_o, u_1, u_2, and u_3. To remove bewilderment, the terms block and structure are going to be used interchangeably.

Step 2: Before computing the difference between pixel pairs, all pixels in each block are first stored as vector. If u_o, u_1, u_2, and u_3 are pixels in the first block, the vector is defined as $u_{vec} = (u_o, u_1, u_2, u_3)$. Similar to what was proposed by (Ali AL_Huti et al., 2015), pixel blocks are categorized into three groups namely expandable, changeable and non-changeable. To avoid the problem of overflow and underflow, the secret data are only concealed in the first and second group. Besides, for expandable blocks data are concealed using (12), while (13) is used for changeable blocks. Due to the fact that non-changeable blocks can lead to the problem of underflow or overflow, they are disregarded during the embedding process.

Step 3: In contrast to the previous method, use the last pixel of each block as the base point. For the pixel block mentioned in Fig. 3.2, the base point would be u_m which is equivalent to u_3 in each block since we are counting from zero to three $(0\ to\ 3)$.

Step 4: Iterate through all defined pixel blocks and compute the difference between pixel pairs using (32). It is also important to mention that (32) totally differs from the previous expression presented in (Ali AL_Huti et al., 2015). Besides, as in (Ahmad et al., 2013), only three differences (v_0, v_1 and v_2) are computed.

$$\begin{cases} v_0 = u_0 - u_3 \\ v_1 = u_1 - u_3 \\ v_2 = u_2 - u_3 \\ v_3 = 0 \end{cases} \tag{32}$$

However, in contrast to their method, v_3 is not being used to conceal the secret data for our method. That is, v_3 is initialized to zero ($v_3 = 0$) since the fourth pixel in each block is taken as the base point. Schematically the process in (32) can be viewed in Fig. 3.4.

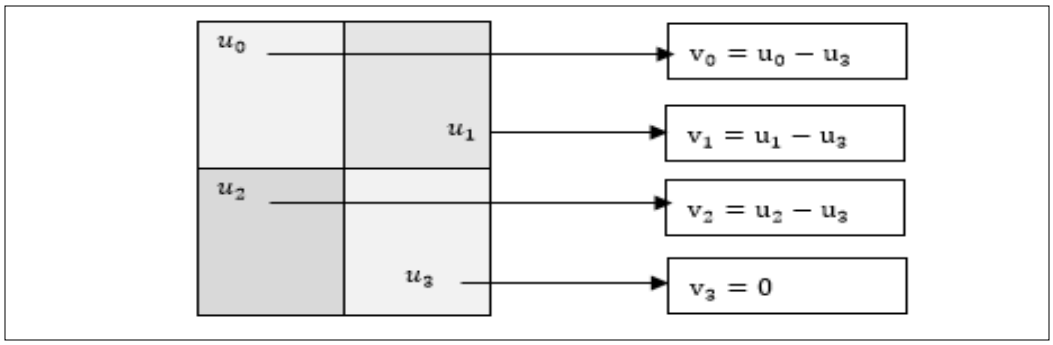

Figure 3.4 Process for Computing the Difference Between Pixels

Step 5: Hide data by first reducing the differences v_0, v_1 and v_2 according to the defined rules (criteria), i.e., compute the reduced difference expansion (RDE) for any difference (v_0, v_1 and v_2) which is greater than one or less than minus one (v_0, v_1 and v_2) $>$ 1 or (v_0, v_1 and v_2) <-1. Similar to the previous research values between 1 and -1 or (-1$\leq$ $v_n \leq$1) are not reduced as they may result in distorting the secret message and the cover image. Note that as mentioned before, the RDE expression in (29) which was implemented by (Ali AL_Huti et al., 2015) is enhanced in order to reduce the difference between pixel pairs to the possible smallest values which are appropriate for data to be embedded suitably. This enhancement is made by doubling the second logarithmic term. By doing so as it is presented in (33), it could be easily seen that by utilizing the new proposed RDE scheme small difference values are obtained. RDE is computed using both parts of (33), those are: (i) if $v_n > 1$, the first part is applied, and (ii) if v_n <-1, the second part of the RDE scheme is applied.

$$v''_n = \begin{cases} v_n - (2^{\lfloor \log_2 v_n \rfloor} + 2(\lfloor \log_2 v_n \rfloor)) & if\ v_n > 1 \\ v_n + (2^{\lfloor \log_2 v_n \rfloor} + 2(\lfloor \log_2 v_n \rfloor)) & if\ v_n < -1 \end{cases} \quad (33)$$

In the above expression v_n for each block starts from 0 to 3 ($0 \leq v_n \leq 3$), $\forall n \in \mathbb{R}^+$except that $v_n = 3$ (v_3) is not utilized to conceal data in each block. The difference between the proposed RDE scheme and the one implemented in (Ali AL_Huti et al., 2015) as it is shown in (29) can be demonstrated as follows: considering a pixel's block $u = (u_o, u_1, u_2, u_3)$ having pixel values $u_0 = 90,\ u_1 = 65,\ u_2 = 100\ and\ u_3 = 40$. By utilizing u_3 as the based point, the difference is computed using (32), thereafter we get the vector v having difference values $v_0, v_1, and\ v_2, \rightarrow v = (v_0, v_1, v_2)$.

$$\begin{cases} v_0 = u_0 - u_3 = 90 - 40 = 50 \\ v_1 = u_1 - u_3 = 65 - 40 = 25 \\ v_2 = u_2 - u_3 = 100 - 40 = 60 \\ v_3 = 0 \end{cases}$$

Since all difference values are still greater than one $(v_0, v_1 \; and \; v_2 > 1)$, they have to be reduced before embedding data. Notice that all of these 3 difference values have to fulfill the same condition. Now let us evaluate how these two reduction schemes differ by first using (i) the existing RDE-scheme in (29); and (ii) the proposed RDE-scheme in (33) whose result can be summarized in Table 3.1.

(i)Existing RDE $\rightarrow v''_n = v_n - (2^{\lfloor \log_2 v_n \rfloor} + \lfloor \log_2 v_n \rfloor)$

$\rightarrow v_0 = 50$

$v''_0 = 50 - (2^{\lfloor \log_2 50 \rfloor} + \lfloor \log_2 50 \rfloor)$

$v''_0 = 50 - \; (32 + 5)$

$v''_0 = 13$

$\rightarrow v_1 = 25$

$v''_1 = 25 - (2^{\lfloor \log_2 25 \rfloor} + \lfloor \log_2 25 \rfloor)$

$v''_1 = \; 25 - (16 + 4)$

$v''_1 = \; 5$

$\rightarrow v_2 = 60$

$v''_2 = 60 - (2^{\lfloor \log_2 60 \rfloor} + \lfloor \log_2 60 \rfloor)$

$v''_2 = 60 - (32 + 5)$

$v''_2 = 23$

(ii)Proposed RDE $\rightarrow v''_n = v_n + (2^{\lfloor \log_2 v_n \rfloor} + 2(\lfloor \log_2 v_n \rfloor))$

$\rightarrow v_0 = 50$

$v''_0 = 50 - (2^{\lfloor \log_2 50 \rfloor} + 2(\lfloor \log_2 50 \rfloor))$

$v''_0 = 50 - (32 + 10)$

$v''_0 = 8$

$\rightarrow v_1 = 25$

$v''_1 = 25 - (2^{\lfloor \log_2 25 \rfloor} + 2(\lfloor \log_2 25 \rfloor))$

$v''_1 = 25 - (16 + 8)$

$v''_1 = 1$

$\rightarrow v_2 = 60$

$v''_2 = 60 - (2^{\lfloor \log_2 60 \rfloor} + 2(\lfloor \log_2 60 \rfloor))$

$v''_2 = 60 - (32+10)$,

$v''_2 = 18$

It is worth to notice that all values between -1 and 1 are not reduced but they are still used for embedding data. From the reduced differences (v''_0, v''_1 and v''_2) obtained in (i) and (ii), we find that by using the proposed RDE-scheme in (33), small difference values are generated compared to the ones obtained using the RDE-scheme in (29). These small difference values that are generated after the reduction process can then be used for embedding data by utilizing (12) or (13). To compute the new pixel in the stego image, in contrast to the previous methods (Ali AL_Huti et al., 2015) and (Ahmad et al. 2013), we provide (34). Furthermore, to prevent the cover image from being worsened, the secret data are not embedded in the last pixel of each block (u_3) since it is taken as the base point.

$$\begin{cases} u'_0 = v'_0 + u_3 \\ u'_1 = v'_1 + u_3 \\ u'_2 = v'_2 + u_3 \\ u'_3 = u_3 \end{cases} \quad (34)$$

To prevent underflow and overflow, each new pixel u'_n (pixel which is used to construct the stego image) in each block must fulfill the condition $0 \leq u'_n = v'_n + u_m \leq 255$ otherwise the whole block is marked as non-changeable. Notice that u_m denotes the last pixel in each

Table 3.1 Comparing the Reduced Difference Values

Original difference (v_n)	Reduced difference	RDE- based Scheme (Ali AL_Huti et al., 2015)	Proposed RDE-based Scheme
$v_0 = 50$	v''_0	13	8
$v_1 = 25$	v''_1	5	1
$v_2 = 60$	v''_2	23	18
	$Average \rightarrow$	13.66	9

block and v'_n denotes the difference having secret bit after using (12) or (13). As in the previous work, the location map LM is utilized in our proposed method. The main purpose of the location map is to keep track of the embedding information for each block which makes the extraction straightforward if it is well defined and recorded. To make the process clear, the bit 1 in location map indicates that the expansion in (12) was utilized while 0 shows that the LSB in (13) was used to embed data.

For example, from (33) two blocks are defined. That is, expandable RDE if the first or second condition are met and non-expandable RDE if (33) is not fulfilled. Moreover, -1 is used to represent those pixel blocks which are unchanged. Each pixel block's information in the location map is stored in the form of vector, i.e., the location map vector $LM = (LM1, LM2, LM3, LM4, LM5)$ is defined and allocated as follows. Assign bits 1, 0 and -1 for expandable, changeable and non-changeable pixel blocks correspondingly. As well as that, for expandable $LM1 = 1$ is defined and $LM2 = 1$ is assigned for expandable RDE. Additionally, for those blocks falling in the category of expandable RDE, it is also important to assign the location map to keep track of information about each pixel reduction. That is, if $v''_n \pm \left(2^{(\lfloor \log_2 v''_n \rfloor)-1}\right) + 2(\lfloor \log_2 v''_n \rfloor) = v_n$, the $LM3, LM4$, and $LM5$ are set to 0 and if $v''n \pm (2^{\lfloor \log_2 | v''n| \rfloor} + 2(\lfloor \log_2 | v''_n | \rfloor)) \neq v_n$, then $LM3, LM4,$ and $LM5$ takes the value of 1.

To distinguish expandable block categories, $LM1 = 1$ and $LM2 = 0$ are further assigned to the blocks which are non-RDE expandable. Non-RDE expandable block means that only those values which are between -1 and 1 are directly utilized without being reduced. Furthermore, $LM1 = 0$ is for changeable blocks. If the differences (v_0, v_1 and v_2) are odd, then the location map $LM3$, $LM4$ and $LM5$ are set to 1 while if the difference values are even, then 0 is assigned to the location map $LM3$, $LM4$ and $LM5$.

Finally, after hiding the needed data, the embedding process terminates and then, the stego image and the location have to be kept separately. That is, they are not concatenated together since doing so may result in decreasing the quality of the stego image. Note that at this stage the concealment process is done, the stego image and the location map can be sent to the intended recipient through the public network. The process for performing embedding

and setting up the location map can be viewed from Fig 3.5 and Fig 3.6. In addition, as this method is having two main stages, the next section discusses the extraction process.

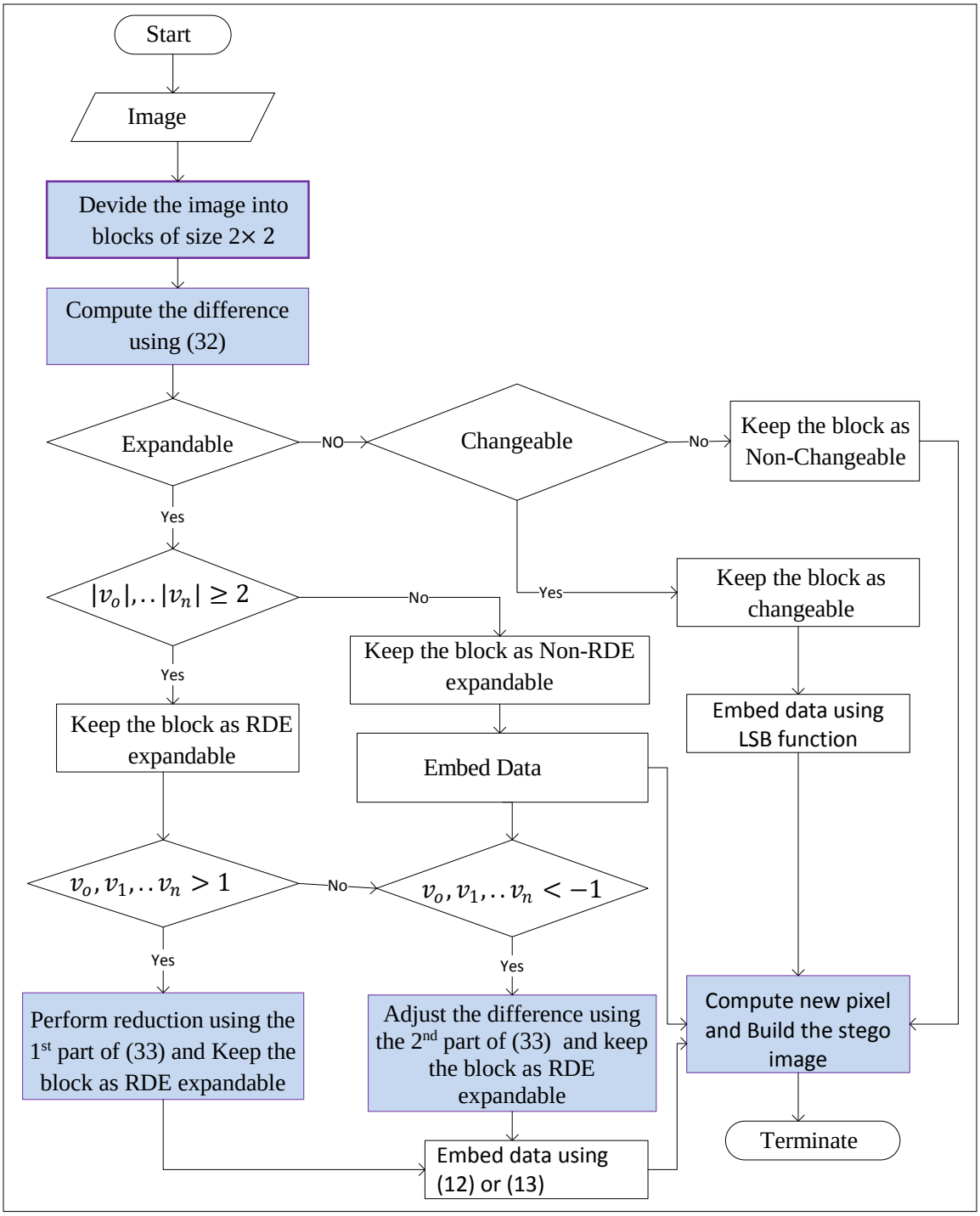

Figure 3.5 Steps for Concealing Data

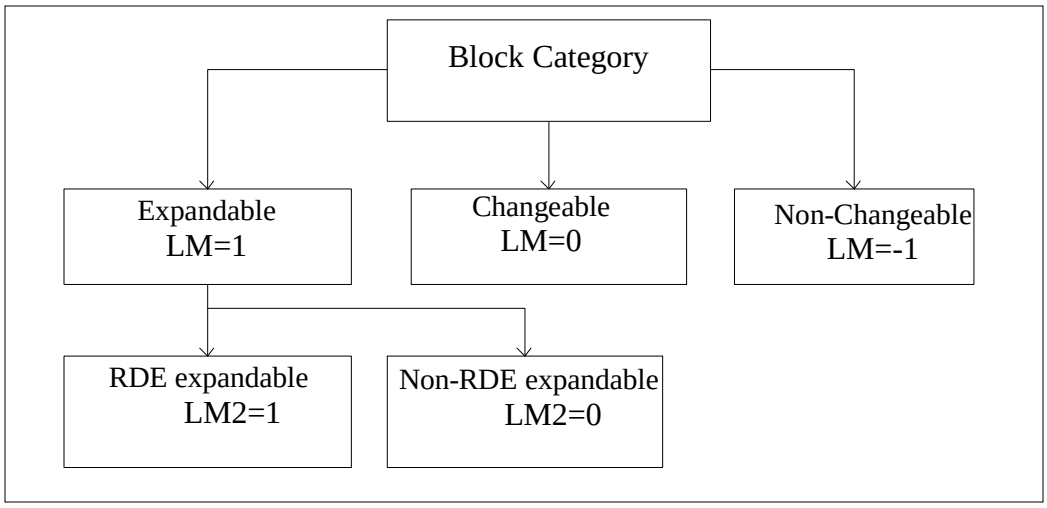

Figure 3.6 Defined Location Map

3.2.2 Phase 2: Extraction Process and Recovery

The extraction process is the reverse of embedding process. It is performed in order to obtain the hidden secret message, reduced difference and then to reconstruct the original cover media. Thus, the following steps are performed throughout this process.

Step1: The extraction phase begins by first segmenting the stego image into blocks, each having four pixels, after that the difference between pixel pairs is computed using (32). That is, $v''_n = (v'_0,\ v'_1,\ v'_2)$ are computed in each block, thereafter the location map is utilized to get the secret message and the value of the original reduced difference. Perform the extraction of expandable RDE if only the location maps $LM1 = 1$ and $LM2 = 1$. Process non-RDE expandable if $LM1 = 1$ and $LM2 = 0$. Moreover, if $LM1 = 0$, the changeable blocks can be accessed. To be able to process non-changeable blocks, the defined location map $LM1$= -1 is used.

Step2: Recovering the original difference and the secret bits for RDE expandable blocks is carried out as follows. To get the secret bits the LSB is extracted from v''_n, after that v''_n has to be right shifted in order to get the original difference v_n which is recovered using the expressions presented below.

First, if $v''_n > 1$ and $LM3, LM4, LM5 = 0$, (35) is used to get the original difference v_n.

$$v_n = v''_n + (2^{(\lfloor \log_2 v''_n \rfloor)-1} + 2(\lfloor \log_2 v''_n \rfloor) - 1) \quad (35)$$

Second, if $v''_n > 1$ and $LM3, LM4, LM5 = 1$, then (36) is utilized to get v_n.

$$v_n = v''_n - (2^{(\lfloor \log_2 v''n \rfloor)-1} + 2(\lfloor \log_2 | v''_n | \rfloor) - 1) \quad (36)$$

Third, if $v''n$ <-1 and $LM3, LM4, LM5 = 1$, use (37) to obtain v_n and then compute the new pixel using (38), where $v_n = (v_o, v_1, v_2, v_3)$.

$$v_n = v''_n - (2^{\lfloor \log_2 | v''_n | \rfloor} + 2(\lfloor \log_2 | v''_n | \rfloor)) \quad (37)$$

$$\begin{cases} u_0 = v_0 + u_3 \\ u_1 = v_1 + u_3 \\ u_2 = v_2 + u_3 \\ u_3 = u_3 \end{cases} \quad (38)$$

Fourth, if $v''_n < -1$ and $LM3, LM4, LM5 = 0$, utilize (39) to get v_n and calculate the new pixel using

$$v_n = v''_n + (2^{\lfloor \log_2 | v''_n | \rfloor} + 2(\lfloor \log_2 | v''_n | \rfloor)) \quad (39)$$

To process non-RDE expandable blocks, the secret message (b) is obtained by taking LSB of v''_n (40) and the expression defined in (41) is used to get v_n.

$$b = v''_n \, mod \, 2 \quad (40)$$

$$v_n = \left\lfloor \frac{v''_n}{2} \right\rfloor \quad (41)$$

The secret bits are extracted from changeable blocks by taking the LSB of v''_n using modulus function (mod 2 of v''_n) Thereafter the original difference v_n is computed as follows.

a. If the location map $LM3, LM4, LM5 = 0$ and the difference v''_n is odd, the extraction is carried out using (42).

$$v_n = 2 \times \left\lfloor \frac{v''_n}{2} \right\rfloor - 1 \quad (42)$$

b. If the location map $LM3, LM4, \ LM5 = 1$ and the difference v''_n is even, (43) is used to recover v_n.

$$v_n = 2 \times \left\lfloor \frac{v''_n}{2} \right\rfloor + 1 \quad (43)$$

Note that the expressions in (42) and (43) are similar to the ones presented in (Ali AL_Huti et al. 2015). Furthermore, in (a) if the location map $LM3, LM4, LM5 = 0$, the difference cannot be even and this is similar to (b), if $LM3, LM4, \ LM5 = 1$, the difference cannot be odd and the

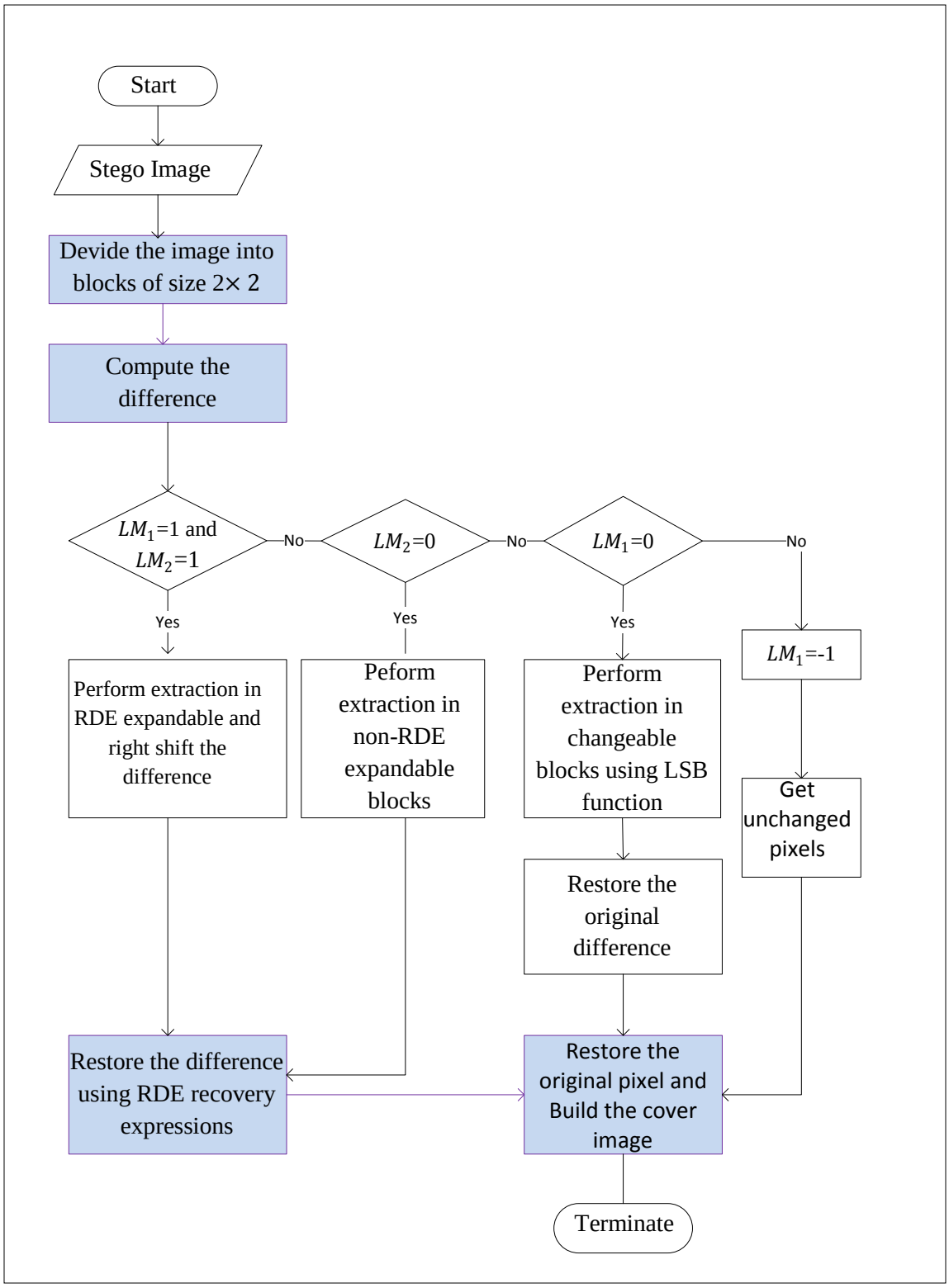

Figure 3.7. Steps for Performing Extraction

Table 3.2 Difference Between the Proposed and the Previous Method

Stage	**Previous method, (Ali AL_Huti et al., 2015)**	**Proposed method**
Computing difference between pixel pairs	$\begin{cases} v_0 = 0 \\ v_1 = u_1 - u_0 \\ v_2 = u_2 - u_1 \\ v_3 = u_3 - u_2 \end{cases}$	$\begin{cases} v_0 = u_0 - u_3 \\ v_1 = u_1 - u_3 \\ v_2 = u_2 - u_3 \\ v_3 = 0 \end{cases}$
Reduction function for computing	$v''_n = \begin{cases} v_n - (2^{\lfloor \log_2 v_n \rfloor} + \lfloor \log_2 v_n \rfloor)\ if\ v_n > 1 \\ v_n + (2^{\lfloor \log_2 v_n \rfloor} + \lfloor \log_2 v_n \rfloor)\ if\ v_n < -1 \end{cases}$	$v''_n = \begin{cases} v_n - (2^{\lfloor \log_2 v_n \rfloor} + 2(\lfloor \log_2 v_n \rfloor)) & if\ v_n > 1 \\ v_n + (2^{\lfloor \log_2 \lvert v_n \rvert \rfloor} + 2(\lfloor \log_2 \lvert v_n \rvert \rfloor))\ if\ v_n < -1 \end{cases}$
Base point pixel	u_0	u_4 (constant for each pixel block)
Block of Pixel	$4\ by\ 4\ \rightarrow 4 \times 4$	$2\ by\ 2\ \rightarrow 2 \times 2$
Computing new pixel	$\begin{cases} u'_0 = u_0 \\ u'_1 = v'_1 + u'_0 \\ u'_2 = v'_2 + u'_1 \\ u'_3 = u_3 + u'_2 \end{cases}$	$\begin{cases} u'_0 = v'_0 + u_3 \\ u'_1 = +v'_1 + u_3 \\ u'_2 = +v'_2 + u_3 \\ u_3 = u_3 \end{cases}$

reason is that these location maps are defined during the embedding process to keep track of information about any operations done in changeable blocks. Generally, the difference between the previous method and the proposed one is provided in Table 3.2 and the entire process demonstrating the data extraction is illustrated in Fig 3.7. Note that the highlighted squares in both figures (Fig 3.5 and Fig 3.7) indicate the parts of the previous method (Ali AL_Huti et al., 2015) that are enhanced in this research.

3.3 Implementing the Proposed Algorithm

To Implement the proposed method MATLAB is employed. As it does provide many features such as manipulating matrix, image processing toolbox, function and data plotting, implementing algorithms, etc., it is chosen to be used for implementation. Furthermore, During the experiment, the well-known public standard grayscale images of size 512 by 512 (512×512) obtained from (Califonia, 2017) and (Microbes Digital Library, 2017) are used to evaluate the performance of the proposed approach.

3.4 Research Time Frame

This section provides details for the duration of this research. The schedule is presented for 6 months, starting from June 2017 until December 2017. The detailed explanation of all tasks accomplished is presented in Table 3.3.

Table 3.3 Activity Scheduling

Activity	**1st Month**				**2nd Month**				**3rd and 4th Month**				**5th and 6th Month**			
Literature Study																
Algorithm Design																
Implementation																
Testing and Validation																
Results Analysis																
Writing, Presenting and Submitting Final Report																

CHAPTER 4
EXPERIMENTAL RESULTS AND DISCUSSION

The experimental results obtained using the proposed approach are presented in this chapter. Besides, different metrics such as embedding capacity and peak signal-to-noise ratio (PNSR) are measured thereafter the discussion on the results is presented. Furthermore, the comparison between this approach and the existing one is also made so as to evaluate its performance. The results are presented in tables and for the sake of clarifying and understanding the research findings, different figures and images are also provided. The main goal of the experiment was to measure and evaluate the distortion level of the stego image with respect to the number of secret bits that are concealed in the cover image. The overall results shows that that the proposed method performs well over the previous one (Ali AL_Huti et al., 2015) where good PSNR and good payload capacity are achieved.

4.1 Testing Environment

The proposed algorithm was developed and tested on a laptop computer having the following specifications. 64-bit Windows 8.1 Professional, Intel (R) Core (TM) i3-4005U CPU@ 1.70 GHz and 4.00 RAM with no pen or touch input display.

4.2 Evaluating the Performance of the Proposed Approach

Various well-known standard grayscale images of size 512 by 512 (512×512) taken from (Califonia, 2017) and (Microbes Digital Library, 2017) are utilized to evaluate the performance of the proposed method on the given size of the secret data. All of these images are freely available to be used and during the experiment, different scenarios are considered, i.e., different images and secret message sizes are used during the experiment. The PSNR and embedding capacity are measured to analyze and evaluate how the stego image degrades with respect to the original cover image.

If the PSNR value is high, the quality of the stego image is better. That is, the cover image is not drastically distorted. The PSNR is computed using the equations provided in (30) and (31). Furthermore, histograms for both original images and their respective stego images are generated to see the variation that occurs in the statistical properties of the original cover images. Fig 4.1 depicts all grayscale images where five genal (non-medical) images and five medical images are used for evaluation.

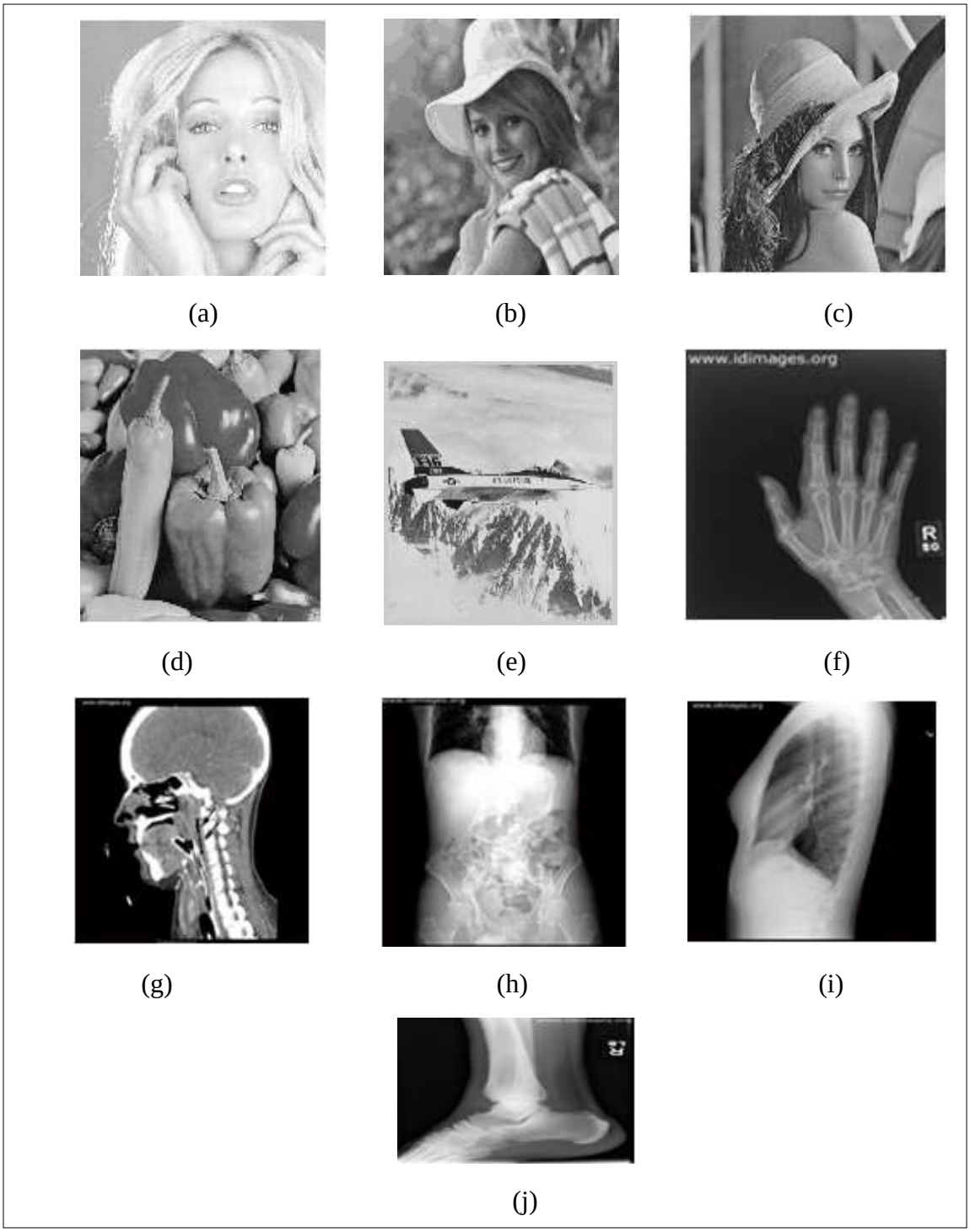

Figure 4.1 Cover Images (a) Tiffany (Girl).tiff (b) Elaine.tiff (c) Lena.tiff (d) Pepper.tiff (e) Aeroplane.tiff (f) Hand medical image.tiff (g) Head medical image.tiff (h) Lung medical image.tiff (i) Abdominal medical image.tiff (j) Leg medical image.tiff

4.3 Results and Discussion

The detailed illustrations and explanations on the experimental results is presented in this section. In addition, as early mentioned different scenarios are considered in order to analyze the changes that occurs in the original pixel values after concelealing the secret data. A binary bit stream of the secret data whose size depends upon the needed payload capacity to be embedded in the image is randomly generated using a function available in MATLAB. During the experiment, five different sizes of the secret message (with $size_1 = 16569$ bits, $size_2 = 37629$ bits, $size_3 = 90000$ bits, $size_4 = 147762$ bits and the last one $(size_5)$ having 196508 bits) are first randomly generated, thereafter they get stored into five different text files to make sure that the same secret message is utilized for all images throughout the experiment.

From the experimental results shown in Table 4.1 and Table 4.2, it is found that with the proposed method, a good PSNR is achieved. That is, by considering the quality, the proposed method outdoes the one implemented by (Ali AL_Huti et al., 2015). Furthermore, since the proposed method has improved the previous reduced difference expansion (RDE), it is ideal to visualize it by plotting the results from Table 3.1, (see Fig 4.2) which shows that by utilizing the proposed RDE-scheme small difference values are obtained which results in a good payload capacity as well as good quality of the stego image. Moreover, it is also important to note that the pixel block and the suggested constant base point for each block have also greatly influenced the quality of stego image. Different figures (Figs 4.3 – 4.8) are provided for results visualization. Additionally, to observe the changes made in the cover images after

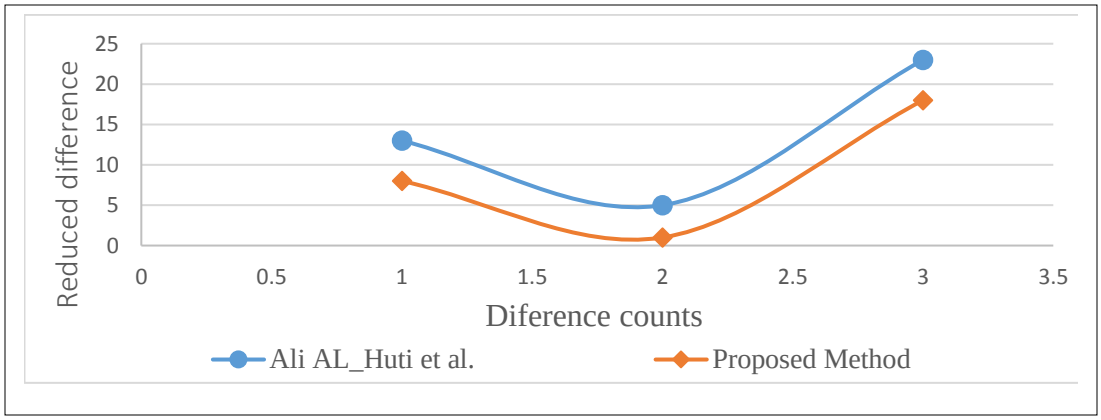

Figure 4.2 Variation of the reduced difference using the proposed method and the one implemented by Al_Huti et al.

Table 4.1 Comparison Between the Method of Al_Huti et al. and the Proposed one Using General (Non-medical) Grayscale Cover Images.

Images	**Al_Huti et al.'s method**		**Proposed method**	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Girl (Tiffany)	16569	41.84	16569	42.54
	37629	36.80	37629	37.77
	90000	32.35	90000	33.54
	147762	30.41	147762	31.63
	196508	27.16	196508	30.25
Aeroplane	16569	41.06	16569	41.59
	37629	38.69	37629	39.09
	90000	31.23	90000	32.16
	147762	27.45	147762	28.65
	196508	25.89	196508	27.36
Lena	16569	46.58	16569	48.27
	37629	40.33	37629	42.03
	90000	33.15	90000	34.96
	147762	29.60	147762	31.47
	196508	28.30	196508	29.98
Pepper	16569	33.88	16569	34.55
	37629	32.74	37629	32.79
	90000	29.66	90000	30.04
	147762	28.14	147762	28.82
	196508	27.00	196508	27.72
Elaine	16569	41.11	16569	42.16
	37629	37.30	37629	38.54
	90000	32.16	90000	33.57
	147762	29.89	147762	31.22
	196508	28.69	196508	29.99

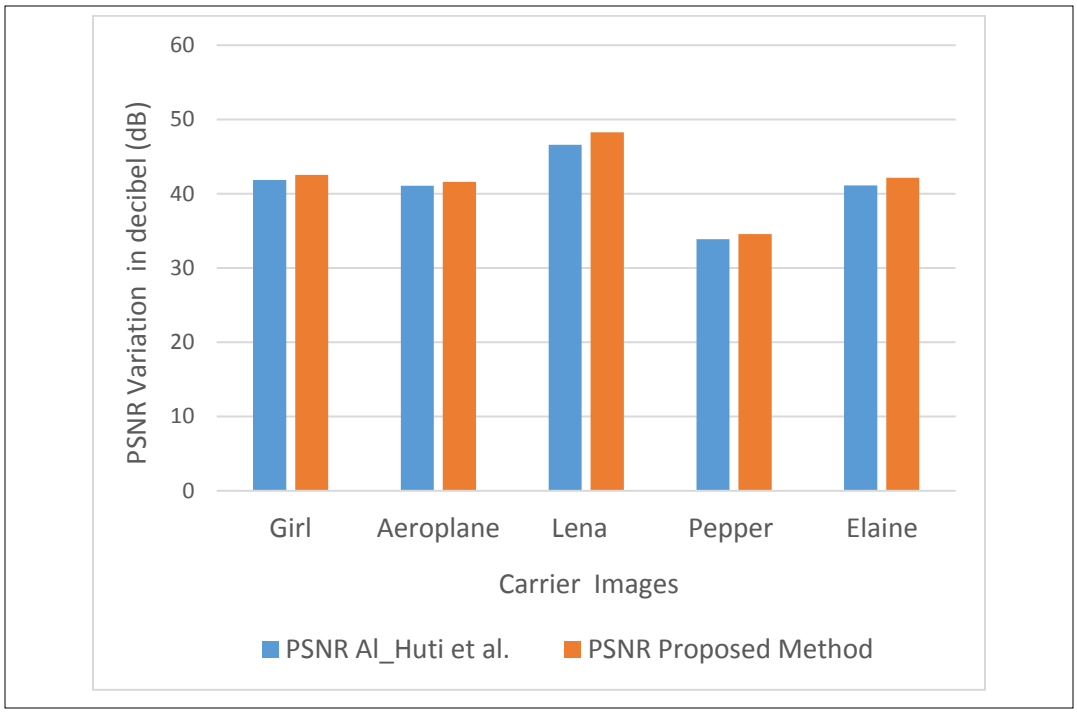

Figure 4.3 PSNR variation after hiding 16569 bits in non-medical images

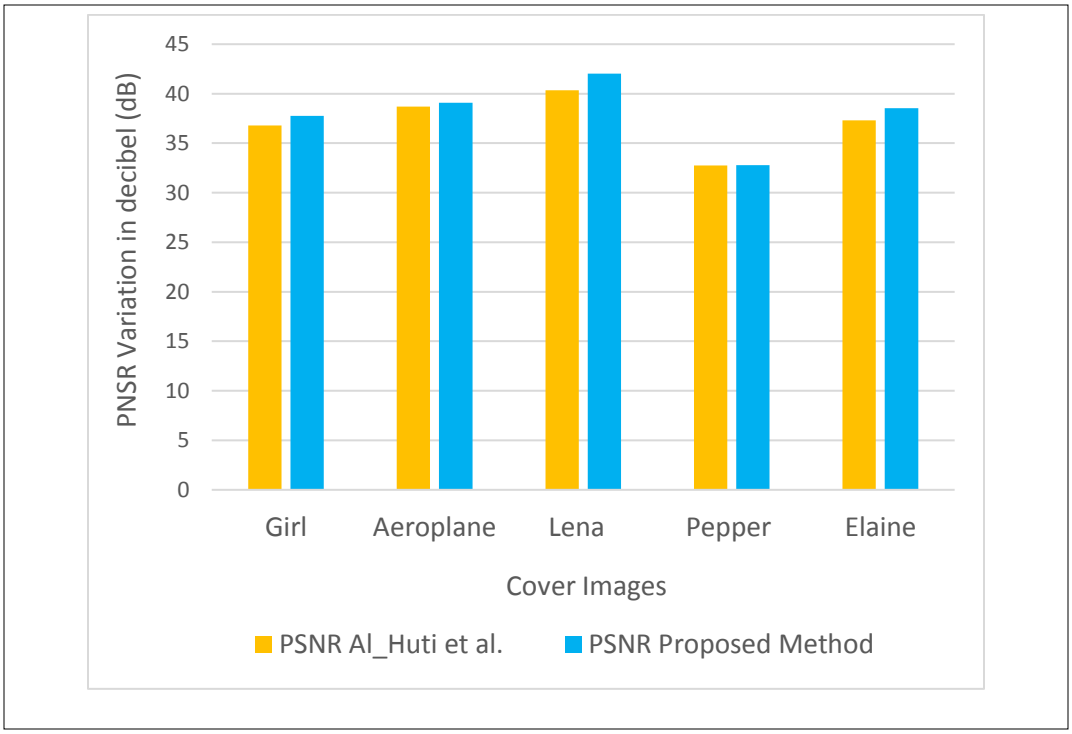

Figure 4.4 PSNR variation after hiding 37629 bits in non-medical images

Table 4.2 Comparison between the Method of Al_Huti et al. and the Proposed Method Using Medical Grayscale Cover Images.

Images	**Al_Huti et al.'s method**		**Proposed method**	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Lung	16569	46.33	16569	46.92
	37629	44.47	37629	45.02
	90000	41.96	90000	44.03
	147762	40.48	147762	41.31
	196508	38.41	196508	39.14
Hand	16569	42.00	16569	43.46
	37629	41.95	37629	43.33
	90000	40.76	90000	41.89
	147762	38.03	147762	38.94
	196508	37.61	196508	38.55
Abdominal	16569	43.95	16569	44.62
	37629	42.38	37629	42.99
	90000	40.78	90000	41.26
	147762	38.03	147762	39.96
	196508	37.81	196508	38.39
Head	16569	42.45	16569	42.77
	37629	40.45	37629	40.81
	90000	35.43	90000	36.71
	147762	32.57	147762	33.89
	196508	31.63	196508	32.86
Leg	16569	47.21	16569	48.37
	37629	43.84	37629	44.84
	90000	40.43	90000	41.24
	147762	39.59	147762	40.26
	196508	38.21	196508	38.79

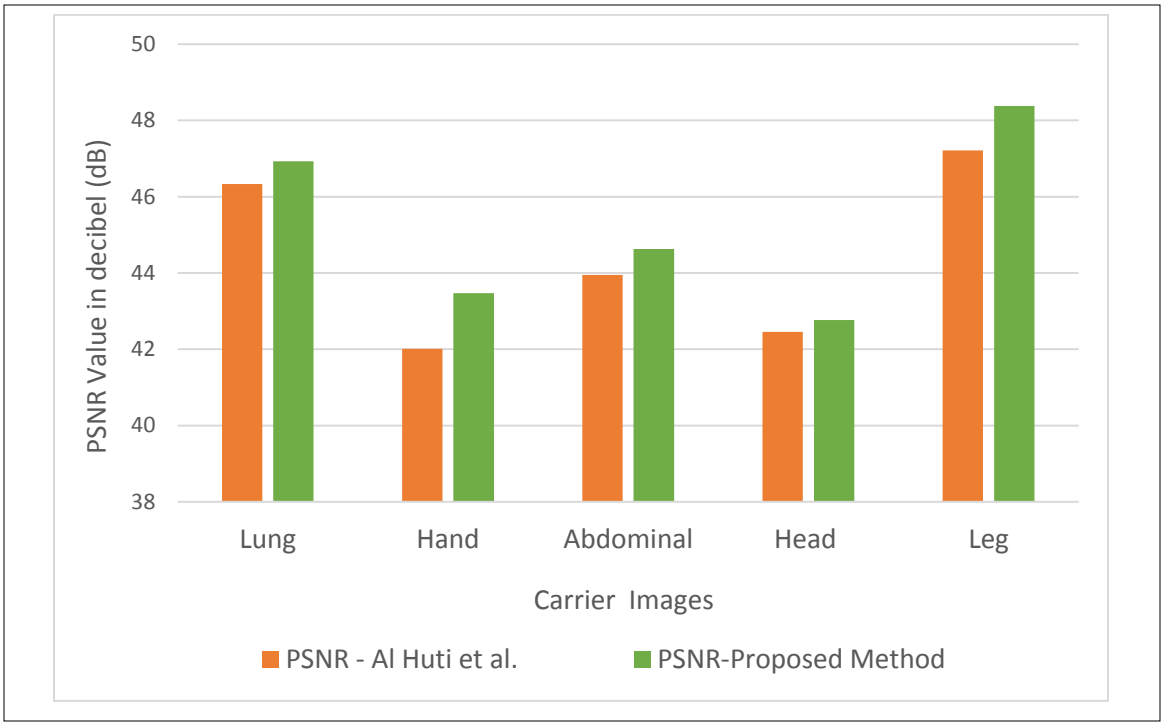

Figure 4.5 Variation of PSNR after hiding 16569 bits in medical cover images

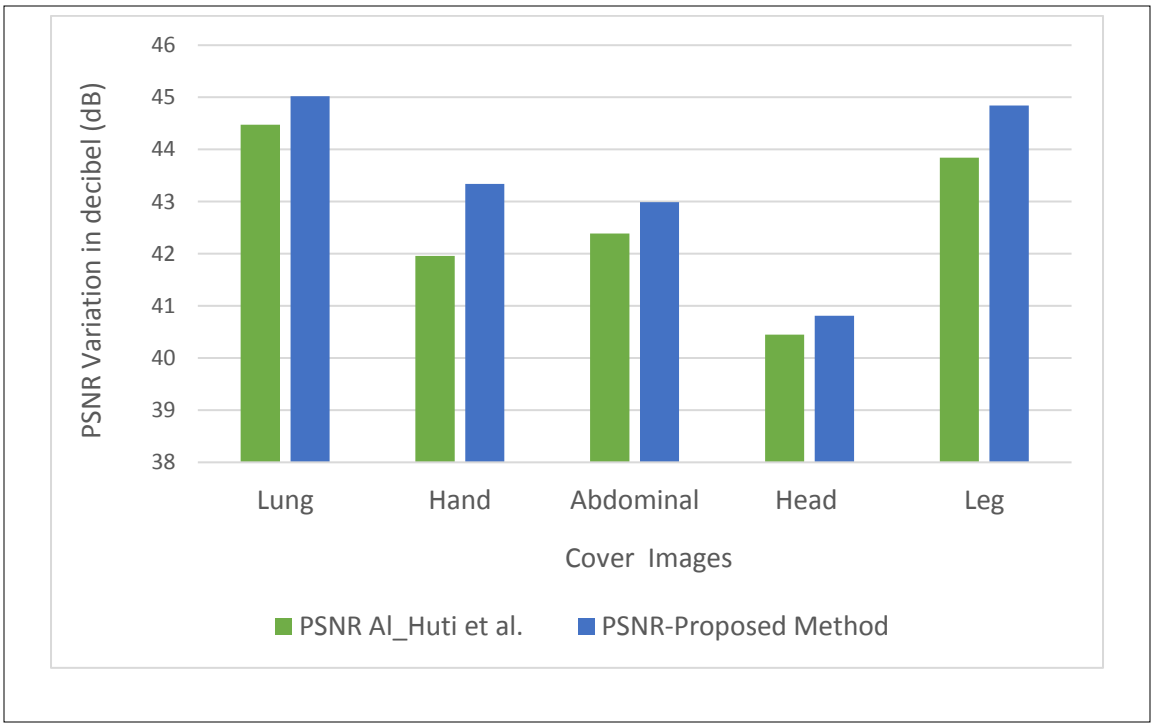

Figure 4.6 Variation of PSNR after hiding 37629 bits in medical cover images

embedding the secret data, Fig 4.9 depicts Elaine cover image, Hand original medical image, Lena cover image and their respective stego images obtained after concealing 16569 bits of secret data while Fig 4.12 depicts the example of the cover and stego image histograms. In addition, from the experimental results, it could be seen that after concealing five different sizes of the secret message into all cover images, good PSNR is achieved and this results in a good visual quality of the stego image, i.e., based on the overall results, it could be inferred that the proposed method has greatly enhanced the previous one (Ali AL_Huti et al., 2015) and this enhancement allows high quality application for data hiding. Nevertheless, as mentioned above (in Table 4.1 and Table 4.2), the value of PSRN goes down after hiding more secret bits in the cover image. That is, after concealing 196508 bits, the PSNR value slightly decreases. The highest PSNR (48.03 dB, see Table 4.2) is obtained after concealing 16569 bits in Leg medical image while the lowest PSNR is obtained from Aeroplane image (27.36 dB, see Table 4.1) after hiding 196508 bits.

For Leg medical image, the idea is that values obtained after computing the difference between pixel pairs were further reduced to the possible smallest values which results in a good PSNR. For Aeroplane image, it means that although the difference values were further reduced using the proposed RDE, the values generated after the reduction process are still large compared to the ones from Leg. Moreover, if there is a high disparity between the neighboring pixels in each block, it results in large difference values which may reduce the quality. Considering all sizes of the secret message, the PSNR from some images tends to be close to each other which implies that the difference values obtained after reduction are almost in the same range. Nonetheless, as the trade-off, there is always a slight change in the quality of stego image whenever the payload capacity is increased or decreased.

As a result, this proposed method can be highly preferable to individuals willing to conceal low or medium payload capacity with low perceptibility and high security level. The reason is that it will be difficult to suspect the existence of the secret data in the stego image while being transmitted to the intended recipients via the internet. Moreover, this will also increase the level of confidentiality, integrity and privacy between the communicating parties or individuals. The results' visualization about the performance of Ali_Huti et al.'s scheme and the proposed one are presented in Figs. 4.3 - 4.12. From Fig. 4.3 and Fig 4.4, we could see

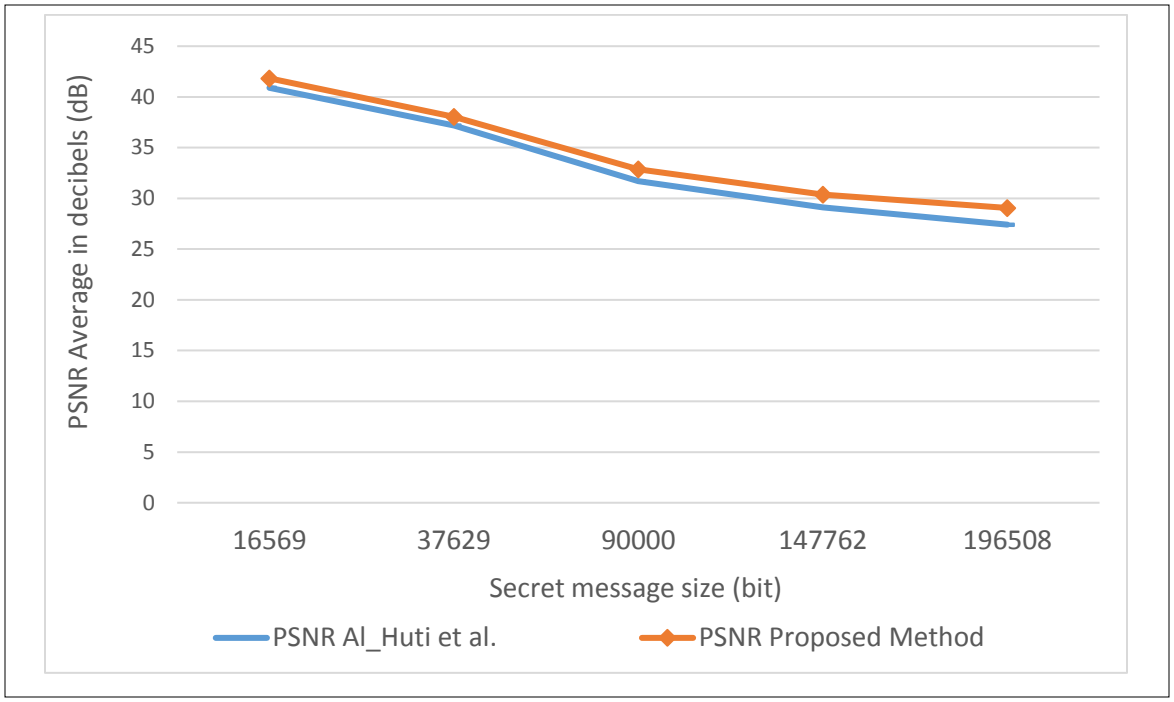

Figure 4.7 The overall PSNR average for all general cover images with respect to each secret

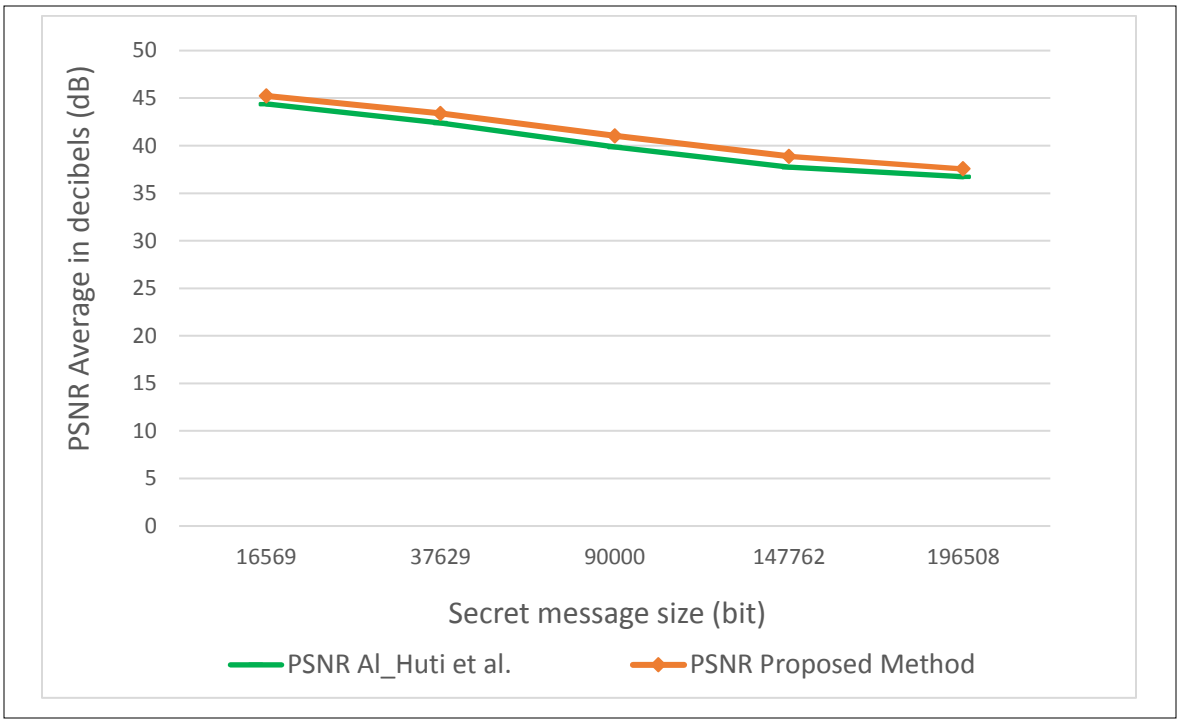

Figure 4.8 The overall PSNR average for all medical cover images with respect to each secret message size

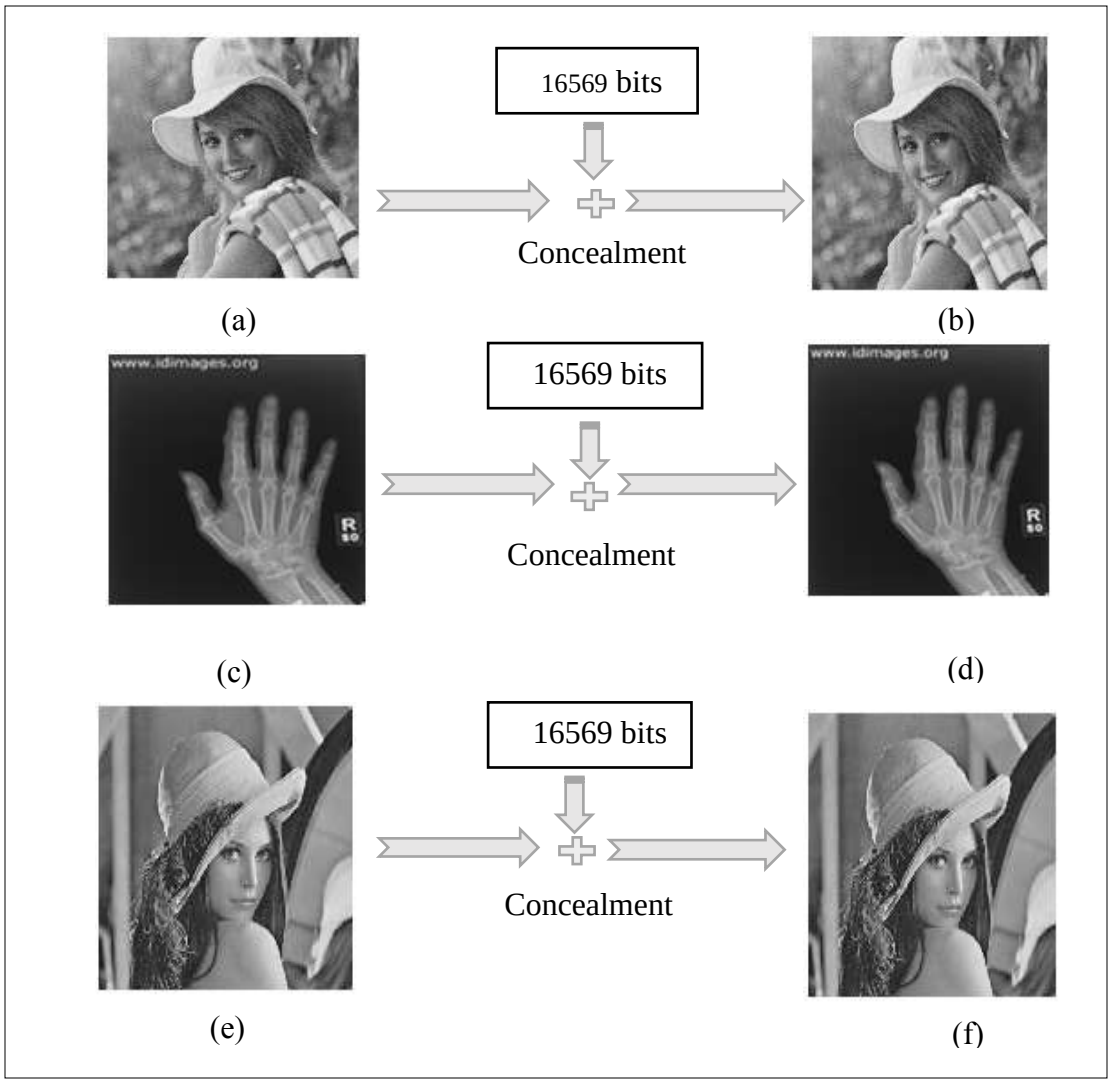

Figure 4.9 "An example of cover images (a) Elaine cover image.tiff before hiding data with Im_Pix_Avg = 136.3565 (b) Elaine stego image.tiff after hiding 16569 bits with Im_Pix_Avg = 136.5613 and PSNR = 42.16 dB (c) Hand medical cover image before hiding data with Im_Pix_Avg = 62.6073(d) Hand medical stego image after hiding 16569 with Im_Pix_Avg = 62.7510 and PSNR = 43.46 dB (e) Lena cover image before hiding data with Im_Pix_Avg = 124.0425 (f) Lena stego image after hiding 16569 bits with Im_Pix_Avg = 124.1560 and PSNR = 48.27 dB obtained using the proposed method".

that after concealing both sizes, the proposed method achieves good results over Ali Al_Huti et al.'s scheme in terms of the visual quality of the stego image. Moreover, Figs. 4.5 and 4.6 show that for all secret message sizes, the proposed method is still achieving good PSNR

compared to the previous one. Fig 4.7 and Fig. 4.8 depict the overall PSNR averages with respect to each secret message size for all types of the cover images. The PSNR average is computed based on five secret message sizes which are used to evaluate the distortion level (changes) encountered in the cover image after concealing each secret message size. E.g., for Girl (also called Tiffany), Aeroplane, Lena, Pepper and Elaine cover images, the PSNR average (in this case 41.829 dB) after hiding the first secret message size (16569 bits) is obtained by computing the average of five PSNR values (PSNR from each cover image, i.e., PSNR_Girl= 46.92 dB, PSNR_Aeroplane = 41.59 dB, PSNR_Lena = 48.27 dB, PSNR_Pepper = 34.55 dB and PSNR_Elaine = 42.16 dB.

Regarding medical cover images the process is similar. Surprisingly, the overall good PSNR average is achieved in medical images. This is because these images are characterized by a high redundancy which allows data to be concealed without much distorting them. It is also worth to note that owing to the fact that the proposed reduced difference expansion scheme effectively reduces the difference values, it also keeps good quality of the stego image. More importantly, if we look at images in Fig 4.9 (a) and (b), (c) and (d), as well as (e) and (f), they are almost similar which makes the proposed method to be highly judged invisible, i.e., it is really difficult to identify the difference between them (the original cover images and their

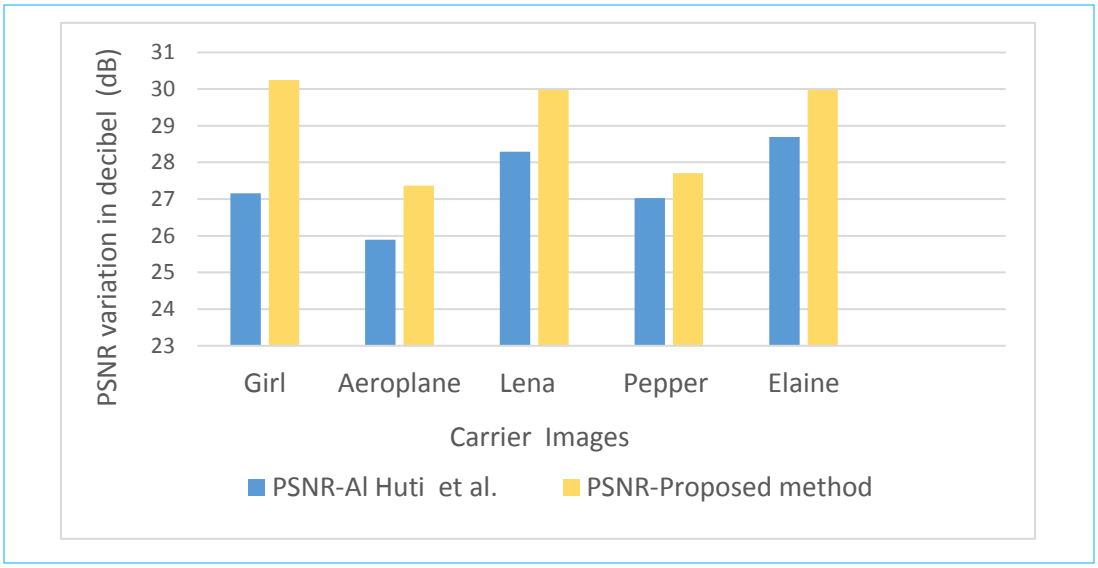

Figure 4.10 Variation of PSNR after concealing 196508 bits in non-medical (general) cover images

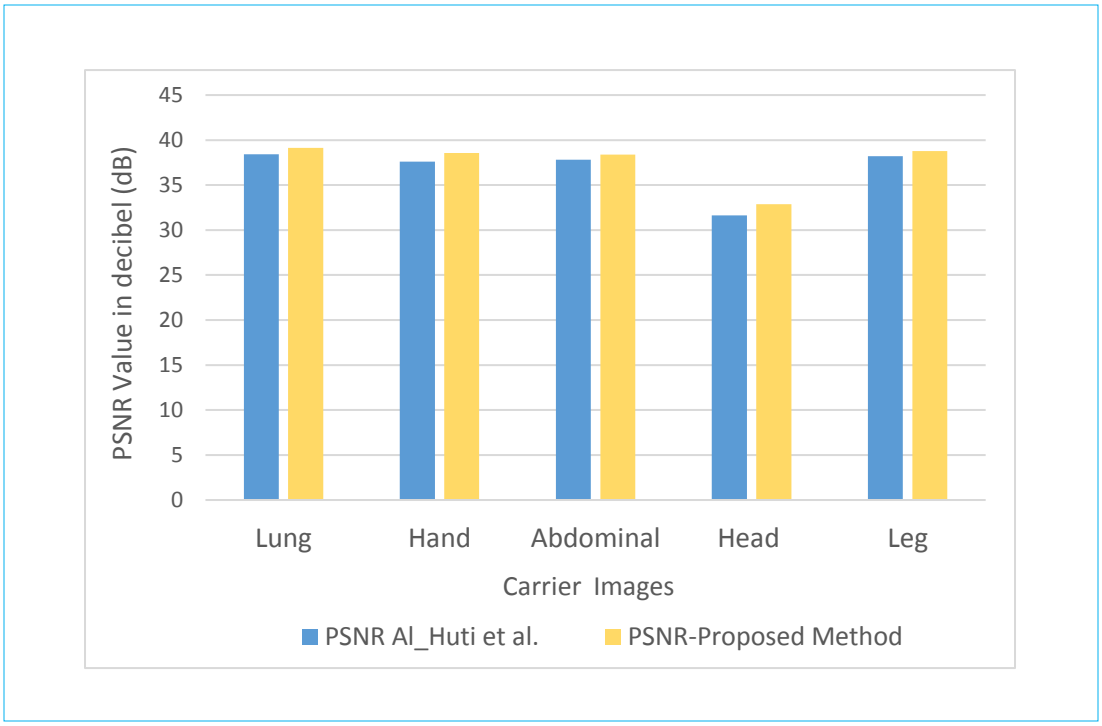

Figure 4.11 Variation of PSNR after concealing 196508 bits in medical cover images

corresponding stego images), which means that there is a high similarity between the stego image and the original cover image. Such degree of similarity can also be revealed by the image pixel values' average (Im_Pix_Avg). For example, the Im_Pix_Avg (136.3565) for Elaine cover image and the one for Elaine stego image (136.5613) as provided in Fig 4.9, they are very close to each other with the only difference of 0.2048 which is actually acceptable.

The PSNR reduction is slightly noticed after concealing 196508 bits in all images, which implies that the distortion level or the degree of similarity between the cover and the stego image is proportional to the embedding capacity (this can be viewed in Fig 4.10 and 4.11). To wrap up the results analysis, Fig 4.12 is provided to illustrate the example of the cover image histogram before and after embedding secret data. The concept of using histogram to visualize the changes made in the image was discussed in the second chapter, i.e., previous research have shown that significant changes in the cover image's histogram can lead to the stego image suspicions which can results in intercepting or interfering the hidden data (Fridrich et al., 2003). Hence, drastic changes in the histogram of the stego image are always undesirable

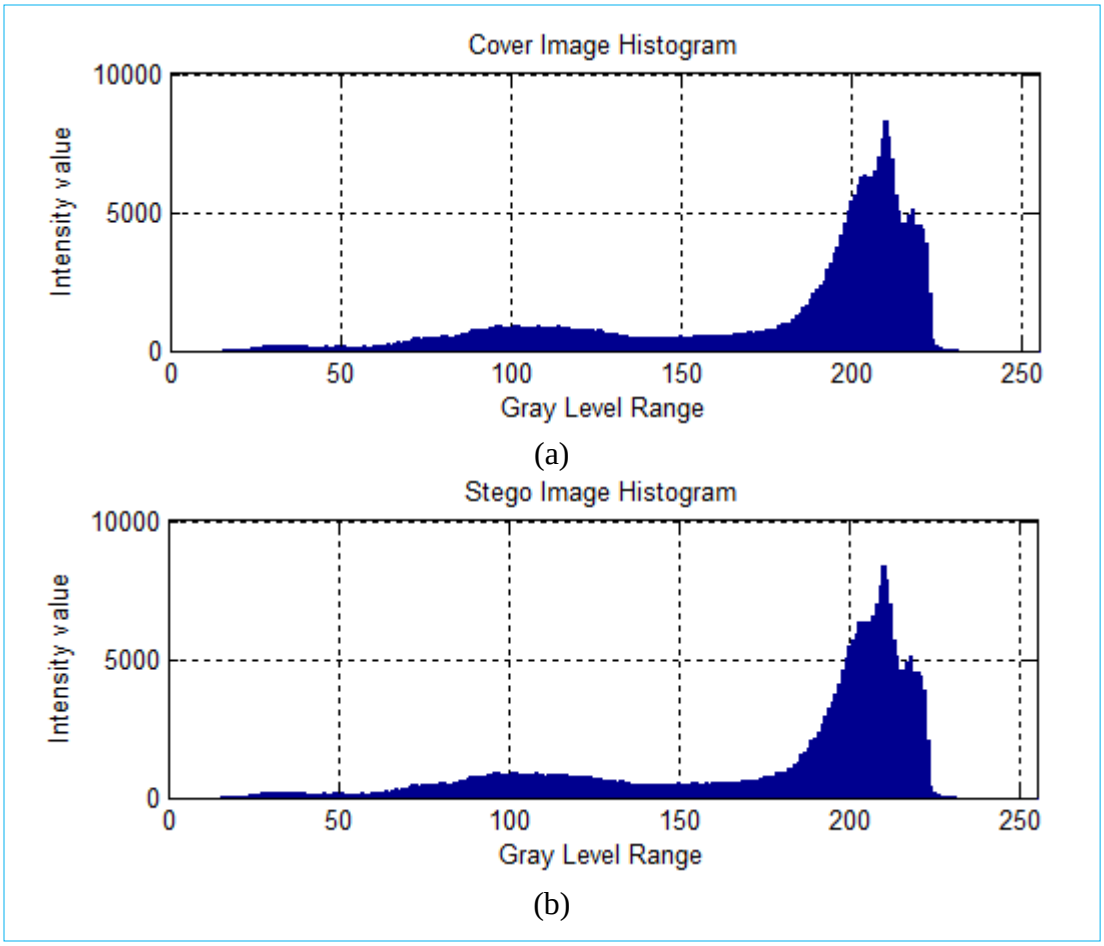

Figure 4.12 (a) Elaine cover image histogram before hiding data with image pixel average = 179.1789 (b) Elaine stego image histogram after hiding 16569 bits, with the image pixels' average = 179.3488 and PSNR = 42.12 dB.

while concealing data in any media. From Fig 4.12 where 4.12 (a) and (b) depict both histograms of Elaine cover image.tiff before and after concealing 16569 bits. If we look at both image histograms in (a) and (b) they are almost similar which reveals their high degree of resemblance. Moreover, considering the pixels' average for both images (cover image pixels' average =179.1789 and stego image pixels' average =179.3488), they tend to be close to each other which also proves their similarities. Generally, the proposed approach can be suitable for all users depending on the embedding capacity to be concealed.

[This page intentionally left blank]

CHAPTER 5
SUMMARY, CONCLUSION AND FUTURE WORK

This chapter wraps up the work carried out in this thesis by presenting a summary of this study, conclusion as well as suggesting the future work to enhance the proposed method. That is, the purpose and contributions of this work couple with their effects on the research findings are summarized thereafter a clear discussion in direction to improve this work is also provided.

5.1 Summary of the Study

Providing better solution to the main problem of maintaining a good visual quality of the stego image and a good embedding capacity which is encountered in the previous data hiding methods was one of the main concerns throughout this study. These two factors have to be taken into considerations while designing digital image data hiding methods since they may lead to the suspicion and interception of the hidden data as well as communication disclosure in case they are not well maintained.

Hence, a new data hiding method that allows confidential data to be concealed in digital grayscale images while preserving and maintaining the aforementioned factors was introduced in this work. The proposed method was developed based on the reduced difference expansion scheme and constant base point for each pixel's block. Correspondingly, to demonstrate the need for this research, a clear study background on the existing data hiding methods was presented in chapter one. Moreover, the literature study providing the current trends on digital image data hiding methods coupled with evaluation metrics was reviewed in the second chapter.

The Methodology detailing the design and functionality of the prosed method was elucidated in the third chapter while the experimental results and discussion were presented in chapter four. Finally, this chapter wraps up the work presented in this dissertation by drawing conclusion on the overall research findings with respect to the research questions which are considered as key motivations for this work.

5.2 Conclusion

The conclusion on the research findings presented in this work is drawn on number of points with reference to the main research questions mentioned in the first chapter.

1. To respond to the first research question, "How a good visual quality of the stego image can be preserved after concealing the secret data? ", the suggested based point was used to compute the difference between pixel pairs in each pixel's block thereafter the proposed reduced difference expansion scheme was applied to reduce the difference values which allows data to be concealed into small values. Note that the base point also reduces the number of pixels which can be out of the gray level range while computing the new pixel to be used for building the stego image. That is, the problem of underflow and overflow is well maintained since two pixels are not added up in order to get the new pixel.

The evaluation parameters (peak signal -to-noise ratio and the embedding capacity) were measured to evaluate the performance. The experimental results obtained (refer to Table 4.1 and Table 4.2) using both categories of the cover images (non-medical images and medical images) show that the visual quality of the stego images was greatly improved. However, different PSNR values were achieved using the same size of the secret data for all images. This implies that apart from the suggested techniques (RDE-scheme, constant base point, and pixel's block), there are other characteristics such as the nature of the image itself (edges, disparity on the pixel values distribution, and high degree of redundancy) which can also influence the results. If there is a high disparity between the neighboring pixels, it results in large difference values which may reduce the quality for certain images.

The highest PSNR was achieved while hiding data in medical images due to their well-known characteristic of having several large smooth areas (also known as high degree of redundancy) which permits data to be concealed without being greatly degraded. However, with the other category of the cover image (non-medical images), good stego image quality is also achieved even though the PSNR values are less than the ones from certain medical images, i.e., considering the quality, the proposed RDE-based method provides better quality of the stego image.

2. The second research question regarding "How the number of secret bits to be concealed in a grayscale digital image can be increased without drastically deforming it?'' was addressed as follows. The size of the pixel's block which allows data to be concealed in the cover image was suggested. It allows 3 bits of the of secret data to be concealed in each pixel's block based on the defined criteria which control the embedding process (further details were given in the

third chapter). More importantly, the proposed RDE-scheme has also contributed to the amelioration of the embedding capacity by increasing the number of embeddable pixel pairs. That is, by concealing secret data into small difference values, new pixel values are kept between 0 and 255 (gray level range) which is ideal since only few pixels are ignored while concealing data, (those are under floor and over floor pixels since they can lead to unrecoverable data).

Additionally, different sizes of the secret message were used throughout the evaluation which can help users to easily determine or choose the appropriate secret data size to be concealed based on how the quality of the stego image is preserved. Accordingly, it can be concluded that the new proposed RDE-scheme and the pixel's block achieve a reasonable embedding capacity which proves the effectiveness of the new data hiding method presented in this work.

5.3 Limitations and Future Work

The application of the proposed RDE-based scheme and constant based point in grayscale digital image data hiding approach has played a significant role in improving and maintaining the quality of the stego image, and the embedding capacity. However, further considerations to improve this work are still highly welcomed due to the limitations identified in its performance. In this way, below we present a point by point on the limitations encountered on this work which can be taken as motivations for future research. As elucidated in the experimental results discussion, increasing the embedding capacity results in slightly decreasing the PSNR value (quality of the stego) which is always undesirable. Therein, further evaluations on the variation of embedding capacity with respect to the PSNR value are still needed.

1. In the future work, it is expected that the quality of the stego image can be improved by varying the reduced difference expansion scheme.
2. The embedding capacity variation can be evaluated using dual imaging technique combined with the reduced difference expansion scheme.

[This page intentionally left blank]

REFERENCES

Agrawal, S. & Kumar, M., 2017. Optik Mean value based reversible data hiding in encrypted images. *Optik - International Journal for Light and Electron Optics*, 130, pp.922–934.

Ahmad, T. et al., 2013. An improved Quad and RDE-based medical data hiding method. In *International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM)*. pp. 141–145.

Alattar, A.M., Reversible watermark using difference expansion of quads. *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04).*, (1), pp.377–380.

Ali AL_Huti, M.H., Ahmad, T. & Djanali, S., 2015. Increasing the capacity of the secret data using DE pixels blocks and adjusted RDE-based on Grayscale Images. In *International Conference on Information, Communication Technology and System (ICTS)*. pp. 225–230.

Alvarez, P., 2004. Using extended file information (EXIF) file headers in digital evidence analysis. *International Journal of Digital Evidence*, 2(3), pp.1–5.

Anderson, R.J. & Petitcolas, F.A.P., 1998. On The Limits of Steganography. *IEEE Journal of Selected Areas in Communications*, 37(6), pp.380–3.

Anon, Califonia UUo, "SIPI Image Database," .[Online]-.available: Available at: http://sipi.usc.edu/database/database.php?volume=misc [Accessed March 22, 2017a].

Anon, Partners Infectious Disease Images - eMicrobes Digital Library - Home. Available at: http://www.idimages.org/ [Accessed March 12, 2017b].

Arham, A. et al., 2016. Combination Schemes Reversible Data Hiding for Medical Images. , pp.2–7.

Arham, A., Nugroho, H.A. & Adji, T.B., 2017. Multiple layer data hiding scheme based on difference expansion of quad. *Signal Processing*, 137, pp.52–62.

Cheddad, A. et al., 2010. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3), pp.727–752.

Datta, B., Mukherjee, U. & Kumar, S., 2016. LSB Layer Independent Robust Steganography using Binary Addition. *Procedia - Procedia Computer Science*, 85, pp.425–432.

El-sayed, H.S., El-Zoghdy, S.F. & Faragallah, O.S., 2016. Adaptive Difference Expansion-Based Reversible Data Hiding Scheme for Digital Images. *Arabian Journal for Science and Engineering*, 41(3), pp.1091–1107.

Fridrich, J., Goljan, M. & Hogea, D., 2003. New methodology for breaking steganographic techniques for JPEGs. *Proceedings of SPIE*, 5020, pp.143–155.

Han, D., Yang, J. & Summers, W., 2017. Inject Stenography into Cybersecurity Education. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops Inject*. pp. 50–55.

Han, S. et al., 2006. Lossless Data Hiding in the Spatial Domain for High Quality Images Lossless Data Hiding in the Spatial Domain for High Quality Images. In *international Symposium on Intelligent Signal Processing and Communications (ISPACS)*.

Holil, M. & Ahmad, T., 2015. Secret data hiding by optimizing general smoothness difference expansionbased method. *Journal of Theoretical and Applied Information Technology*, 72(2), pp.155–163.

Huang, F., Qu, X. & Kim, H.J., 2016. Reversible Data Hiding in JPEG Images. *IEEE Transactions On Circuits And Systems For Video Technology*, 26(9), pp.1610–1621.

Hussain, M. et al., 2017. rightmost digit replacement crossmark. *Signal Processing : Image Communication*, 50(November 2016), pp.44–57.

Kalita, M. & Tuithung, T., 2016. A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution. *International Conference on Systems, Signals, and Image Processing*, 2016–June, pp.6–10.

Kuo, W. et al., 2016. An Improved Data Hiding Scheme Based on Formula Fully Exploiting Modification Directions and Pixel Value Differencing Method. In *11th Asia Joint Conference on Information Security*. pp. 136–140.

Kurniawan, Y. et al., 2016. Hiding Secret Data by using Modulo Function in Quad Difference Expansion. In *International Conference on Advanced Computer Science and Information Systems (ICACSIS 2016)*. pp. 433–437.

Laffont, A. et al., 2017. Enhanced Pixel Value Modification based on Modulus Function for RGB Image Steganography. In *2nd International Conference on Advanced Mechatronics, Intelligent Manufacture, and Industrial Automation (ICAMIMIA 2017)*.

Lahiri, S. et al., Image steganography on coloured images using edge based data hiding in DCT Domain. In *Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual*.

Li, Q. et al., 2017. A novel game-theoretic model for content-adaptive image steganography. *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops A*, pp.232–237.

Liao, X., Wen, Q. & Zhao, Z., 2012. A Novel Steganographic Method with Four-Pixel Differencing and Modulus Function. *Fundamenta Informaticae*, 118, pp.281–289.

Lin, C.N. et al., 2010. Using quad smoothness to efficiently control capacity-distortion of reversible data hiding. *Journal of Systems and Software*, 83(10), pp.1805–1812.

Lou, D.C., Hu, M.C. & Liu, J.L., 2009. Multiple layer data hiding scheme for medical images. *Computer Standards and Interfaces*, 31(2), pp.329–335.

Lu, T., Tseng, C. & Wu, J., 2015. Dual imaging-based reversible hiding technique using LSB matching. *Signal Processing*, 108, pp.77–89.

Lu, Y. & Lyu, W., 2015. A Novel High-capacity Reversible Data-hiding Scheme Using two Steganographic Images. In *8th International Conference on BioMedical Engineering and Informatics (BMEI)*. pp. 667–671.

Maniriho, P. & Ahmad, T., 2017. A Data Hiding Approach Using Enhanced-RDE in Grayscale Images. In *the 2nd International Conference on Advanced Mechatronics, Intelligent Manufacture, and Industrial Automation (ICAMIMIA).*

Maniriho, P. & Ahmad, T., 2017a. Enhancing the Capability of Data Hiding Method Based on Reduced Difference Expansion. *Engineering Letters*.

Maniriho, P. & Ahmad, T., 2018b. Information Hiding Scheme for Digital Images Using Difference Expansion and Modulus Function. *Journal of King Saud University-Computer and Information Sciences (JKSUCIS)*.

Nagaraj, V., Vijayalakshmi, V. & Zayaraz, G., 2013a. Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. *IERI Procedia*, 4, pp.17–24.

Nagaraj, V., Vijayalakshmi, V. & Zayaraz, G., 2013b. Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. In *2013 International Conference on Electronic Engineering and Computer Science Color*. Elsevier B.V., pp.

17–24.

Saleema, A. & Amarunnishad, T., 2016. A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks. In *International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST -2015)*.

Simmons, G.J., 1883. The prisoner's problem and the subliminal channel, Advances in Cryptology. In *Proceedings of CRYPTO'83, in: Lecture Notes in Computer Science, Plenum, New York*. pp. 51–67.

Subhedar, M.S. & Mankar, V.H., 2014. Current status and key issues in image steganography: A survey. *Computer Science Review*, 13–14(C), pp.95–113.

Swain, G., 2016. Digital image steganography using variable length group of bits substitution. *Procedia - Procedia Computer Science*, 85(Cms), pp.31–38.

Tayel, M., Gamal, A. & Shawky, H., A Proposed Implementation Method of an Audio Steganography Technique. In *2016 18th International Conference on Advanced Communication Technology (ICACT)*. pp. 180–184.

Tian, J., 2003. Reversible Data Embedding Using a Difference Expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8), pp.890–896.

Tsai, Y., Tsai, D. & Liu, C., 2013. Reversible data hiding scheme based on neighboring pixel differences. *Digital Signal Processing*, 23(3), pp.919–927.

Tyagi, A., Roy, R. & Changder, S., 2015. High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum. In *Second International Conference on Advances in Computing and Communication Engineering High*. pp. 488–493.

Verma, H.K. et al., 2013. Bi-Directional pixel-value differencing approach for RGB Color Image. In *2013 Sixth International Conference on, Contemporary Computing (IC3)*. pp. 47–52.

Wang, C.M. et al., 2008. A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, 81(1), pp.150–158.

Wang, K., Lu, Z. & Hu, Y., 2013. A high capacity lossless data hiding scheme for JPEG images. *The Journal of Systems & Software*, 86(7), pp.1965–1975.

Wang, X., Ding, J. & Pei, Q., 2015. A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition. *Information Sciences*, 310, pp.16–

35.

Yi, H., Wei, S. & Jianjun, H., Improved Reduced Difference Expansion Based Reversible Data Hiding Scheme for Digital Images. In *9th International Conference on Electronic Measurement & Instruments, 2009. ICEMI '09.* pp. 315–318.

[This page intentionally left blank]

APPENDIX 1

LIST OF NOTATIONS AND SYMBOLS

Cover Image → CI

Secret Data → S

Stego Image → SI

The n^{th} Original Pixel → u_n

Pair of Pixel → P

Difference between pixel pairs → v_n

Reduced Difference → v''_n

Modified Difference → v'_n

New Pixel → u'_n

Location Map → LM

The Base Point Pixel in Each block → u_m

Block of Pixel → Blk_p

And → &

Image Pixels' Average → Im_Pix_Avg

Rightwards Arrow: →

[This page intentionally left blank]

APPENDIX 2

ABBREVIATIONS AND ACRONYMS

DE: Difference Expansion

RDE: Reduced Difference Expansion

PSNR: Peak Signal-to-Noise Ratio

SD: Spatial Domain

TD: Transform Domain

DWT: Discrete Wavelet Transform

DCT: Discrete Cosine Transform

DD DT: Double Density Dual Tree

HT: Hadamard Transform

CT: Curvelet Transform

Bpp: Bit Per Pixel

PVD: Pixel Value Differencing

JPEG: Joint Photographic Experts Group

TIFF: Tagged Image File Format

RDH: Reversible Data Hiding

MATLAB: Matrix Laboratory

IRDE: Improved Reduced Difference Expansion

LSB: Least Significant Bit

RGB: Red Green Blue

GDE: Generalized Difference Expansion

CPU: Central Processing Unit

RAM: Random Access Memory

LM: Location Map

EX-RDE: Expandable Reduced Difference Expansion

NON-EX-RDE: Non-Expandable Reduced Difference Expansion

FFEMD: Formula Fully Exploiting Modification Directions

8nPVD: 8-Neighboring Pixel Value Differencing

[This page intentionally left blank]

Author's Biography

Pascal Maniriho received his Bachelor of Technology with Honors in Information and Communication Technology from Umutara Polytechnic, Eastern Province, Rwanda, in September 2013. He completed his Master of science in Informatics, Faculty of Information Technology and Communication at Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia, in January, 2018. His research interests include information security, data hiding, network and database security, mobile ad hoc networks, wireless sensor networks, and big data analysis. He is currently a member of IAENG and Academia international journals. For any queries, you may address the author through pascal15@mhs.if.its.ac.id or pascaliuslionceau@gmail.com.

[This page intentionally left blank]