THESIS

ENHANCING IMAGE-BASED DATA HIDING METHOD USING REDUCED DIFFERENCE EXPANSION AND DIFFERENCE INTEGER TRANSFORM

MAURICE NTAHOBARI
NRP. 5116201702

SUPERVISOR
Tohari Ahmad, S.Kom., MIT., Ph.D.
NIP. 197505252003121002

MASTERS PROGRAM OF COMPUTER SCIENCE

NET CENTRIC COMPUTING

DEPARTMENT OF INFORMATICS

FACULTY OF INFORMATION TECHNOLOGY

INSTITUT TEKNOLOGI SEPULUH NOPEMBER

SURABAYA

2018

Thesis submitted to meet one of the requirements to obtain a Master degree

in Computer Science

At

Institut Teknilogi Sepuluh Nopember Surabaya

By:

Maurice Ntahobari
NRP. *5116201702*

With Title:
ENHANCING IMAGE-BASED DATAHIDING METHOD USING REDUCED DIFFERENCE EXPANSION AND INTEGER TRANSFORM SCHEME

Exam date: 3rd -01-2018
Even graduation: 2018

Approved by:

Tohari Ahmad,S.Kom,MIT,Ph.D (Supervisor 1)
NIP. 197505252003121002

Royyana Musliim Ijtihadie, S.Kom,M.Kom,pH.D (Examiner 1)
NIP: 197708242006041001

Waskitho Wibisono,S.Kom,M.Eng,Ph.D (Examiner 2)
NIP. 197410222000031001

Dr.Eng. Radityo Anggoro, S.kom, MSc (Examiner 3)
NIP. 19841016200812100002

Dean faculty of Information
Communication and Technology,

Dr. Agus Zainal Arfin S.Kom.,M.Kom
NIP. 19720809199512100l

ACKNOWLEDGMENT

I would like to convey my thanks to almighty Good for his love and protection from my childhood, in all my studies primary school, high school, undergraduate and to this master's graduate level.

My thanks goes to my family, my lovely wife in this entire world Cecile Mushimiyimana and my son Ikaze Pacis Uberi Maurice Balbao who bring happiness through their love and encourage me to be strong and believe that every things will be done. I thank her again for her uncomplaining to allow me to leave her for three years and stay alone in my hometown Rwanda. My wife, I recognize your support to achieve on this level of accomplish this thesis. My gratitude goes to other members of my entire family, my father Faustin Mukeshimana, my mother Beatrice Nyirabaganga even though you passed away but whatever I do remember the words you told me before you pass away which is " My son, you will be a man. Take care to your brothers and sisters". I will always respect those words. My thanks also go to the family of Gratien Hategekimana and Donata Mukabakina who raised me and for their valuable support during my studies in terms of finance. You are important people.

So far so good, I would like to give my sincere gratitude to my supervisor Tohari Ahmad, S.Kom.,MIT.,Ph.D for the continuous supports in my masters study and researches, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this research thesis. I could not have imagined having a better supervisor and mentor for my study like him.

Besides my supervisor, I would like to thank the rest who contributed a lot in my studies to achieve on this success. All lecturers who give courses in the option of NCC like Prof.Ir. Supeno Djanali, M.Sc.,Ph.D, Royyana Muslim Ijtihadie, S.Kom, M.Kom, Ph.D, Waskitho Wibisono, S.Kom, M.Eng, Dr.Eng. Radityo Anggoro, S.Kom, M.Sc, Henning Titi Ciptaningtyas, S.Kom.,M.Kom., for their encouragement,

insightful comments and they always listen to me as a child and his parents. They are not only lecturers but also parents.

Certainly, I give my grateful thanks to my advisor Dr. Agus Zainal Arifin, S.Kom.,M.Kom for his guidance and supports to solve academic maters where it was needed and I thank my fellow classmates for their friendship and for all the fun we have had in this two years.

DEDICATION

This thesis is dedicated to my family and friends. A special filling and appreciation to my lovely wife Cecile Mushimiyimana and my son Ikaze P.U. Maurice Balbao whose words of encouragement and push for tenacity ring in my ears. The family of Gratien Hategekimana and Donata Mukabakina who had never left my side. They are fantastically special.

I also dedicate this work to my lecturers, classmates who have helped me through the process of accomplishing the work. I will always appreciate what they have done to help me in developing my background skills in Informatics Technology.

I dedicate this work to my friends Pierre Damien Uwitije whom we shared food and everything including advices of how to survive in studying situation. He was my best friend I met in ITS Surabaya and we stayed closer in our dormitory known as Asrama mahasiswa ITS.

DECLARATION

I, Maurice Ntahobari declare that this thesis entitled “Enhancing Image-Based Data Hiding Method Using Reduced Difference Expansion and Difference Integer Transform” has been written by me and it is the records of my work carried out by me or principally by myself in collaboration with my supervisor Tohari Ahmad, S.Kom., MIT., Ph.D.

The work has not been submitted in any previous works for the fulfilment of the requirement of masters degree program. This work was admitted as a research of a student in 2018 and as a candidate for the degree of masters in department of informatics engineering with specialization in Network Centric Computing. This special record was carried out in the Institut Teknologi Sepuluh Nopember between 2016 and 2018.

Date .....

Maurice Ntahobari

.....

ENHANCING IMAGE-BASED DATA HIDING METHOD USING REDUCED DIFFERENCE EXPANSION AND DIFFERENCE INTEGER TRANSFORM

Student Name : Maurice NTAHOBARI
NRP : 5116201702
Supervisor : Tohari Ahmad, S.Kom.,MIT.,Ph.D.

ABSTRACT

Data hiding is a technique that is used to hide secret information within a cover media. In its growth of technology, this technique is not only used for concealing data but also for data authentication and copyright identification. Furthermore, in implementing data hiding algorithm, the technique can leads to diminishing the quality of cover media. In this context, cover media could be image, audio, text or video. Since, hiding secret message within cover media for example image destroys its visual quality. Therefore, unauthorized users can suspect the existence of secret data within that image.

To achieve on high quality stego image is still a challenging problem. In the past years, different data hiding algorithms have been developed to secure data during transmission process by increasing the visual quality. However, there is still a room to contribute in order to achieve on high performance algorithm in terms of visual quality. This is why currently many data hiding method are being proposed.

In this thesis, a new data hiding algorithm is proposed based on difference expansion that aims to improve the quality of stego image for a given payload capacity. In this

proposed method, an image is divided into blocks then a pixel value is used in order to calculate the difference, and it is subtracted from each pixel in a pixel block as the base point. Then, the difference is reduced before embedding using proposed method. Thereafter, the secret message is embedded within the reduced difference. Moreover, at the recipient side, the reverse of embedding process is performed to extract, recover the secret message and cover image respectively without any damage.

The outcome from the new proposed method is compared to the previous method and the performance is better. The performance has been increased by the highest improvement of 2.4 dB that was obtained for head image when the size of 5 kb was embedded. The highest PSNR value of 42.609 dB was gained for chest image and the low PSNR value of 34 dB was obtained for head image. In general, the new method performs better for all size of secret message.

Keywords: *Data hiding, Data protection, information security, secret data, visual quality, reversible data hiding, reduced difference expansion*

TABLE OF CONTENT

TABLE OF FIGURES

TABLE OF TABLES

LIST OF ACRONYMS

1. DE: Difference Expansion
2. RDE: Reduced Difference Expansion
3. PSNR: Peak Signal to Noise Ration
4. MSE: Mean Square Error
5. GIF: Graphics Interchange Format
6. JPG(JPEG): Joint Photographic Expert Group
7. PNG: Portable Network Graphics
8. TIFF: Tagged Image File Format
9. DCT: Discrete Cosine Transform
10. DWT: Discrete Wavelet Transform
11. IWT: Integer Wavelet Transform
12. LSB: Least Significant Bit
13. NCC: Net Centric Computing
14. dB : decibel
15. RAM: random Access Memory
16. HP: Hewlett-Packard

CHAPTER 1
INTRODUCTION

This chapter explains the basic points in making this thesis. These include background, research hypothesis, problem formulation, research contribution, research objectives, research benefits and the scope of the research.

1.1 Background

In this generation of information technology, files or information sharing between users in remote have been needs for everyone, anytime and anywhere. Public network that is normally used for such communication is however unsecure. This means that everything being transferred through the internet can be intercepted and changed. If the modified message is forwarded to the receiver, message integrity and confidentiality are violated. Hence, the end-to-end communication should be protected against security threads in modern communication.

As one of the methods to protect data, data hiding technique allows to hide credential or secret information in multimedia file such as text, audio, image or videos. In the simplest form, it was implemented thousands years ago before the information technology was developed (Huang, Chuang, & Wu, 2008). The technique has been used in the Second World War (Por & Delina, 2008). In that time, Germany soldiers have used steganography to secure communication by creating a microdot where a text or an image was reduced onto a small disc to prevent unauthorized users from detecting the existence of a secret message (Cheddad, Condell, Curran, & Kevitt, 2010). Not only that because in history, ancient Herodotus have used it to secure communication in difference ways. For example, there is where they used to shave the hair of their slaves and put message on it. Then, once the head‘s hair grew up, they were sent through their enemies where at the destination the hair was shaved then a message was able to be read. In this scenario, slave’s hair is taken as a cover then, growing hair is as embedding data then shaving hair is like extraction of a message.

For simplicity, in this thesis the terms data hiding and steganography are used interchangeably. Steganography has a slightly difference from watermarking in some extents compared to cryptographic technique. Cryptography secures information by transforming them into different domain and become unreadable format. However, the technique gives a hint to adversary that a message is being transmitted (Patel & Meena, 2016; Saroj, Chauhan, & Sharma, 2015). This may lead to attack where attackers do their best to do cryptanalysis. It makes the information to be unreadable to the unauthorized users. In contrast, steganography still employs the same domain but requires other data as a carrier or cover media file while watermarking technique hides data related to cover as its copyright identification or protection (Muhammad, Sajjad, Mehmood, Rho, & Baik, 2016). In the case where unauthorized users intercepting the data, they may not realize that, a secret message is being transmitted due to the common appearance between original cover and stego media.

In general, after the embedding process, the resulted stego data is sent over public networks as depicted on Figure 1.1. The Figure shows three steps of data hiding, such as embedding process, attacking process and extraction process. The embedding process involves the action of concealing secret information into a cover while the attacking process maybe adding noise to the media content or modify the content. This is commonly known as active attack where secret message is modified then fake information is transmitted to the destination. The attacker may also monitor the message being transmitted without a severe action. This is known as passive attack where the attacker does not change anything about the message.

At the destination side, both the message and cover are extracted and recovered accordingly. This process works on reversible data hiding, which is different from irreversible one, where only secret message is extracted (Chakraborty, Jalal, & Bhatnagar, 2013). Examples of reversible data hiding algorithm are Least Significant Bit (LSB)-based method, Difference Expansion (DE) method and their variations (Tian, 2003; Liu, Lou, & Lee, 2007).

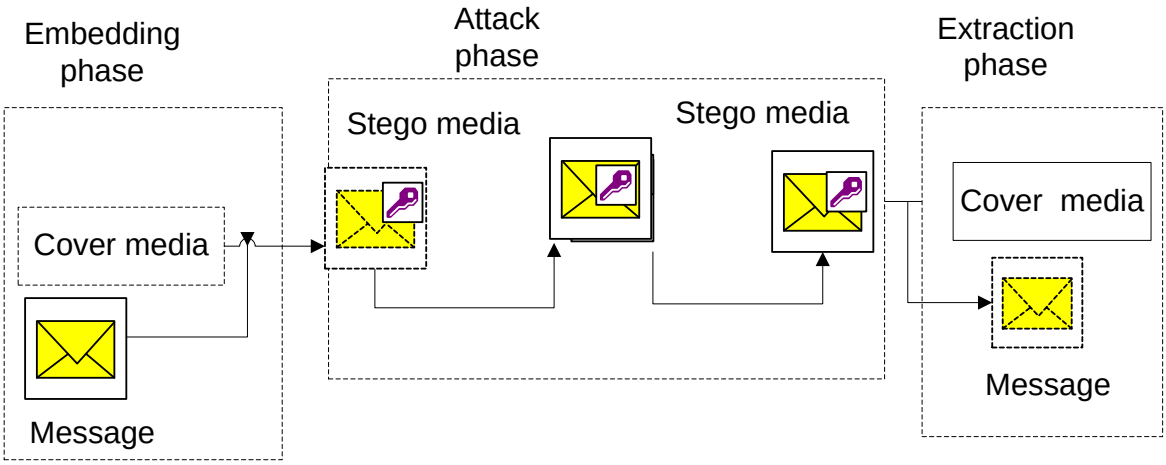

Figure 1. 1 The processes of reversible data hiding

The LSB based algorithm is done by replacing the LSB bit value of pixels in the cover image (Al-Afandy, Faragallah, & Elmhalawy, 2016; Goel, Gupta, & Kaushik, 2014). Due to its easiness, this algorithm is vulnerable to attack because it is easily performed. Furthermore, Difference Expansion algorithm was proposed by Tian in (Tian, 2003). The algorithm exploits the redundancy information within an image to hide a secret message. This method has lower embedding capacity since each block of two pixels is used to only carry 1 bit. Another method in (Govind P.V, M.K, & Varghese, 2015) was introduced to increase the payload capacity. It was developed based on image interpolation and difference expansion as preprocessing. Next, another DE-based method was designed (Kumar, Natarajan, & Muraledharan, 2014), it combines pixel pair method and difference expansion proposed by Liu et al (Liu, Lou, & Lee, 2007), to improve payload capacity. The method allows embedding high payload capacity but quality of stego image is low which means image is highly distorted. The main problem faced by the previous difference expansion data hiding based method is low visual quality of stego image compared to original cover image when a given embedding capacity is hidden.

In general, it is a challenging problem to develop a data hiding algorithm, which supports both high visual quality and payload capacity simultaneously. This is because they are inversely proportional (Yi, Wei, & Jianjun, 2009; Hua, Shoujian, & Daozhen, 2010). This means the increase in one parameter decreases the other.

In this thesis, I propose a data hiding algorithm that is based on difference reduction to have good quality of stego image for a given payload capacity. This will be combined with integer transform scheme based on fixed pixel value to achieve on high visual quality that misleads attackers due to high similarity between original image and stego image.

The integer transform scheme is all about the choice of base point to compute the differences within a pixel block. This is because a better choice of based point and a reduced difference expansion influence the performance of a designed algorithm in terms of visual quality of stego and original image. The algorithm is reversible which is advantageous in medical environment for accurate patient diagnosis.

1.2 Research hypothesis

In this thesis, two main hypotheses are taken to be considered in the evaluation of the proposed method. These are:

1. The reduction of difference between two adjacent pixels increases the visual quality of stego image.
2. Increasing payload capacity decreases quality of stego image

1.3 Problem formulation

By considering the background of this thesis, problem formulation is as follow:

1. How the visual quality of stego image can be increased to protect secret data?
2. How the size of secret message affects the quality of stego image?

1.4 Research contribution

The contribution in this thesis is to propose a new data hiding method based on difference expansion technique and the fixed base point in the computation of differences. The first contribution is about a new formula of difference reduction that is different to previous method to have better quality of stego image after data embedding because the reduction of difference increases the visual quality of stego image (Ahmad, Holil, Wibisono, & Ijtihadie, 2013). The proposed method will results to good quality of stego image. This is because the resulted stego pixels will be closer to original pixel before data embedding.

The second contribution is about the choice of base point (difference integer transform scheme) to compute the difference expansion, because this also with in combination with reduced difference expansion influence the quality of stego image due to that many image pixel blocks will be used to carry secret data rather than being ignored because of overflow and underflow.

1.5 Research objective

By considering the problem formulation mentioned in (1.3), the objective of this research is to Protect secret data by increasing visual quality of stego image based on reduced difference expansion and difference integer transform scheme (the choice of base point to compute difference between two neighboring pixels).

1.6 Research benefits

The purpose of this thesis is to develop a sophisticated data hiding algorithm that will help to secure data during transmission. People in communication channel will ensure that they are communicating securely so that data integrity, which means being sure that data have not changed during transmission, and confidentiality, which means being sure that data are being accessed by intended receiver, are preserved. At the destination both secret information and cover image are recovered which is benefit in some field such as medical environment for health practitioners to be sure

about the patients being treated and better diagnosis. This is also important in military services and even in digital forensic for law enforcement.

This research has also a big benefit to the readers in information technology especially in the field of information security because it gives the basics for researchers, scholars about security in communication channel and the idea of data protection using data hiding algorithm or another techniques like cryptography. It is also a benefit for me as the author of this book to fulfill the requirement of holding a masters degree in Network Centric computing.

1.7 The scope of this thesis

To accomplish this thesis, the following tools and software will be use:

1. The medical and common grayscale images of resolution 512×512 pixels
2. MATLAB R2014a was used as tool to simulate my proposed algorithm.
3. A random generated binary bits (1, 0) of different size 5 Kb, 10 Kb and 20 kb using randi MATLAB function will be considered as secret message to be embedded within image.
4. The comparison of proposed method and previous method is done to prove the performance of the new proposed method.

CHAPTER 2
BASIC THEORY AND LITERATURE STUDY

2.1 Theory

This chapter focuses on the theories about security in computer network in general and goes in deep by explaining the security system structure. Here, the author highlighted as green the part that the new proposed method will be focusing on because there are different techniques to provide data security depending on where the system is being used and the purpose of the method itself.

2.1.1 Information security

In computer network, information security is considered as a set of approaches for managing the essential processes, tools and policies to fight against, detect, document and counter threats to digital and non-digital data. The responsibility of information security comprise setting up a set of business processes that will defend information assets despite of how the information is formatted or whether it is being transmitted, processed or is stored in a any storage. In this context, information security system is achieved through different techniques as it is presented on Figure 2.1. As it is shown this work focuses ensuring the security of data using data hiding approach.

Data hiding and cryptography are the two foremost techniques for protecting data during its transmission. In cryptography, the plain text is transformed into an indecipherable format called cipher data. In this technique, the transformation of plain text into cipher text involves secret key, which may be public key, or private key for both encryption and decryption respective to the sender and receiver side. Figure 2.2 illustrates the concept of cryptography.

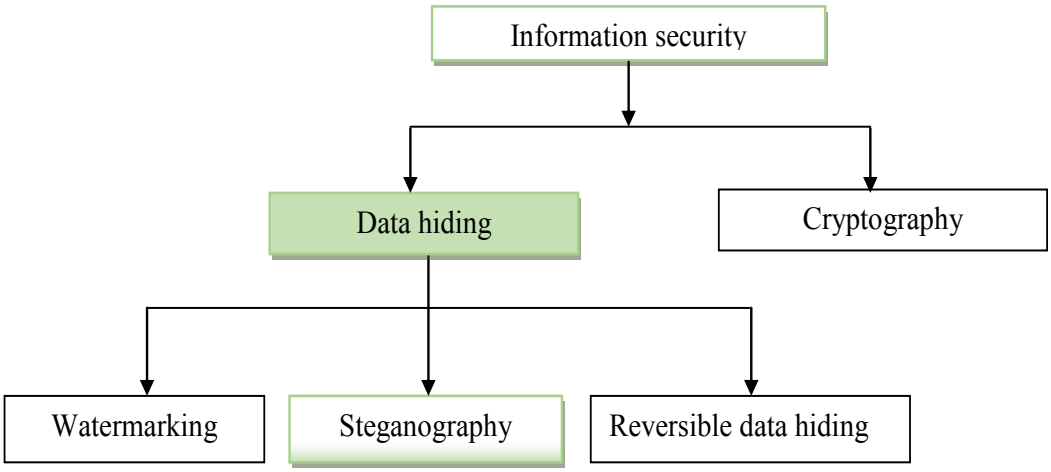

Figure 2. 1 Types of information security systems (Shaik, Thanikaiselvan, & Amitharajan, 2017)

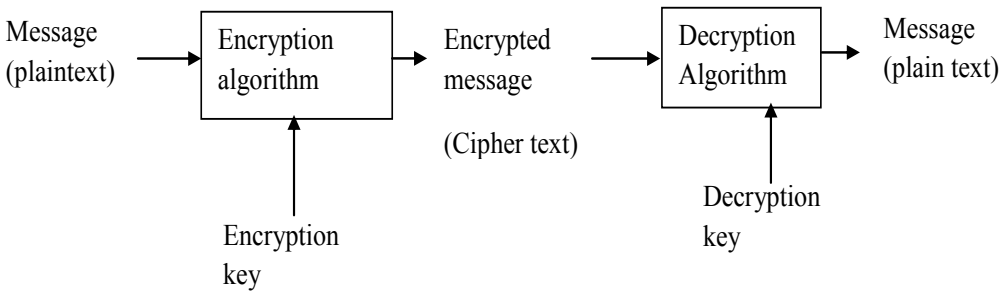

Figure 2. 2 The concept of cryptography

The cryptographic techniques can achieve to its objective in different ways. This is why there are two types of cryptograph. These are public key cryptography also known as asymmetric key cryptography and symmetric key cryptography. In symmetric key cryptography presented on Figure 2.3, both sender and receiver share the same secret key.

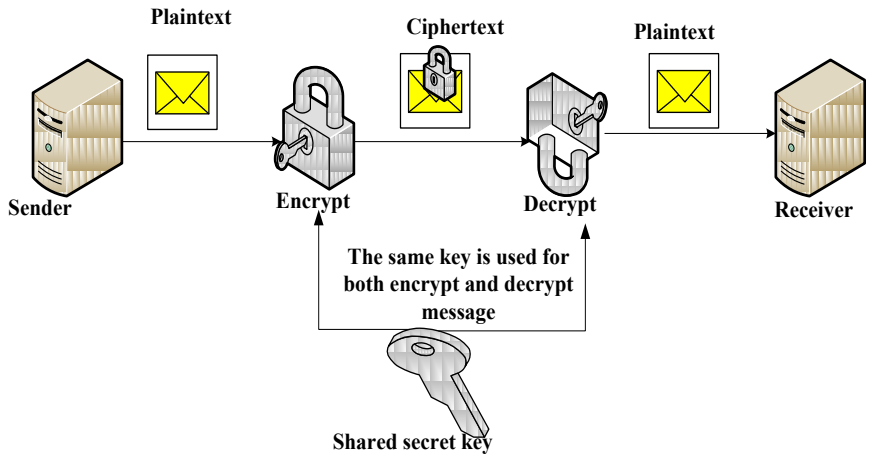

Figure 2. 3 Symmetric key encryption (Alexander, 2016)

Hoverer, for public key or asymmetric key cryptography both sender and receiver have private and public key respectively for encryption and decryption of a message shown on Figure 2.4. Here, a pair of keys is used. Everyone (bob and Alice) keeps a private key privately since both parties own it while public key is known and accessible. Hence, it is stored in key repository. The message is encrypted using the sender public key then it is transmitted through public network to the receiver who uses his private key to decrypt the message.

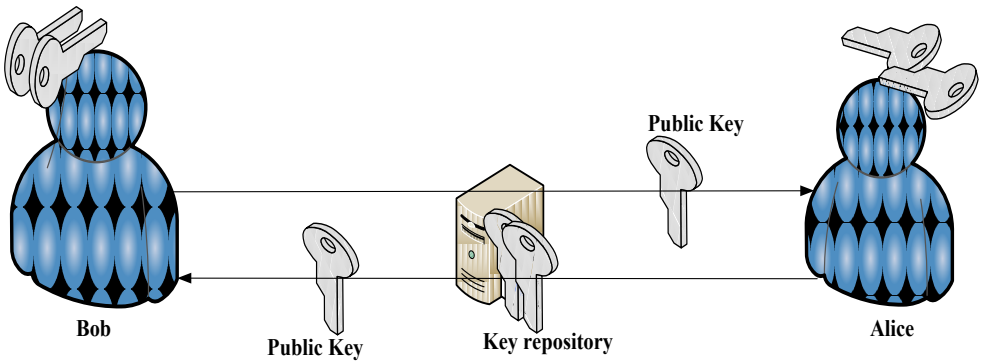

Figure 2. 4 Public key encryption (Alexander, 2016)

The limitation of cryptography is that the third parties are always aware about the communication of incomprehensible data. This can lead to brute force attack so that an algorithm can be broken to access secret information (cryptanalysis).

2.1.2 Data hiding

Data hiding is a process of inserting secret data inside a multimedia file such as image, video, audio or text. In this method, two inputs are required those are secret data and cover media. The output from these inputs is a stego cover.

Any data hiding method must consider three properties such as embedding capacity that is the amount of data to be carried within a media, the visual quality that is how an original media have changed compared to stego media and Robustness that is how the algorithm resist to attacks.

Hiding the existence of secret information is the main advantage of data hiding techniques over cryptography. There are some applications, which use cryptography and data hiding at the same time in the same process. In this case, secret data are first encrypted then data hiding techniques are applied. This increases the robustness of a stego system because even though a message is intercepted, the computation time is high to extract the secret message and cryptanalysis techniques to decrypt an encrypted message are needed.

Digital watermarking, steganography and Reversible Data Hiding (RDH) are three types of data hiding approaches used to secure data. However, they is a slight difference between them. Watermark is a sequence of digital bits placed in a digital cover file that recognizes the file's copyright information while steganography is dedicated for secrete communication. It changes the image in such a way that only the sender and the intended receiver can detect the message sent through it. Since it is invisible, the detection of secret data is not simple.

2.1.3 Image

Digital image is an array that contains real or complex values. Those values are represented by a certain row of bits. An image can be represented by the size of the M row and N columns and it is defined as a two dimension function $f\ (x, y)$, where x and y are spatial coordinates, and amplitude f at the coordinate point (x, y) called the intensity or gray level of the image at the point (x, y).

An image is said to be a digital, if the values of x, y and the overall gray image level value are finite and discrete. Figure 2.5 represents a digital image coordinates while the equation (2.1) shows an image as matrix. The value at the position x, y that is the slice between the line and columns are known as picture elements, image elements, pels, or pixels.

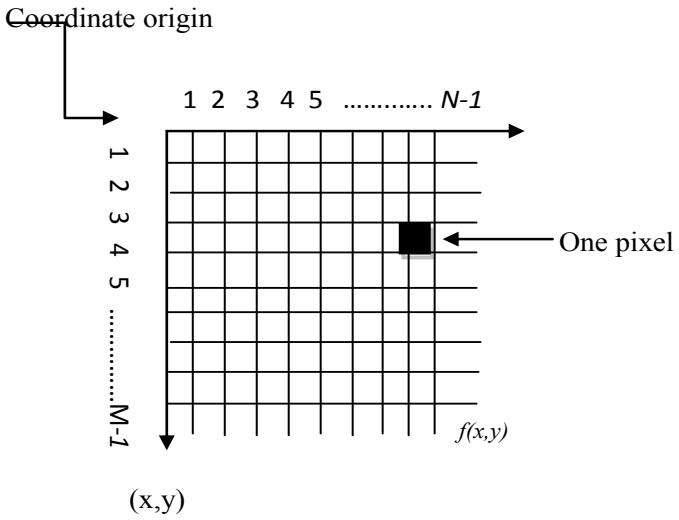

Figure 2. 5 Digital image representation

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) \ldots\ldots\ldots f(0,N-1) \\ f(1,0) & f(1,1) \ldots\ldots\ldots f(1,N-1) \\ . & . \quad\quad . \\ . & . \quad\quad . \\ . & . \quad\quad . \\ f(M-1,0) & f(M-1,1) \ldots\ldots\ldots f(M-1,N-1) \end{bmatrix} \quad (2.1)$$

2.1.4 Types of Images

Images are classified based on the format they can be stored. They are four main types of Images file and each type differs from another. These types are .tiff, .jpeg .gif and png file format.

2.1.4.1 TIFF

The tiff also known as .tif is a file format that end with an extension of .tiff. It stands for Tagged Image File Format. This type creates a very large file in sizes and it is uncompressed, which means that it contains a lot of image details information that makes the file to be too big. This type exists for color image like RGB, CMYK for print.

2.1.4.2 JPEG

Joint Photographic Expert Group also known as JPG in short, is a file format extension for images. This file extension indicates an image that has been compressed to accumulate a lot of information in a small file. This image format is automatically given to all images taken by camera. This is the reason that with a camera it is possible to take many pictures as possible on one camera card. jpeg is compressed in a way that it makes losses of some image details during the compression in order to make the file small. Hence, it is called as loss compression.

2.1.4.3 GIF

The GIF acronym stands for Graphics Interchange Format. The file is saved using the extension .gif. The format is compressed. However, the compression is different to that of jpeg where gif is lossless compression instead of loss compression. The details information about image is maintained but the file cannot be small as it can be for jpeg.

2.1.4.4 PNG

It stands for Portable Network Graphics. The file format is the same as gif; the only difference is that it supports a range of color and better compression than gif. The image with that format is like the one obtained when taking a screen short because most screen short are the mixture of images and text.

2.1.5 Grayscale image

The grayscale image is the image where the pixel value for red, green and blue colors channels (RGB) has the same value. In other words, they have the same intensity value. This indicates that a grayscale image is a digital image that has only one channel on each pixel. The gray color is referred as the grayscale image color that is between white and black. One of grayscale image type is grayscale image with color depth 8 bits where there are 256 gray color combinations, ranging from 0 up to 255. The pixel value 0 indicates the black color whereas the 255 pixel value indicates the white ones.

2.1.6 Image data hiding

The image data hiding also known as image steganography Figure 2.6, is largely used in covert communication. In image steganography, the embedding algorithm transforms cover image into a stego image by inserting secret message inside it. The embedding approach may involve stego key for high security. An image data hiding is classified into two main categories such as spatial domain and transforms domain data hiding. The spatial domain data hiding (Figure 2.7), makes use of a set of straightforward pixel manipulation approaches that produce gaps in the cover image pixel to hide secret message where the changes are not easily noticeable using human vision system. In this category, it is where least significant bit and difference expansion techniques are allocated.

In image data hiding that is based on transform domain on Figure 2.8, spatial pixel values are transformed to frequency coefficients by using dimensional

transform methods such as Discrete cosine transform (DCT), discrete wavelet transform (DWT), Integer wavelet transform (IWT), and so on. These coefficients are utilized for hiding secret data in transform domain data hiding. In this case, coefficients are changed based on the secret data to be embedded. As an advantage, this modification does not affect the visual quality of stego image. Frequently, transform domain data hiding methods are the derived method from spatial domain data hiding algorithms.

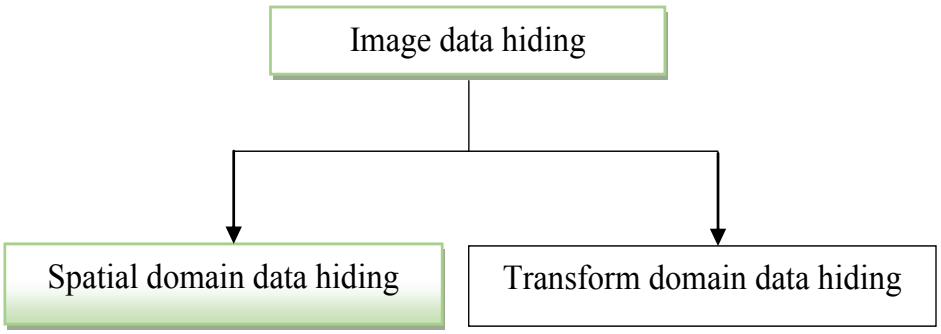

Figure 2. 6. The types of image data hiding approach (Shaik, Thanikaiselvan, & Amitharajan, 2017)

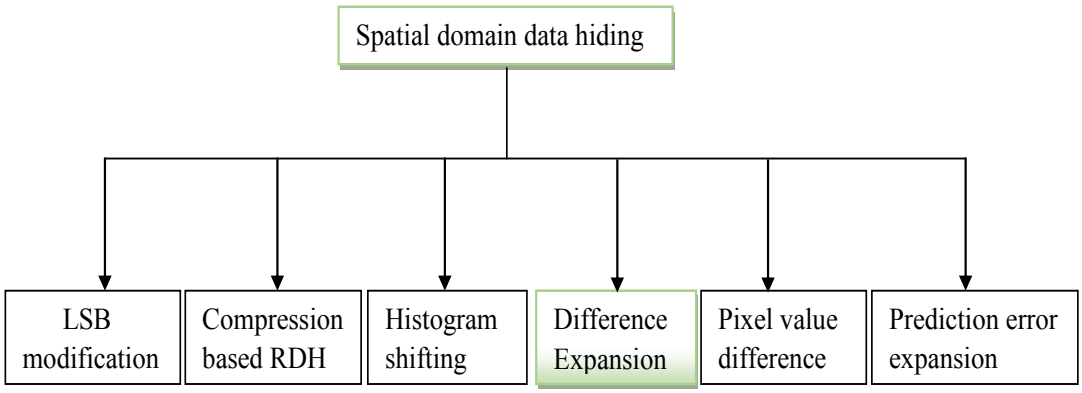

Figure 2. 7 Spatial domain data hiding techniques (Shaik, Thanikaiselvan, & Amitharajan, 2017)

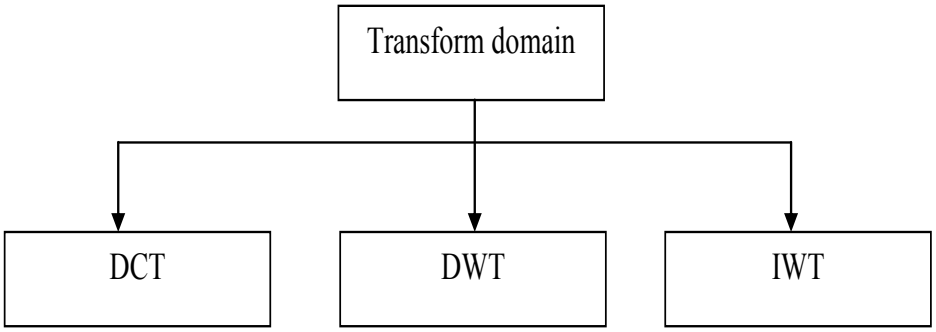

Figure 2. 8 Image data hiding in transform domain
(Shaik, Thanikaiselvan, & Amitharajan, 2017)

2.1.7 Embedding capacity

The embedding capacity is the measure of how much data are being able to be carried within a stego cover without causing the unauthorized users to suspect the presence of secret data.

2.1.8 Visual quality

The visual quality of stego image defines how is the level of similarity between the original cover and the embedded cover. This is known as the similarity, which means that it not exactly the same as the original cover but at least looks alike.

2.1.9 Robustness

The robustness of an algorithm or a method is the measure of how the method resists to an attack or how hard is to break the algorithm. This is called steganalysis that is the technique of determining whether transmitted media has a message encoded into it and if possible extract that message. It is just an art of destroying a stegaographic algorithm to reveal hidden data.

2.1.10 Reversible data hiding

A reversible data hiding is an approach that is performed in such a way that both cover media and secret information can be recovered and extracted respectively.

The Figure 2.9 shows the scheme of reversible data hiding approach. This indicates that secret data (which is indicated by orange color on the figure) are inserted into cover media (indicated by green color) using embedding algorithm. Then, the resulted to stego media (indicated by a mixture of two colors which are green and orange) is used to transport the secret data through the internet to the destination as it is seen on the same figure. At the destination side, both secret data and cover media are extracted and recovered unmodified. This kind of method is applied to hide sensitive data like patient records in medical environment, military imagery and digital forensic for law enforcement. The example here is the difference expansion based method and least significant bit method.

2.1.11 Irreversible data hiding

Irreversible data hiding algorithm is an method used to hide data within multimedia file but it drawback is that only secret information are extracted while cover media is not fully recover.

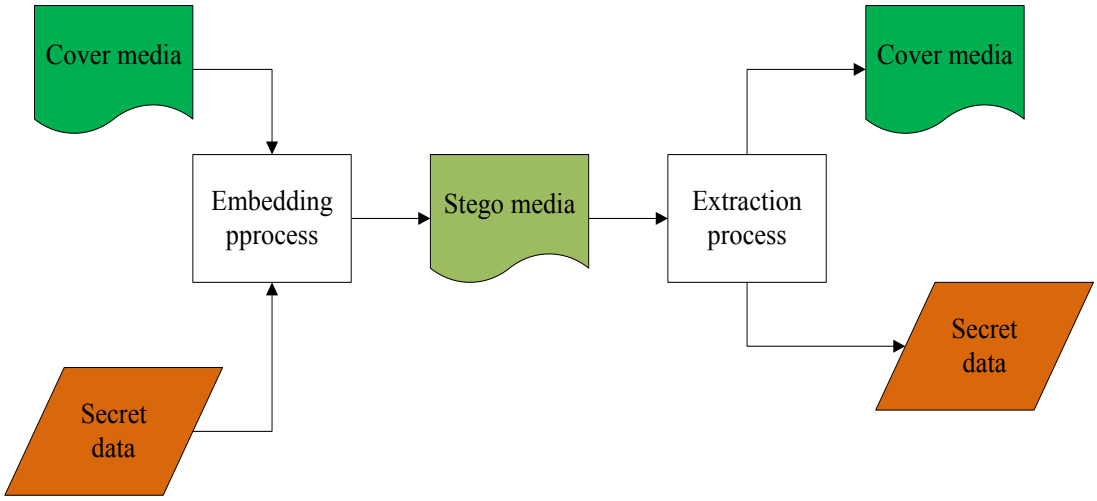

Figure 2. 9. The reversible data hiding scheme

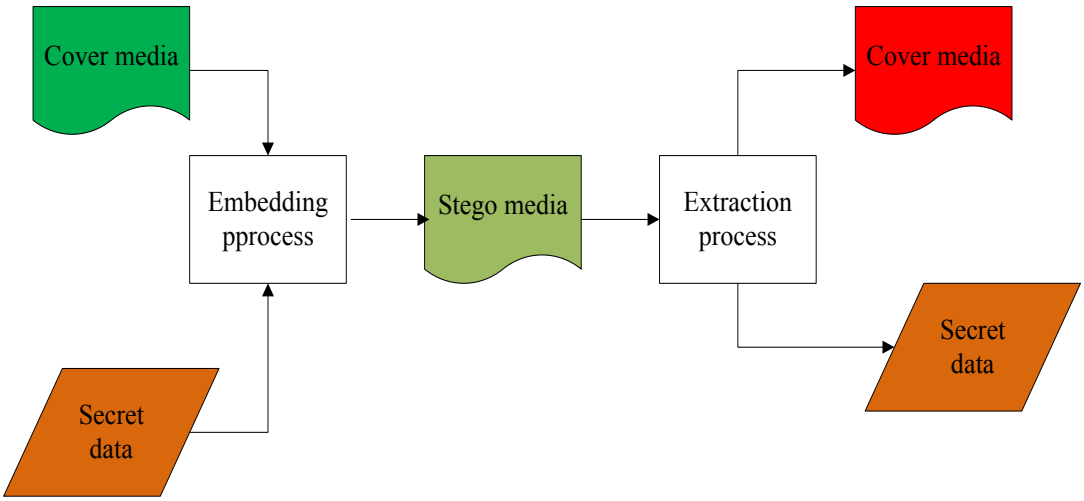

Figure 2. 10. The scheme of irreversible data hiding process

The Figure 2.10 illustrates the irreversible data hiding approach where the cover media at the destination (after extraction process) is marked as red to show that it is different to the original cover media, which was green before secret data insertion.

2.2 Literature study

This part discusses about the methods that are related to the new proposed one. In this section, a clear understanding of these methods is given and their advantages and disadvantages are illustrated.

2.2.1 Integer transform scheme

The integer transform scheme is all about the selection of the base point to compute the difference between adjacent pixels. This is because good base point selection results to lower number of rejected pixel block and it is caused by overflow and underflow issues. This has a big impact on similarity between original and stego cover media. The Similar technique has been used in different data hiding algorithm

such as difference expansion. In (Alattar, 2004),integer transform has been used where the first difference was considered as the average of all pixels in a pixel block and other difference was obtained by subtracting a pixel from its preceding in a pixel block as it is shown on Figure 2.11.

The same techniques have utilized for the similar purpose in (Alattar, 2003) by the same author but this time, the used pixel block was only composed by three pixels. This means that three differences were barely computed then, the first difference is taken as an average of three pixels in each pixel block and then the first pixel was considered as base point to calculate the differences as shown on the Figure 2.12. Here, the embedding capacity is two bits in a single block that is 0.6 average bits for a single pixel.

As the researches continue in this filed some researchers prefer to used the base point from outside of the image pixels in a pixel block. For example in (Ahmad & Holil, 2014) where the base point have been selected to be an average of all pixels in a block. Then, the differences were obtained by making difference between each pixel and the computed average. And again, in (Ahmad & Holil, 2015), the method used the variance of four blocks as the smoothness value while the median was considered as base point to be utilized in the difference computation. These have shows better results for both embedding capacity and visual quality.

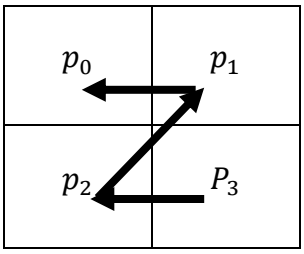

Figure 2. 11 Difference integer transform scheme (Alattar, 2004)

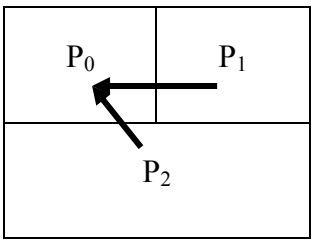

Figure 2. 12 Difference Integer transform scheme (Alattar, 2003)

2.2.2 Difference expansion

In the literature, data hiding algorithm based on difference expansion has been developed to secure communication channels. The main purpose of this method is to obtain a new image called stego image that is similar to the original image used as carrier of secret message.

The difference and average in each block are computed then, message is hidden in a difference. The average contributes in the formation of new pixel (stego pixel). The algorithm is going to be illustrated because it is the basis of the new proposed algorithm in this thesis. Its illustration is as follow:

Suppose p_n , p_{n+1} are two successive pixels and h_n , $h_{\ n}$ be the difference without secret message and difference with secret message embedded, respectively while $p_{\ n}$ is the pixel whose difference contains secret data s_i. In the research, n tooke the value 0 to 1 because a block is composed of two pixels and only a single difference is computed which means n for difference is subjected to be 1. The index i is an index for secret message that takes value 1 because only a single bit from a secret message is embedded within a difference. In addition, $\bar{x}$ denotes the average between those two pixels. The $\bar{x}$ symbol is an average between the two adjacent pixels. These can be seen from equation (2.2) to (2.6)

$$h_n = p_{n+1} - p_n \tag{2.2}$$

$$h_{\ n} = 2 \times h_n + s_i \tag{2.3}$$

$$p_{\ n} = \bar{x} + \left\lfloor \frac{h_{\ n}+1}{2} \right\rfloor \tag{2.4}$$

$$p_{n+1} = \bar{x} - \left\lfloor \frac{h_n}{2} \right\rfloor \quad (2.5)$$

$$\bar{x} = \left\lfloor \frac{p_{n+1} + p_n}{2} \right\rfloor \quad (2.6)$$

In the extraction process, the difference between stego pixels is computed then least significant bit is applied to it to remove secret message. Original difference is calculated which in turn is used to compute the original pixel. First, the differences between stego pixels are computed then, the secret message is taken from each of those differences. See equation (2.7) and (2.8)

$$h_n = p_{n+1} - p_n \quad (2.7)$$

$$s_i = LSB(h_n) \quad (2.8)$$

After getting secret message, the original difference has obtained by using equation (2.9) where the difference computed from stego image has right shifted:

$$h_n = \left\lfloor \frac{h_n}{2} \right\rfloor \quad (2.9)$$

Then the original pixel is given back by using equation (2.10) and (2.11) where the former is used to compute the first pixel while the latter is used to compute the second pixel

$$p_n = \bar{x} + \left\lfloor \frac{h_n + 1}{2} \right\rfloor \quad (2.10)$$

$$p_{n+1} = \bar{x} - \left\lfloor \frac{h_n}{2} \right\rfloor \quad (2.11)$$

This demonstrates that DE that is a reversible data hiding method where both secret message and cover have recovered without any damage. In Figure 2.13, the embedding and extraction process are demonstrated using example. In this example, after computing difference and average, the embedding process starts and it is followed by extraction process. At the end, both original pixel pair and secret message are recovered and extracted respectively.

Overflow and Underflow in this technique is an issue. Overflow happens when obtained pixel value is greater than 255 while underflow is when it is less than 0. To ensure that the problem is avoided, the following condition (2.12) should be fulfilled:

$$0 \leq \bar{x} + \left\lfloor \frac{h_n + 1}{2} \right\rfloor \leq 255 \; and \; 0 \leq \bar{x} - \left\lfloor \frac{h_n}{2} \right\rfloor \leq 255 \tag{2.12}$$

In this method, a pixel block may have one of three characteristics that is expandable, changeable or non changeable block where a block is considered as expandable if equation (2.13) is fulfilled and become changeable if equation (2.14) is fulfilled. A non changeable block is ignored because they cause over flow and underflow problem. This illustrates that during embedding block characteristic are being considered.

$$|2 \times h_n + s_i| \leq min\big(2 \times (255 - \bar{x})\big), 2 \times \bar{x} + 1 \tag{2.13}$$

$$\left|2 \times \left\lfloor \frac{h_n}{2} \right\rfloor + s_i\right| \leq min\big(2 \times (255 - \bar{x})\big), 2 \times \bar{x} + 1 \tag{2.14}$$

2.2.3 Reduced difference expansion

In 2007, Tian proposed method have improved by (Liu, Lou, & Lee, 2007) to increase the quality of stego image and maintaining load capacity high. The method has been improved by reducing the difference between two pixels. In this method, the difference to be reduced is the one that is greater or equal by two. The RDE equation is shown in equation (2.15)

$$|h_n| = \begin{cases} |h_n| & if \; |h_n| < 2 \\ |h_n| - 2^{\lfloor log_2(|h_n|) \rfloor - 1} & if \; |h_n| \geq 2 \end{cases} \tag{2.15}$$

After computing the reduced difference for each difference in a block, the embedding is carried out on the obtained difference. The method uses location map to successful is able to restore the original difference value. The location map number is the same as the number of blocks in an entire image that means every block is identified by a location map.

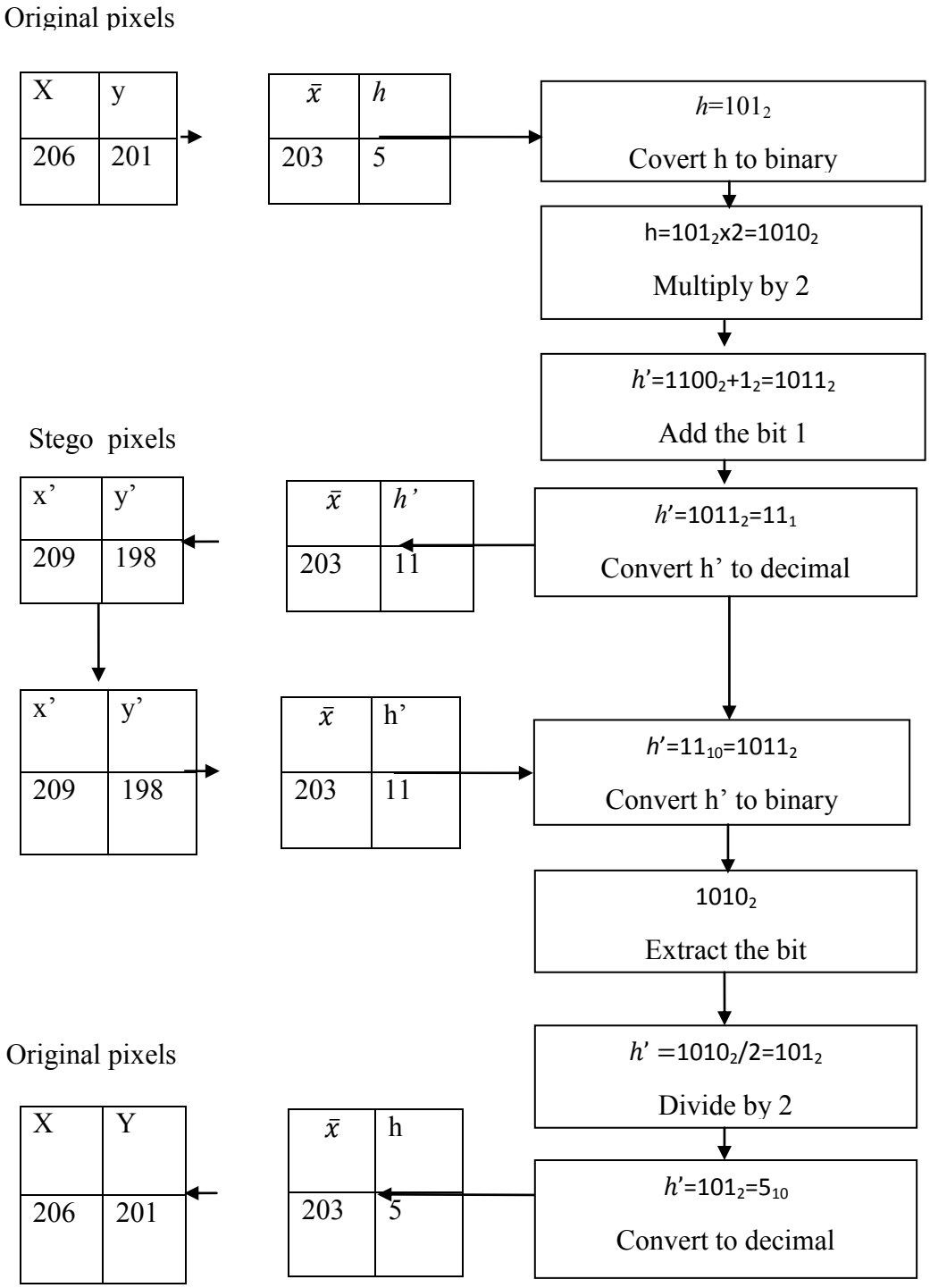

Figure 2. 13. Example of embedding and extraction process for difference expansion based method (Al-Qershi & Ee, 2009)

In the extraction process the following equation (2.16) has used to recover original difference which will be used to compute original pixel where loc: means location map.

$$|h_n| = \begin{cases} |h\ _n| & if\ |h\ _n| \le 1\ and\ loc = 0 \\ 2 & if\ \ |h\ _n| = 1\ and\ loc = 1 \\ |h\ _n| + 2^{\lfloor log_2 |h\ _n| \rfloor}\ if\ \ |h\ _n| > 1\ and\ loc = 0 \\ |h\ _n| + 2^{\lfloor log_2 |h\ _n| \rfloor - 1}\ if\ |\ h\ _n| > 1\ and\ loc = 1 \end{cases} \quad (2.16)$$

By using this method, the visual quality of stego image has increased but the capacity of hidden message is reduced because only differences that are greater than two are used. This means some block have not used for example if a difference is equal to one or minus one.

2.2.4 Improved reduced difference expansion

The RDE method have a drawback that, the visual quality was still law which means the dissimilarity between stego image and original image was still high .The method have improved in (Yi, 2009)u in 2009 by adjusting the RDE function proposed by (Yi, Wei, & Jianjun, 2009) to reduced the cover image distortion further more. The equation becomes (217). The location map is used as follow (2.18) to recover original difference. In the extraction side, the original difference is recovered (2.19) with the help of location map. After that, the original pixel is correctly recovered, hence the method is reversible.

$$h\ _n = \begin{cases} h_n\ - 2^{\lfloor log_2(|h_n|) \rfloor - 1} & if\ 2 * 2^{n-1} \le h_n \le 3 * 2^{n-1} - 1 \\ h_n - 2^{\lfloor log_2(|h_n|) \rfloor} & if\ 3 * 2^{n-1} \le h_n \le 4 * 2^{n-1} - 1 \end{cases} \quad (2.17)$$

where $n = \lfloor log_2(|h_n|) \rfloor$

$$loc = \begin{cases} 0 & if\ 2 * 2^{n-1} \le h_n \le 3 * 2^{n-1} - 1 \\ 1 & if\ 3 * 2^{n-1} \le h_n \le 4 * 2^{n-1} - 1 \end{cases} \quad (2.18)$$

$$h_n = \begin{cases} h''_n\ + 2^{\lfloor log_2(|h_n|) \rfloor + 1} & if\ loc = 0 \\ h''_n + 2^{\lfloor log_2(|h_n|) \rfloor} & if\ loc = 1 \end{cases} \quad (2.19)$$

2.2.5 Difference expansion of quads

Due to low embedding capacity of DE method, in (Alattar, 2004), a difference expansion based on quad pixels was proposed with the purpose to increase embedding capacity. In its implementation, four pixels have grouped into a block (see on Figure 2.14). Moreover, the differences have been computed between the two adjacent pixels. The previous method (Tian, 2003) was able to hide only one secret bit within a block. The proposed allow hiding three secret bits per block. This means Tian's method in (Tian, 2003) can hide only 0.5 bpp while the method in (Alattar, 2004) allows 0.75 bpp (bit per pixel) to be hidden in one quad pixel block. The integer transform to compute the differences is shown in equation 2.20 where the first difference is the average of all pixel in a quad pixels block.

$$\begin{cases} h_0 = \left\lfloor \frac{p_0+p_1+p_2+p_3}{4} \right\rfloor \\ h_1 = p_1 - p_0 \\ h_2 = p_2 - p_1 \\ h_3 = p_3 - p_2 \end{cases} \quad (2.20)$$

In the equation 2.20 $\lfloor . \rfloor$ means the least near integer value. The bit insertion is carried on each difference without being reduced. This is performed based on the category of pixel block where if the block is expandable the following equation (2.21) is used and if the block is changeable the equation is used (2.22) while non-changeable block is ignored which means that pixels will not change during the stego pixel construction. The inverse integer transform function to constructed stego pixels that later gives stego image is calculated using the equation (2.23)

p_0	p_1		
p_2	p_3		

Figure 2. 14 The example of block of 2×2 pixels

$$\begin{cases} h'_1 = 2 \times h_1 + s_1 \\ h'_2 = 2 \times h_2 + s_2 \\ h'_3 = 2 \times h_3 + s_3 \end{cases} \quad (2.21)$$

The extraction process is the reverse of embedding process. After computing the integer transform function from stego image block, least significant bit is taken from the difference then original difference is obtained to reconstruct original image. The same as its previous method this method use location map to locate where the secret message have embedded which is important during extraction. By using this method, the load capacity has increased however, the quality of image after embedding has decreased.

$$\begin{cases} h_1 = 2 \times \left\lfloor \frac{h_1}{2} \right\rfloor + s_1 \\ h_2 = 2 \times \left\lfloor \frac{h_2}{2} \right\rfloor + s_2 \\ h'_3 = 2 \times \left\lfloor \frac{h_3}{2} \right\rfloor + s_3 \end{cases} \quad (2.22)$$

$$\begin{cases} p'_0 = h_0 - \left\lfloor \frac{h_1+h_2+h_3}{4} \right\rfloor \\ p'_1 = h_1 + p_0 \\ p'_2 = h_2 + p_1 \\ p'_3 = h_3 + p_2 \end{cases} \quad (2.23)$$

2.2.6 An Improved Quad and RDE based Medical Data Hiding Method.

In 2013 previous methods have improved by (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) by combining both the method in (Alattar, 2004) and in (Liu, Lou, & Lee, 2007) to improve both quality and payload capacity. The proposed method uses a block of four pixels. The difference between this method and the one in (Alattar, 2004) method resides on the integer difference transform scheme where the first difference have been considered as zero (2.24).

$$\begin{cases} h_0 = 0 \\ h_1 = p_1 - p_0 \\ h_2 = p_2 - p_1 \\ h_3 = p_3 - p_2 \end{cases} \quad (2.24)$$

To reduce image distortion after embedding process, different reduction formula proposed by (Liu, Lou, & Lee, 2007) have adjusted to get small difference as it is illustrated on equation (2.25) where the reduction is performed form both negative and positive values except the value which are between and including one and minus $1 \leq h_n \geq -1$which may cause overflow or underflow.

$$h = \begin{cases} h_n - 2^{\lfloor log_2(h_n) \rfloor} & if \ h_n > 1 \\ h_n + 2^{\lfloor log_2(|h_n|) \rfloor} & if \ h_n < -1 \end{cases} \quad (2.25)$$

The category of pixel block expandable, changeable and non changeable are considered during embedding process but here expandable has divided into RDE expandable and non RDE expandable where if a block is classifier in this categories differences are reduced before embedding while for non RDE expandable, the embedding is performed directly to the original difference.

The location map is used to identify the category of a block and the place where secret message have embedded Figure 2.15. After that, the inverse integer transforms function to make embedded image pixel become (2.26). The method have improved the visual quality of stego image however, the embedding capacity is still low. The implementation flowchart for embedding process in this method is illustrated on Figure 2.16

$$\begin{cases} p_0 = p_0 \\ p_1 = h_1 + p_0 \\ p_2 = h_2 + p_1 \\ p_3 = h_3 + p_2 \end{cases} \quad (2.26)$$

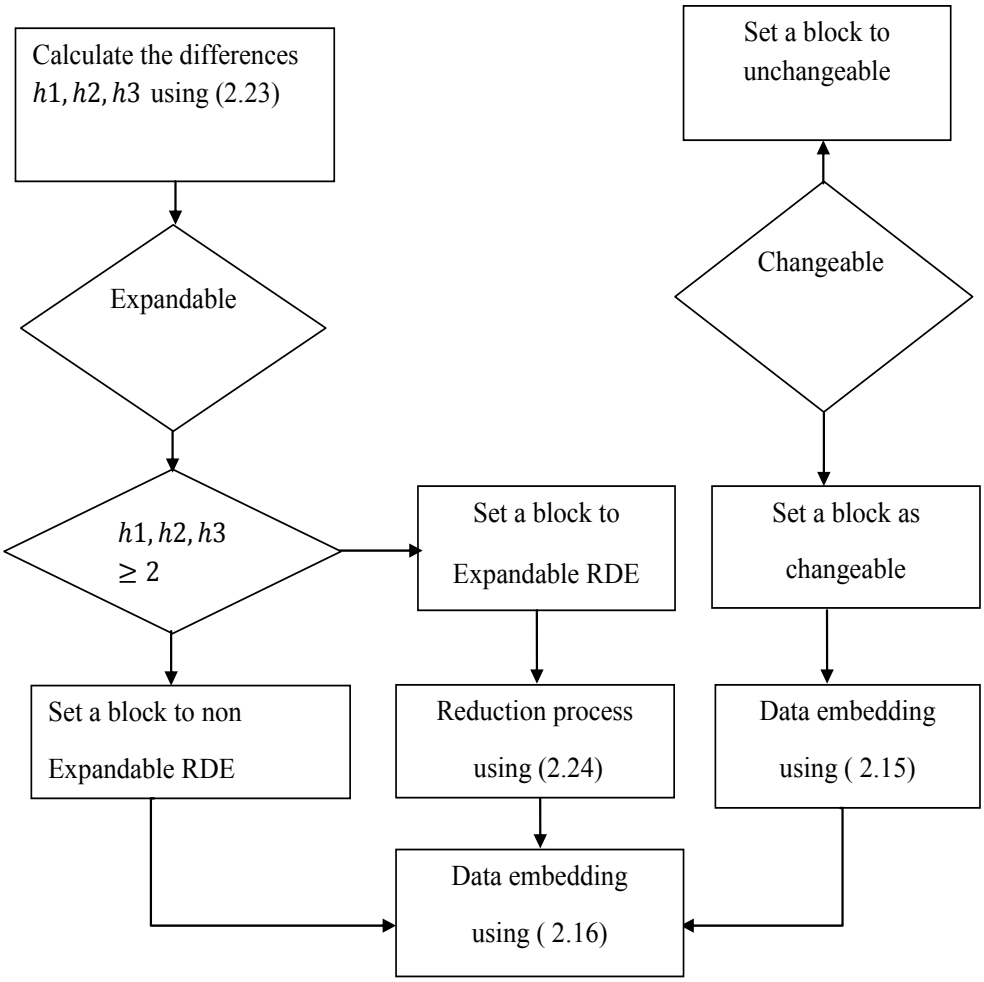

Figure 2. 15 the Embedding flowchart in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)

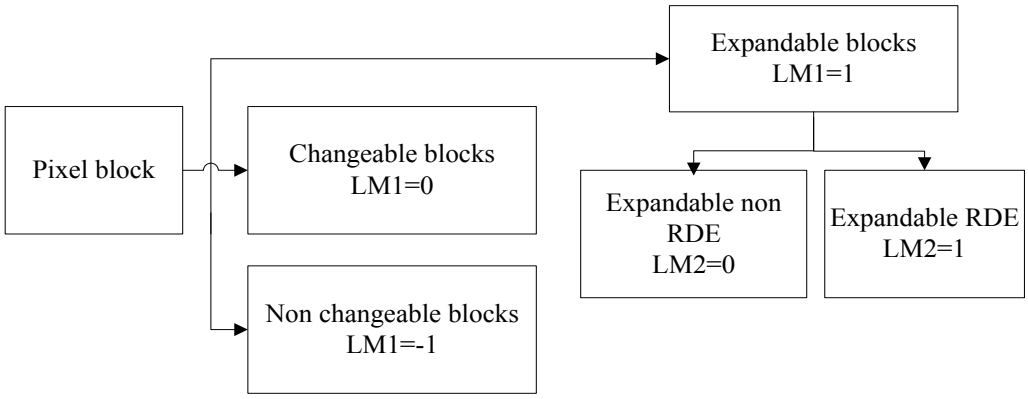

Figure 2. 16 Location map in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)

2.2.7 Increasing the capacity of the secret data using DE pixels blocks and adjusted RDE-based on Grayscale Images

Recently in 2015, a new data hiding method have proposed by (AL_Huti, Ahmad, & Djanali, 2015)where previous method (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) has improved in terms of embedding capacity by using an image block size of sixteen pixels which is seen on Figure 2.17 where it indicates an example of a 4×4 pixel block. This time, one block can contain fifteen differences that means 0.9375 bit per pixel. The difference integer transform function (2.27) and pixel recovery function (2.28) are represented respectively.

$$\begin{cases} h_0 = 0 \\ h_1 = p_1 - p_0 \\ h_2 = p_2 - p_1 \\ h_3 = p_3 - p_2 \\ \quad . \\ \quad . \\ \quad . \\ h_{15} = p_{15} - p_{14} \end{cases} \tag{2.27}$$

$$\begin{cases} p'_0 = p_0 \\ p'_1 = h''_1 + p_0 \\ p'_2 = h''_2 + p'_1 \\ p'_3 = h''_3 + p'_2 \\ \quad . \\ \quad . \\ \quad . \\ p'_{15} = h''_{15} + p'_{14} \end{cases} \tag{2.28}$$

p_0	p_1	p_2	p_3
p_4	p_5	p_6	p_7
p_8	p_9	p_{10}	p_{11}
p_{12}	p_{13}	p_{14}	p_{15}

Figure 2. 17 The example of an image pixel block of 4×4 pixels

To maintain acceptable visual quality of image after embedding, the RDE function proposed by (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) has adjusted to reduce the difference further more (2.29) where the equation become:

$$h''_n = \begin{cases} h_n - \left(2^{\lfloor log_2(h_n) \rfloor} + \lfloor log_2(h_n) \rfloor\right) & if\ h_n > 1 \\ h_n + \left(2^{\lfloor log_2(|h_n|) \rfloor} + \lfloor log_2(h_n) \rfloor\right) & if\ h_n < -1 \end{cases} \quad (2.29)$$

In this year 2017, (Arham, Nugroho, & Adji, 2017) another data hiding algorithm named multilayer data hiding based on difference expansion have developed to increase load capacity. The method combine (Alattar, 2004) integer transform scheme where one pixel become a base point for one layer and form the next layer another pixel become a base point until all pixel in a block are reached. The process is executed sequentially to make a multilayer. The output stego image for one layer becomes the input for next layer and so on. To reduce the distortion after embedding, preprocessing has done using RDE proposed by (Yi, Wei, & Jianjun, 2009). The method increases the embedding capacity however as usual visual quality is decreased.

CHAPTER 3
RESEARCH METHODOLOGY

This chapter discusses about the main steps to be followed in accomplishing this thesis. Any research in academic goes through various steps like literature study, algorithm design, implementation, method testing, result and analysis then prepare the final report. The research activities concerning this thesis are subjected to be finished within five months starting from June until October 2017. The steps in the section of research methodology are illustrated in form of diagram on Figure 3.1

3.1 Literature study

Researches start from the previous works and forward to the next step by improving the existing method or create a new method. The previous works are considered as references used to carry out the research in question.

The references may be journals, conference papers, books or online sources. The information got from the literature can be used and become helpful to define the problem formulation and get more information about the new proposed algorithm. This means literature study must be related to the research topic being studied.

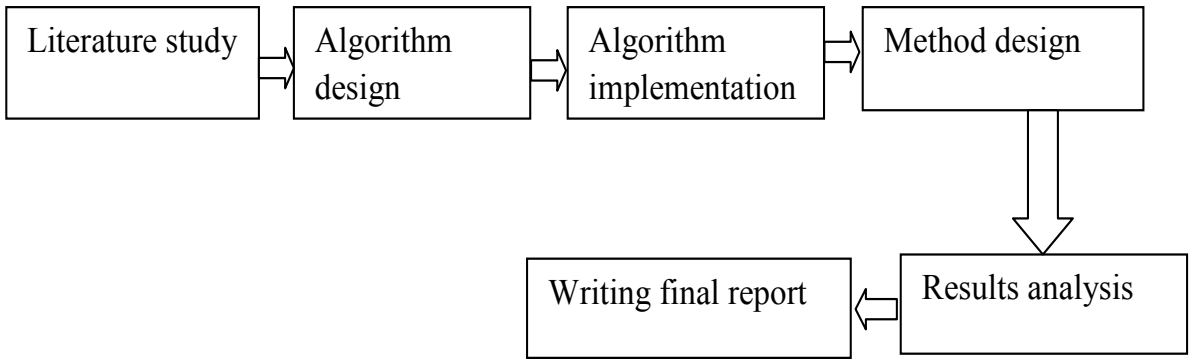

Figure 3. 1 The diagram of research methodology

3.2 Method design

In this research, a new data hiding algorithm that aim to improve the visual quality after secret data embedding within an image for a given payload capacity is presented. The algorithm is based on difference integer transform scheme and a reduced difference expansion.

3.2.1 New integer transform scheme

In the research, an image block size of 2×2 to hide three bits in one pixel block is considered. The new integer transform scheme is computed by considering the base point, which is the second pixel in each quad pixel block. This is the pixel at top right corner in each block. The Figure 3.2 represents the size of pixel block and the corresponding base point to compute the differences. This process is illustrated on equation (3.1)

$$\begin{cases} h_0 = p_0 - p_1 \\ h_1 = 0 \\ h_2 = p_2 - p_1 \\ \vdots \\ h_3 = p_3 - p_1 \end{cases} \tag{3.1}$$

Different from (Ahmad, Holil, Wibisono, & Ijtihadie, 2013), the second difference is zero because the pixel is fixed so $p_1 - p_1 = 0$. This will be used during the extraction because by keeping this difference as zero means that the second pixel is constant then it is subtracted from each pixel in a pixel block.

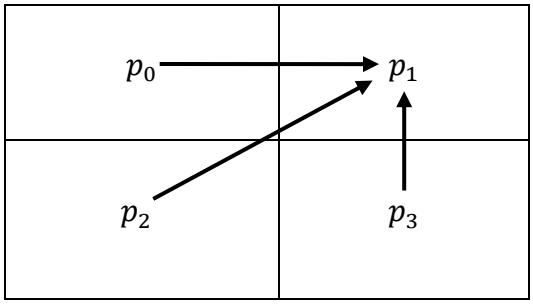

Figure 3. 2 The example of pixel block and the corresponding based point.

3.2.2 New reduced difference expansion

In the past years, various difference reduction processes have been proposed by many researchers for example in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) and in (Kumar, Natarajan, & Muraledharan, 2014). However, none has achieved the optimal quality of stego image. This gives us an intention to propose the difference reduction algorithm in combination of a new proposed integer transform scheme to create a method that gives better performance results compared to the existing method presented in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013). An RDE adjustment algorithm method minimizes the difference to achieve on good quality of stego image. The proposed RDE equation is illustrated in (3.2). In case, the difference between pixels is greater than 1 $(h_n > 1)$, the first expression is used otherwise the second one is applied which is when the difference is less than minus 1 ($h_n < -$). The proposed method goes through out two processes such as embedding process and extraction processes.

$$\begin{cases} h''_n = h_n - \left(2^{\lfloor log_2(h_n) \rfloor - 1} + \left\lfloor \sqrt[\lfloor log_2(h_n) \rfloor]{h_n} \right\rfloor\right), if\ h_n > 1 \\ h''_n = h_n + \left(2^{\lfloor log_2(|h_n|) \rfloor - 1} + \left\lfloor \sqrt[\lfloor log_2(|h_n|) \rfloor]{|h_n|} \right\rfloor\right), if\ h_n < -1 \end{cases} \quad (3.2)$$

$$\forall n \in \mathbb{R}^+, 0 \leq n \leq 3$$

3.2.2.1 The embedding process operation

Similar to other reduced difference expansion algorithm like (Arham, Nugroho, & Adji, 2017) and (Zhengwei, Lifa, Yunyang, Shaozhang, & He, 2017) the embedding process starts by dividing images into pixel blocks. The same as in (Alattar, 2004) the pixel block of four pixels is used to implement the new proposed data hiding method. After dividing the pixels into blocks and compute the difference by subtracting the fixed pixel from each pixel, then difference is saved as vector $h_n = (h_0, h_2, h_3)$ and they are grouped into three categories: expandable, changeable and non-changeable pixel block. The expandable pixel block is itself-categorized into two types such as RDE expandable and non RDE expandable

(Ahmad, Holil, Wibisono, & Ijtihadie, 2013). A pixel block is expandable if the absolute value of the result from the difference between pixels is greater than 2 ($h_n \geq 2$). In (Liu, Lou and Lee, 2007), if a pixel block is in the category of expandable and the difference is greater than 1 ($h_n > 1$), the first part of equation (2.28) is used to compute the reduced difference and when for the difference that is less than minus 1 ($h_n < -1$), the second part of equation (2.28) is used. In this work, the proposed RDE in (2.28) is adjusted and become the expression in (3.1). The same as in (Ahmad *et al.*, 2013), the original difference is reduced if and only if it is greater than 1 ($h_n > 1$) by using the first part of the expression (3.1) while in case the difference is less than minus 1 ($h_n < -1$), the second part is used.

The non changeable pixel block is not used to hide secret data due to the fact that it causes the overflow or underflow issue. After getting the reduced difference the embedding of secret message is done based on the method proposed by (Tian, 2003) which is applied for every difference if a pixel block is in the category of expandable. For expandable RDE, expandable non RDE and changeable pixel block. The location map is required to identify that the embedding has carried out on a specific category. It will help during extraction to locate the type of block and the difference where a secret bit has been inserted. This location map is defined in a vector as follow: $loc = loc_1, loc_2, loc_3, loc_4, loc_5$.

The location map loc_1 is assigned the value $1, 0, -1$ to identify pixel category as expandable, changeable and non changeable respectively while loc_2 takes the value 1 for reduced expandable and 0 for non RDE expandable. If a block is changeable, the embedding is done on the difference without the reduction using the equation in (2.16). in order to identify that during embedding process, the used pixel block was changeable, the location map and the original difference is used as follow: If the difference h_n is odd, the location map from loc_3 to loc_5 be assigned the value 1 else if the original difference h_n is even so the location map from loc_3 until loc_5 are assigned the value 0.

If a block is expandable RDE, the embedding is performed using the equation in (2.15) after the reduction of the original difference. The location map from loc_3 until loc_5 is assigned the value 1 if and only if the first part of expression (3.3) is verified and the location map from loc_3 until loc_5 is given the value 0 if and only if the second part is verified. If a block is expandable non RDE, the embedding is performed on the original difference without a reduction and the location map loc_1, loc_2 are given the value 1 and 0 respectively.

$$\begin{cases} h_n = h''_n \pm \left(2^{\lfloor log_2(h'') \rfloor - 1} + \left\lfloor \sqrt[\lfloor log_2(h''_n) \rfloor]{h''_n} \right\rfloor\right) \\ h_n = h''_n \pm \left(2^{\lfloor log_2(h''_n) \rfloor} + \left\lfloor \sqrt[\lfloor log_2(h''_n) \rfloor]{h''_n} \right\rfloor\right) \end{cases} \quad (3.3)$$

The new pixel is computed using equation (3.4) where the pixel at the second position is not changed and it is added to each embedded difference. The Figure 3.3 represents the overall embedding process in a form of flowchart to illustrate the activity systematically.

$$\begin{cases} p'_0 = h'_0 + p_1 \\ p'_1 = p_1 \\ p'_2 = h'_2 + p_1 \\ \vdots \\ p'_3 = h'_3 + p_1 \end{cases} \quad (3.4)$$

3.2.2.1.1 Embedding flowchart

The embedding flowchart presented on Figure 3.3 shows the overall embedding process from the starting point where an entire image is divided into blocks and secret message is inserted within difference until the end where a stego image is constructed.

3.2.2.2 Extraction process operation

The process of extraction is the process that gives back the secret data and recovers original images that have used as the host of secret message. It is a reverse of embedding process.

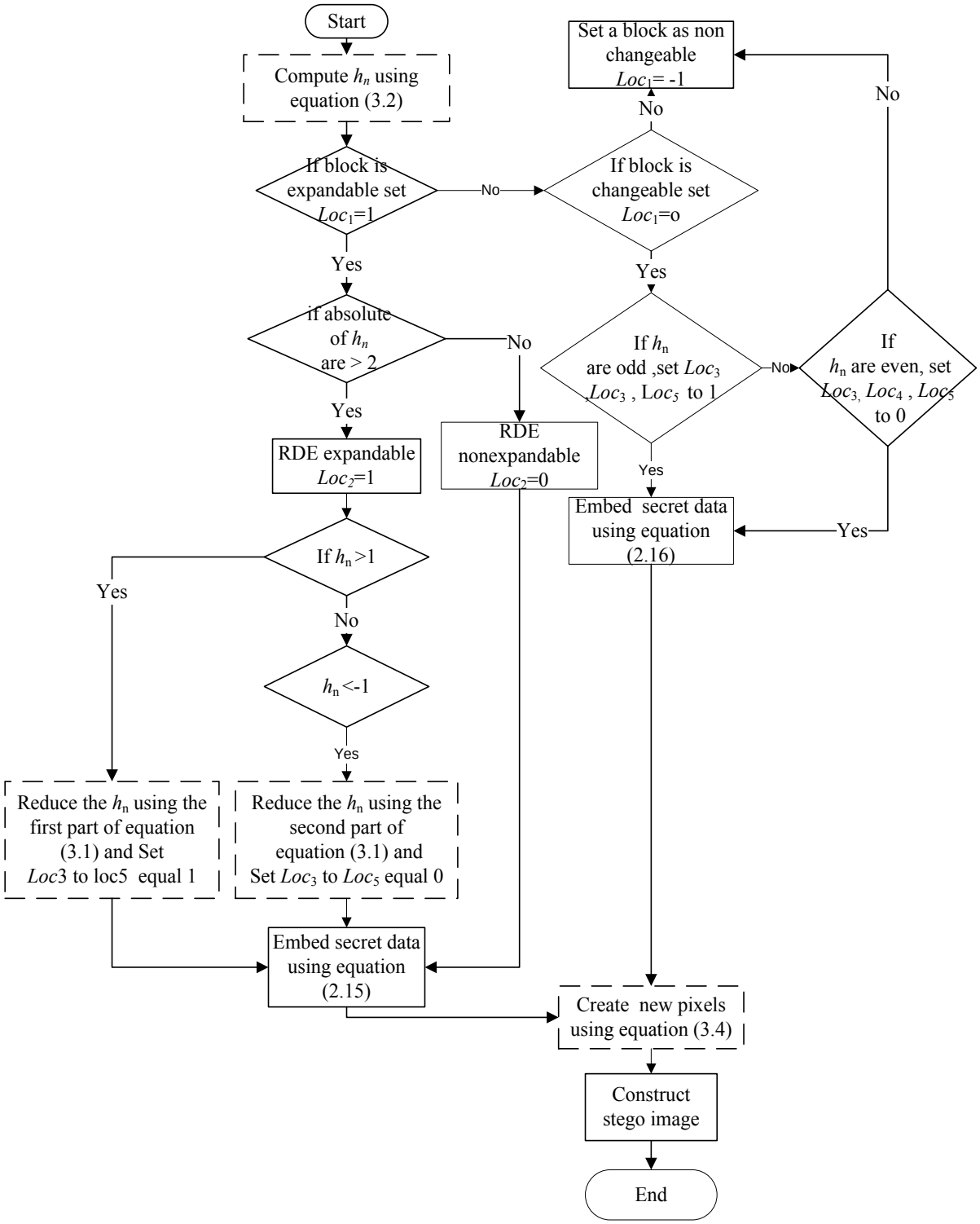

Figure 3. 3 The flowchart of embedding process flowchart

The process starts by dividing stego image into blocks of the same size as the size of pixel block used in the embedding process and compute the differences between the pixels that make stego pixel block. The extraction of secret message is performed directly on the difference by taking least significant bit from each difference. The obtained difference from stego image is the one that have secret message. Therefore, due to the reduction that have performed during embedding process when the block was expandable RDE,

In this new algorithm, similar to (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) if $loc_1 = 1$ and $loc_2 = 1$ the block is expandable RDE while if $loc_1 =$ and $loc_2 =$ the block is considered as expandable non RDE. If the location map is assigned the values -1, the block is said to be non changeable but remember during embedding non changeable block has not used so no need to check it in the extraction process. It is mentioned that expandable block has two parts such as RDE expandable for $h_n >$ and RDE expandable for $h_n < -1$. If the location map from loc to loc are equal to 1, the first part of the expression (3.5) is used else if the location map from loc_3 to loc_5 are equal to 1, the second part is used to get the original difference. The secret message is recovered by applying *LSB* (.) on h''_n as equation (3.6).

$$\begin{cases} h_n = h''_n + 2^{\lfloor log_2(|h''_n|)\rfloor - 1} + \left\lfloor \sqrt[\lfloor log_2(h''_n)\rfloor]{h''_n} \right\rfloor \\ h_n = h''_n + 2^{\lfloor log_2(|h''_n|)\rfloor} + \left\lfloor \sqrt[\lfloor log_2(h''_n)\rfloor]{h''_n} \right\rfloor \end{cases} \tag{3.5}$$

$$s_i = LSB(h''_n) \tag{3.6}$$

If a pixel block is non RDE expandable, the formula proposed by Alattar in (Alattar, 2004) is used to recover the original differences as mentioned below on the expression (3.7). If the block is changeable and the location map from loc_3 to loc_5 are 0 and the difference is even, the original difference is recovered using the first expression in (3.8) and if the location map from loc_3 to loc_5 are 0 and if the difference is odd, the second equation (3.8) have used to give back the original difference.

$$h_n = \left\lfloor \frac{h''_n}{2} \right\rfloor \tag{3.7}$$

$$\begin{cases} h_n = \left\lfloor \frac{h''_n}{2} \right\rfloor \\ h_n = \left\lfloor \frac{h''_n}{2} \right\rfloor + 1 \end{cases} \tag{3.8}$$

The secret message is obtained by computing least significant bit of the difference h'_n . The original image is reconstructed using the equation (3.9) where p_n, h_n , p'_n is original pixel, original difference and stego pixel respectively.

$$\begin{cases} p_0 = h_0 + p'_1 \\ p_1 = p'_1 \\ p_2 = h_2 + p'_1 \\ \quad . \\ p_{n-1} = h_n + p'_1 \end{cases} \tag{3.9}$$

3.2.2.2.1 Extraction flowchart

The extraction flowchart on Figure 3.4 illustrates the step by step to extract secret message and recover original image. It starts by dividing stego image into blocks and end by reconstructing original image.

3.3 Algorithm implementation

In this section, the environment in which the designed data hiding algorithm implementation took place is described. This includes computer specifications, software and dataset, which is composed on medical and common image dataset. In addition, the obtained results for different size of embedded data are discussed.

3.3.1 The dataset description

In this section, the details of the dataset images used to hide in secret data is given. We provide the resolution, the block size and talk about the secret message to be use to test the performance of the new proposed method. In the implementation, five grayscale medical and five different common images are used.

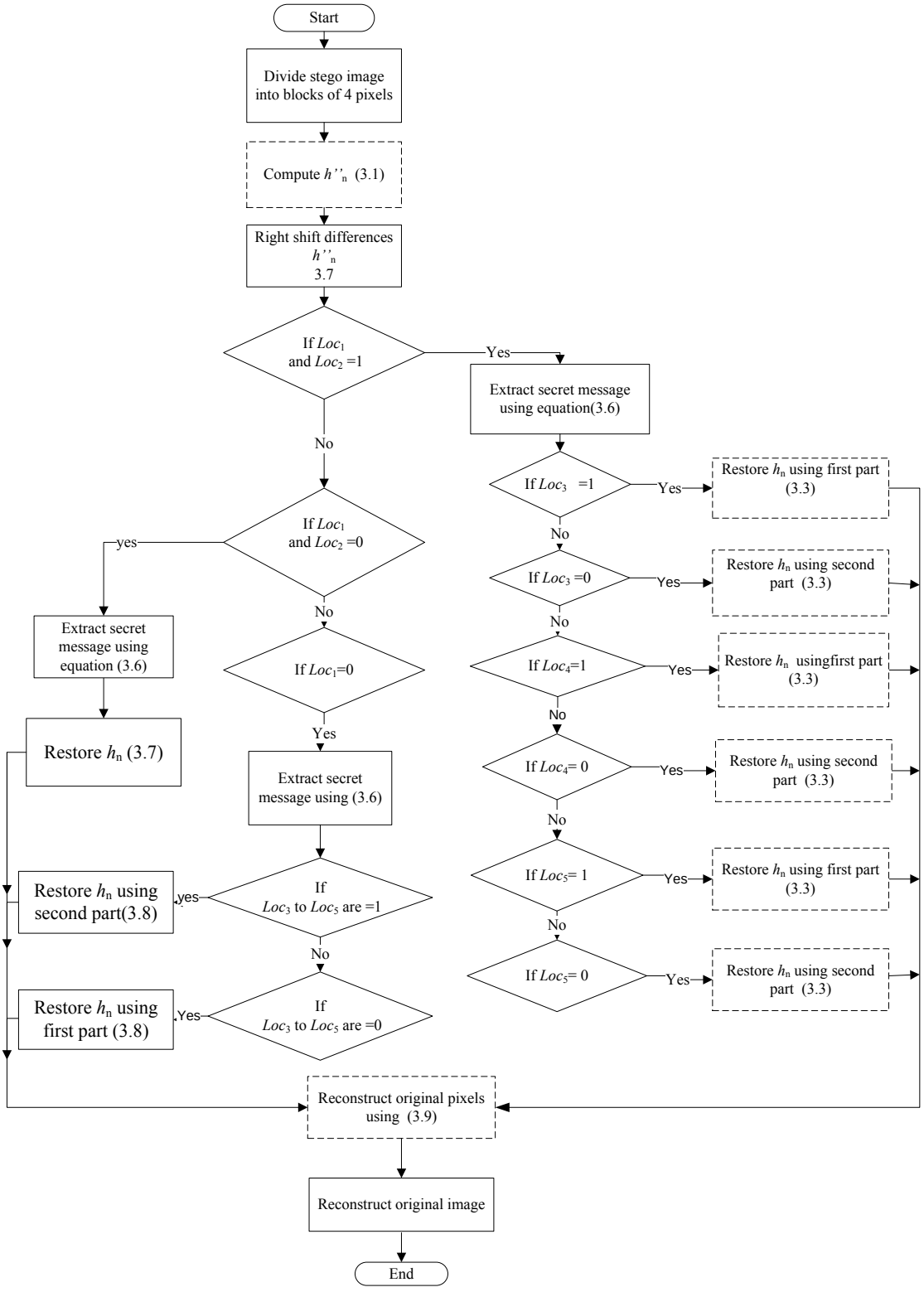

Figure 3. 4 The secret and original image extraction and recovery flowchart

The example of medical images is presented on Figure 3.5 while the example of common images is presented on Figure 3.6. The medical images are images that represent body parts of human being.

These are images commonly used in medical environment during patient diagnosis. The process involves radiography where the human body parts are scanned then health practitioners analyze picture. Hence, in current technology especially in telemetry patient data can be share through sharing the picture with specific patient record for better diagnosis. In this thesis, the used medical grayscale image of resolution 512×512 are taken from (Partners infectious disease images- emicrobes Digital Library, 2017).

The common images are images that are taken for no specific purpose. This includes image of object, people or anything photographed. The images used in this work are available at (Weber, 1977). These images can be used in data hiding to protect their copyright by inserting the information with no relationship with the image. The medical images to be used are leg, head, hand, chest and abdominal respectively. All images are of type jpeg while for common images are Baboon, Elaine, Lena, Boat and pepper which are of types tiff.

The secret message is randomly generated using MATLAB function called randi. The message is in binary format. These binary bits are considered as secret message because as we know, any message needs to be converted into digital format (1 or 0) before it is being used in digital system.

3.3.2 Algorithm testing and evaluation

In this section, the details about the testing of the method where we talk about the environment in which we run the method are provided and discussion about parameter are considered in order to evaluate the performance of the designed algorithm.

Leg Head Chest

Figure 3. 5 the example of gray medical images

Baboon Boat Pepper

Figure 3. 6 The example of grayscale images

3.3.2.1 The testing environment

This method is tested using different tools such as software and hardware. On the hardware side, the method was tested in a laptop computer of HP Compaq that has Intel motherboard and a processor of 2.24Hz Intel Celeron. The storage capacity of this computer is 320 GB and its volatile memory (RAM) is 4GB. On another side, the software used are mainly the window operating system 2007, Microsoft office 2007 and MATLAB as the programming language.

3.3.2.2 The method evaluation parameters

In this part, the parameters considered to decide that the proposed method is performing well compared to the previous method are illustrated. The evaluation considers the visual quality of stego image after the embedding data inside the

original image. It is represented by the Peak Signal to Noise Ratio (PSNR), which indicates the level of distortion in the stego image compared to original image. If there is no modification between stego image and original image, PSNR value tends to infinite. Therefore, the higher PSNR value is the more the quality of stego image. The PSNR value depends on the value of means square error (MSE). This is the error between the original image and the image with embedded data. The formula to compute PSNR and MSE are illustrated on (3.10) and (3.11) respectively. Where *N*: is the number of pixels present in the image, I_i is the original image while I'_i is the stego image.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(I_i - I'_i)^2 \quad (3.10)$$

$$PSNR = 10 \times log_{10}\frac{255^2}{MSE} \quad (3.11)$$

From many researches, it has been clearly observed and proved that the higher is PSNR value, the better is the method. The obtained results are analyzed for different images used to see if the proposed method performs better based on visual quality for a specific payload capacity. Moreover, the result produced by the new method is compared to the results from the previous method to prove the performance of the new designed algorithm.

3.4 Activity schedule

The remaining part is the representation of the time schedule to accomplish this task. The Figure 3.6, shows that the entire task will take five months starting from June until October 2017. Each research activity will take at least one month to be terminated as it is indicated by the highlighted section in green. After performing all the activities in chapter 3, it will be a time to write the final report. This report will describe all the steps that have performed to achieve on the obtained results. These are the basic theory, literature methodology, and implementation. Thereafter the results will be discussed and give the conclusion.

Activity	Months																			
	June				July				August				September				October			
Literature study																				
Algorithm design																				
Implementation																				
Testing &evaluation																				
Result analysis																				
Writing final report																				

Figure 3. 7. Project Activity from May to October

CHAPTER 4
RESULTS AND DISCUSSION

In this chapter, first the results from the implementation of our designed and previous algorithm are presented. Secondly, they are interpreted and discussed by proving that the new proposed method performs better for many extends when compared to previous method.

4.1 Results

These results are presented using three different tables after the algorithm implementation where each table contains the results obtained when different embedding capacity is hidden. For example, by evaluating the proposed method on medical images, we can see that Table 4.1 contains the PSNR values obtained by hiding 5 kilobyte of secret message. In Table 4.2, the presented results are the one obtained when the embedding capacity of 10 kilobyte is hidden while in Table 4.3, the presented results are gained for a 20 kilobyte embedded within different medical images. Similar to common images, the results can be seen in Table 4.4 when 5kb is hidden, Table 4.5 for 10 kb and Table 4.6 where 20 kb of secret bits are embedded.

4.2 Discussions

From the presented results, we realized that the performance of the proposed methods is better for Lena and Elaine image on the side of common images while on the side of medical images, the performance is better for chest followed by abdominal image. The highest performance is obtained on chest image when the secret message of 5kb is embedded. Here, the performance increase is about 1.87 dB compared to previous algorithm proposed in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013). With the same embedding capacity, the lowest performance is observed for head image where the increase is about 1.256 dB. Here, the new proposed method still performed well even though PSNR value decreases compared to chest image. This is shown in Table 4.1. In Table 4.2, the embedding capacity has changed from 5 kb to 10 kb. It is

clear that by increasing embedding capacity, the quality of stego image decreases. Here, the performance is still better for chest image for both methods and the proposed method performs well.

Table 4. 1 The PSNR value obtained by hiding 5 kb of secret bits in medical images

Images	Previous method in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)	Proposed method
	PSNR(dB)	PSNR(dB)
Abdominal	40.219	40.999
Leg	40.0875	40.518
Head	33.6507	34.906
Hand	39.8570	40.386
Chest	40.7396	42.609
Average	38.89814	39.883

Table 4. 2 The PSNR value obtained by hiding 10 kb of secret bits in medical images

Images	Previous method in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)	Proposed method
	PSNR(dB)	PSNR(dB)
Abdominal	37.6781	38.715
Leg	38.0088	39.137
Head	31.9048	33.054
Hand	37.5563	38.130
Chest	38.0617	39.685
Average	36.6419	37.744

Table 4. 3 The PSNR value obtained by hiding 20 kb of secret bits in medical images

Images	Previous method in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)	Proposed method
	PSNR(dB)	PSNR(dB)
Abdominal	37.6805	38.717
Leg	38.0537	39.135
Head	31.9050	33.046
Hand	37.5609	38.131
Chest	38.0634	39.6861
Average	36.6527	37.743

Performance is still better for chest image for both methods and the new method performs well. The highest increase is about 1 dB and the worst PSNR value is always present for head image nevertheless, the increase is 1.1 dB and this still indicates the strength of a new algorithm.

The same results are presented in Table 4.3 where the embedding capacity of 20 kb has embedded in different medical images. The visual quality for chest image is the most excellent while the nastiest performance is gained from head image.

By comparing the performance of new algorithm when different embedding capacity are hidden using the same image (here we choose chest image), we can see that the visual quality decreases when the size of secret message increases. This can be seen on Figure 4.1 where it is applicable for both previous and new proposed method.

In this designed algorithm, the main objective of insuring the security of data during transmission by using data hiding to hide the existence of secret information within media file from adversary have achieved.

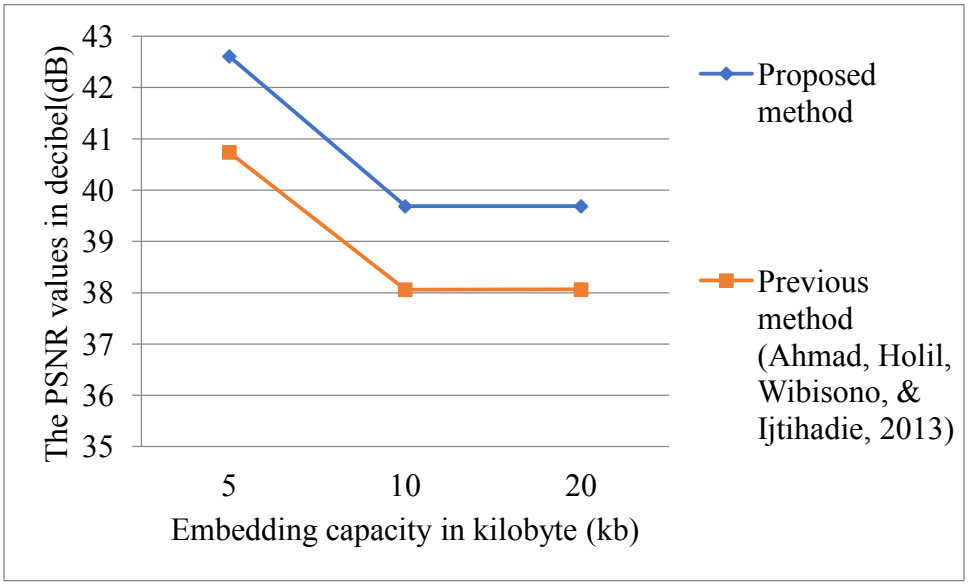

Figure 4. 1.The performance comparison between the proposed method and that in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) based on PSNR values for chest image

This can be seen on Figure 4.2 where after hiding 20 kb of secret message, it not possible to notices that the stego file contains data by using naked eyes even though changes can be seen using other techniques.

In the following section, the performance of both previous and new designed algorithm is performed based on the average of visual quality for both methods when secret message of difference size is embedded within medical images then comparison is made.

Therefore, we can remark that the visual quality decreases as long as the embedding capacity increases and new algorithm also performs well. This can be seen on Figure 4.3 where the obtained results when the algorithms are implemented on common images are shown in Table 4.4 for 5 kb of secret message and in Table 4.5, Table 4.6 for 10 and 20 kb of secret message respectively.

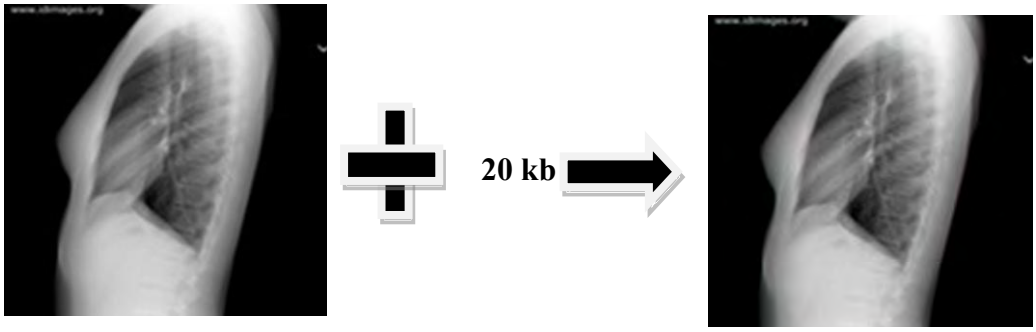

Figure 4. 2. Chest image before and after embedding 20 kb of secret message

In these results, the visual quality is low when comparing to the implementation of the algorithms on medical images. This is because they are of different nature and their intensity (the value of pixels) is different. This may results to that many non-changeable pixel blocks that are present in medical images than in common images. Here, we can mention that, the more non-changeable pixel block are present, the high PSNR value is gained.

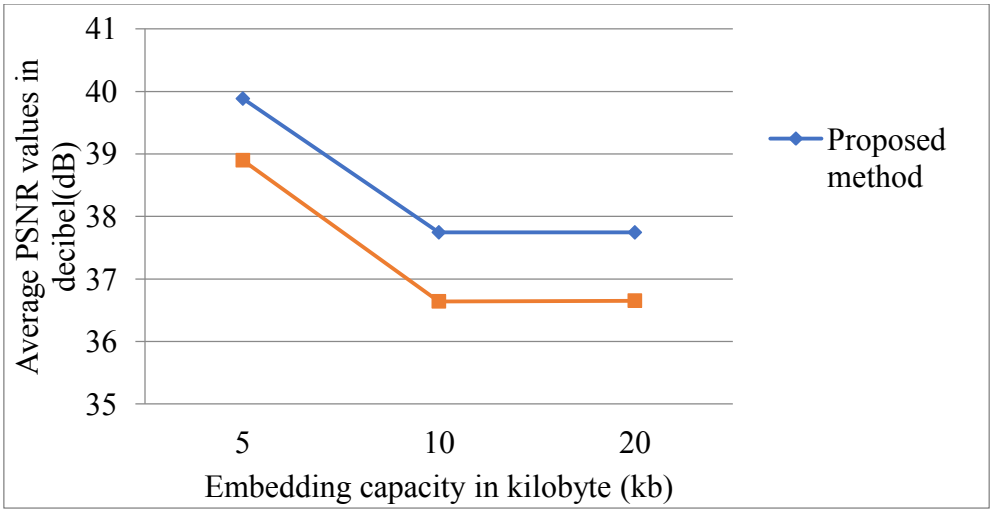

Figure 4. 3. The Comparison between the proposed method and that in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) based on the average performance for all medical images

This because more pixels will be used to carry secret message and in case few non changeable pixel block are present, there is a high probability that more pixel will

involve in transporting secret bits. This might be the cause of low PSNR value for common images.

In Table 4.5, the 10 kb of secret message was embedded and the performance is better for Elaine image where the increases performance of 0.8 is obtained and a new algorithm still performs better. Again, the stego pixel cannot be suspected to carry secret message by means of human vision system. This can be seen on Figure 4.4 where 20 kb were embedded within baboon image and the appearance is as the same as the original baboon image.

The performance comparison for a common image when difference size of secret message is used is done using Lena image and the results shown that the performance of these two methods is different where the new proposed method performs better than the previous. This is plotted on Figure 4.5 where the high performance is observed for small embedding capacity (5kb) and low performance is seen for high embedding capacity (20kb).

Table 4. 4 The PSNR value obtained by hiding 5 kb of secret bits in common images

Images	Previous method in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)	Proposed method
	PSNR(dB)	PSNR(dB)
Pepper	28.719	29.466
Baboon	22.317	23.120
Lena	31.079	31.968
Elaine	30.999	30.093
Boat	26.901	27.705
Average	28.003	28.470

Table 4. 5The PSNR value obtained by hiding 10 kb of secret bits in common images

Images	Previous method in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)	Proposed method
	PSNR(dB)	PSNR(dB)
Pepper	27.0988	28.115
Baboon	20.6956	21.671
Lena	28.4768	29.778
Elaine	28.9600	29.778
Boat	25.7041	26.669
Average	26.186	26.996

The average performance of the new proposed algorithm and the previous algorithm for all common images is represented on Figure 4.6. It demonstrates that the new algorithm improves the performance and high performance is clearly obtained for small secret size, which is 5 kb, and low performance is found for many secret bits embedded in common images.

The performance of designed algorithm maybe affected by many factors including the nature of image it also depends on the arrangement of pixels and the secret message bits embedded. For example in case the embedded bits is 1 and another bits is 0, the change in pixel after bit insertion to the original difference is different which may results to different PSNR value that characterize the visual quality evaluation criteria.

Table 4. 6 The PSNR value obtained by hiding 20 kb of secret bits in common images

Images	Ahmad et al. (Ahmad, Holil, Wibisono, & Ijtihadie, 2013)	Proposed method
	PSNR(dB)	PSNR(dB)
Pepper	27.0985	28.114
Baboon	20.6953	21.670
Lena	28.4761	29.780
Elaine	28.755	28.9590
Boat	25.7039	26.672
Average	26.1800	26.998

In this research, we also discovered that the performance of a data hiding algorithm based on a reduced difference expansion does not only depends on difference reduction process but also on the choice of base point during the computation of original differences. This is due to that reduced difference expansion depends on difference expansion. Therefore, bad choice of base point may results to the rejection of many pixel blocks, which may not contribute in carrying secret message bits. Hence, a combination of a reduced difference expansion and a better base point results to high performance in terms of visual quality for a given embedding capacity.

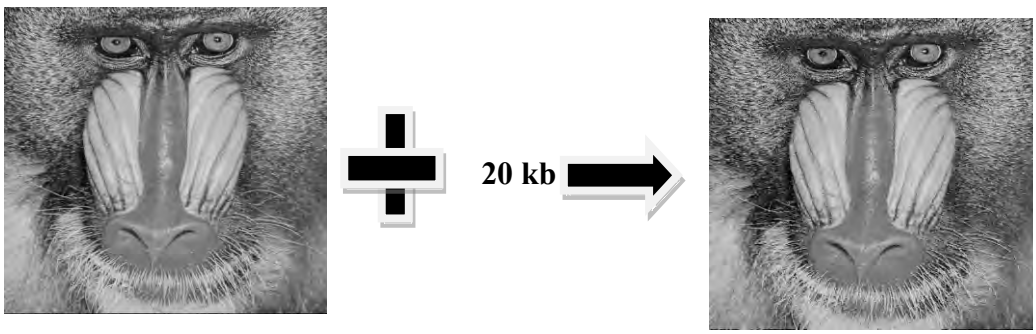

Figure 4. 4. Baboon image before and after embedding 20 kb of secret message

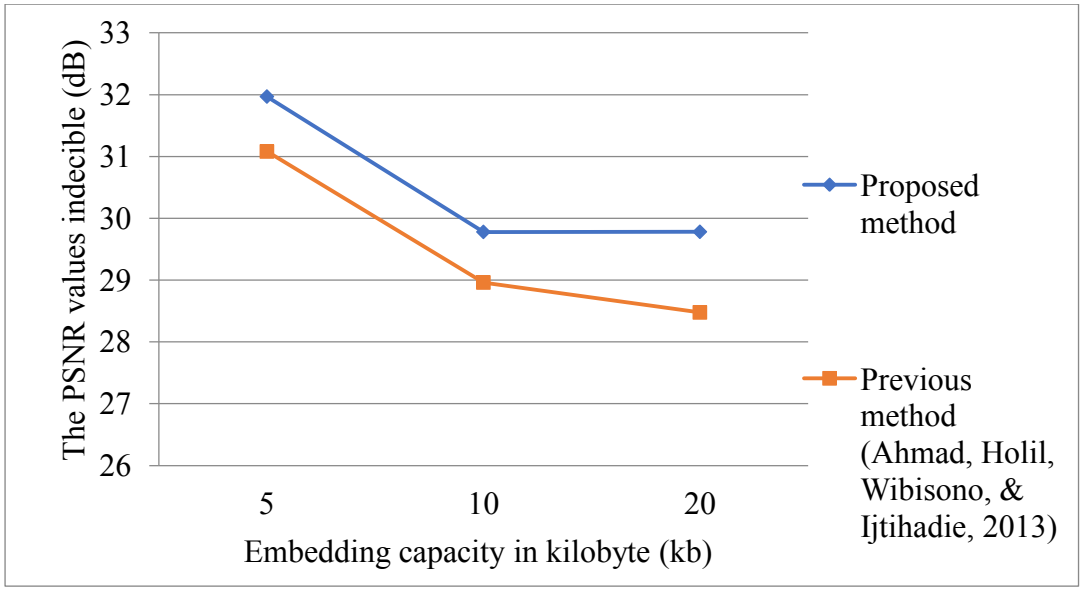

Figure 4. 5. The performance comparison based on PSNR value for Lena Image

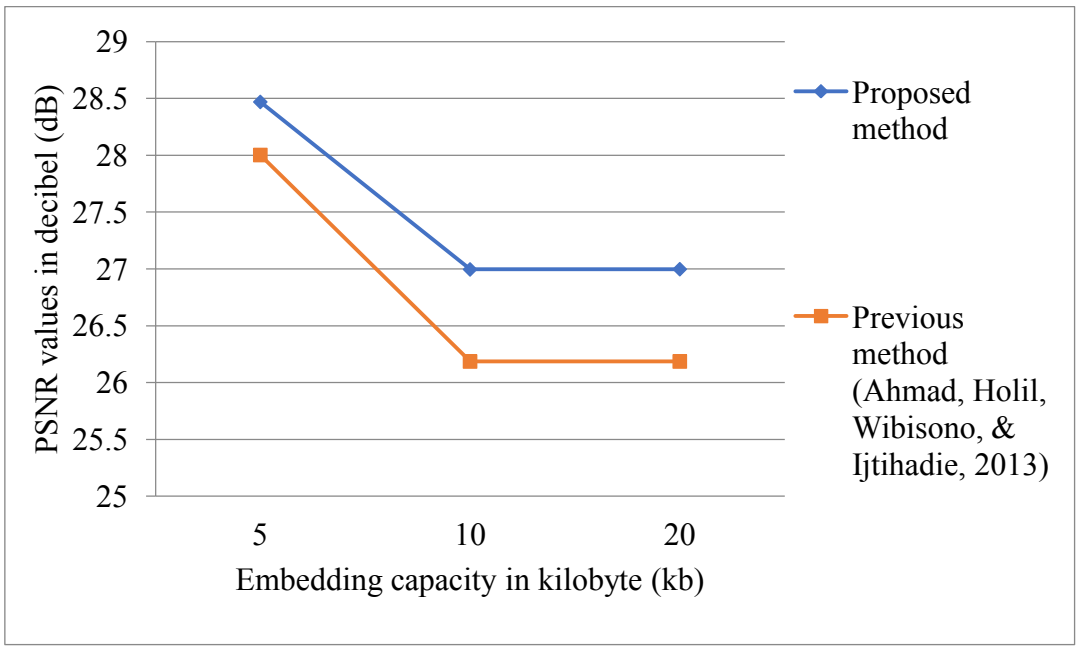

Figure 4. 6. The performance comparison based on average PSNR value for all common images

4.3 Summary

In this thesis, a new integer transform scheme and a new reduced difference expansion were proposed. The implementation have been done using medical and common image datasets. The secret message of different size (5Kb,10Kb and 20Kb) was embedded in each image and the the average performance was evaluated. The obtained results demonstrate that the performance is high for medical images. The comparison of the proposed method and that in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) was done .

The performance is better for chest image (40.7396 dB), (42.609 dB) when a secret message of 5kb is embedded while its low for head image (33.6507dB),(34.906 dB) for previous method in (Ahmad, Holil, Wibisono, & Ijtihadie, 2013) and the proposed one respectively. The results is still the same for common images eventhough the quality is reduced compared to the medical images where the performance is hight for Lena (31.079 dB), (31.968dB) and low for baboon (22.317 db), (23.120 dB) respective to previous and the proposed method. This is applicaable for all secret size. Consequently, we remark that as long as the payload capacity increases, the quality of stego image decreases gradually and depends on the used image. This is due to the nature of images influenced by the intensity of pixels (high intensity (white) and low intesity (black)). As in gray scale images the pixel values are inbetween 0 and 255, in cased the images body tends to white, it affects the computed difference which also affected the PSNR values. Hence, common images have low visual quality.

Again, the proposed method performs better due to that, first my propoed reduced difference expansion balanced the difference reduction instead of high reduction because the reduction is peformed in both positive and negative values of difference. However, it is clear that the positive values are reduced while the negative values are increased. In fact, it is as if there is no redcution. So a good base point and a balanceed reduced difference expansion is required to achieve on high performance.

CHAPTER 5
CONCLUSION AND RECOMMENDATION

In this chapter, we draw out conclusion based on the obtained results from chapter 4. Then, we give suggestion to the next researchers to continue the search in data hiding field by designing a data hiding algorithm that may perform better than the one in this thesis.

5.1 Conclusion

In this thesis, an integer transform scheme base on a fixed pixel value in a block of four pixel combined with a reduced difference expansion were applied on different types of grayscale image dataset such as common and medical images. The obtained results demonstrate that:

1. The visual quality is improved for almost all images and the performance depends on the amount of secret data hidden in a specific image.
2. The visual quality decreases as long as the embedding capacity increases and the quality of stego image is directly proportional to the payload capacity where increasing one entity decreases another and verse versa.

We also realized that the nature of image affects the performance of a data-hiding algorithm. This is mainly caused by the pixel intensity which maybe different from one image to another.

5.2 Recommendation

Based on the results, we recommend that during the design of a data-hiding algorithm, the properties of cover media and its types should be considered. The presented algorithm can be improved by proposing another integer transform scheme and a better reduced difference expansion based on the properties of the cover media. These properties are either smoothness or roughness of image.

For example, a new proposed method could be evaluated on common images so that the improvement of the visual quality of stego image can be achieved. This is because a good embedding capacity is the one that may totally confuse the adversaries and allow high embedding capacity. On the side of medical images as cover media, the method can be also in terms of embedding capacity by applying a multilayer data hiding algorithm of the method in this thesis. Therefore, high embedding capacity maybe achieved by hiding more than one bit in a pixel.

BIBLIOGRAPHY

Ahmad, T., & Holil, M. (2014). Increasing the Performance of Difference Expansion-based Steganography when Securing Medical Data. *Smart Computing Review , 4* (4), 307-322.

Ahmad, T., & Holil, M. (2015). Secret Data Hiding by Optimizing General Smoothness Difference Expansion Based Method. *Journal of Theoretical and Applied Information Technology* , 155-163.

Ahmad, T., Holil, M., Wibisono, W., & Ijtihadie, R. M. (2013). An improved quad and RDE-based medical data hiding method. *Computational Intelligence and Cybernetics* (pp. 141-145). Yogyakarta, Indonesia: IEEE.

Ahmad, T., Holil, M., Wibisono, W., & Ijtihadie, R. M. (2013). An improved quad and RDE-based medical data hiding method. *Computational Intelligence and Cybernetics* (pp. 141-145). Yogyakarta, Indonesia: IEEE.

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. *International Conference on Information, Communication Technology and System* (pp. 225-230). Surabaya,Indonesia: IEEE.

Al-Afandy, K. A., Faragallah, O. S., & Elmhalawy, A. (2016). High security data hiding using image cropping and LSB least significant bit steganography. *Information Science and Technology. 3*, pp. 34-38. Tangier, Morocco: IJERA.

Alattar, A. M. (2003). Reversible Watermak Using Differenc Expansion of Triplets. *IEEE* , 501-504.

Alattar, A. M. (2004). Reversible watermark using difference expansion of quads. *IEEE Transactions on Image Processing , 13* (8), 1147 - 1156.

Alexander. (2016, March 17). *Symetric key cryptography.* Retrieved from http://alexander.holbreich.org/symmetric-key-cryptography/

Al-Qershi, O. M., & Ee, K. B. (2009). An Overview of Reversible Data Hiding Schemes based on Difference Expansion Technique. *First International Conference on Software Engineering & Computer Systems.* Penang, Malaysia.

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

Chakraborty, S., Jalal, A. S., & Bhatnagar, C. (2013). Secret image sharing using grayscale payload decomposition and irreversible image steganography. *Journal of Information Security and Applications , 18* (4), 180–192.

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

Goel, S., Gupta, S., & Kaushik, N. (2014). Image Steganography – Least Significant Bit with Multiple Progressions. *ProceInternational Conference on Frontiers of Intelligent Computing: Theory and Applications. 2*, pp. 105-112. Switzerland: Springer.

Govind P.V, S., M.K, S., & Varghese, B. M. (2015). A two stage data hiding scheme with high capacity based on interpolation and difference expansion. *International Conference on Emerging Trends in Engineering, Science and Technology. 24*, pp. 1311 – 1316. Science Direct(ICETEST).

Hua, Z., Shoujian, D., & Daozhen, Z. (2010). A reversible watermarking scheme for vector drawings based on difference expansion. *Computer-Aided Industrial Design & Conceptual Design* (pp. 1441-1446). Yiwu, China: IEEE.

Huang, C.-H., Chuang, S.-C., & Wu, J.-L. (2008). Digital invisible-Ink data hiding based on spread-spectrum and quantization techniques. *IEEE Transactions on multimedia , 10* (4), 557-569.

Kumar, V., Natarajan, & Muraledharan, S. (2014). Difference expansion based reversible data hiding for medical images. *nternational Conference on Communication and Signal Processing.* India: IEEE.

Liu, C.-L., Lou, D.-C., & Lee, C.-C. (2007). Reversible data embedding using reduced difference expansion. *Intelligent Information Hiding and Multimedia Signal Processing* (pp. 890-896). Kaohsiung, Taiwan: IEEE.

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems* .

Partners infectious disease images- emicrobes Digital Library. (2017, April). Retrieved from www.idimages.org: www.idimages.org

Patel, N., & Meena, S. (2016). LSB based image steganography using dynamic key cryptography. *Emerging Trends in Communication Technologies. 85*, pp. 62-69. Dehradun, India: IJACSA.

Por, L. Y., & Delina, B. (2008). Information hiding: A new approach in text steganography. *International Conference on Applied Computational Science.* Hangzhou, China.

Saroj, S. K., Chauhan, S. K., & Sharma, A. K. (2015). Threshold cryptography based data security in cloud computing. *International Conference on Computational Intelligence & Communication Technology*, *387*, pp. 53-55. Ghaziabad, India.

Shaik, A., Thanikaiselvan, V., & Amitharajan, R. (2017). Data Security Through Data Hiding in Images: A Review. *Journal of Artificial Intelligence* , 1-21.

Tian, J. (2003). reversible data embedding using difference expansion. *IEEE transaction , 13* (8), 890 - 896.

Tian, J. (2003). reversible data embedding using difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology , 13* (8), 890 - 896.

Weber, A. (1977). (USC-SIPI) Retrieved October 2017, from http://sipi.usc.edu/database/database.php?volume=misc

Yi, H., Wei, S., & Jianjun, H. (2009). Improved reduced difference expansion based reversible data hiding scheme for digital images. *International Conference on Electronic Measurement & Instruments*, (pp. 315-318). Beijing, China.

Zhengwei, Z., Lifa, W., Yunyang, Y., Shaozhang, X., & He, S. (2017). An improved reversible image watermarking algorithmbased on difference difference expansion. *International Journal of Distributed Sensor Networks* .

AUTHOR'S BIOGRAPHY

Maurice Ntahobari is the elder son in a family of seven children composed on three boys and four girls. He was born in Kirehe district in Rwanda's Eastern province on 23rd June 1985. He was born by matrimonial family made of Faustin Mukeshimana and Beatrice Nyirabaganga. The author studies High School in Mathematics and Physics at Nyamagabe Secondary school of science. He studied his bachelor at National University of Rwanda where he followed Computer Science and Systems. He obtained his Bachelor of Science in computer science and systems with second class Honors, upper division in the graduation ceremony held at University of Rwanda on 28th/08/2013. From 2012 until 2015, he was working as IT instructor at Groupe Scolaire de Gishubi. The author has married with Cecile Mushimiyimana on 20th/12/2014 and up to now, he is a legendary of one bit of son and wife. In 2015, the author decided to upgrade his studies where he went in the republic of Indonesia at Institut teknologi Sepuluh Nopember Surabaya where he studies Indonesia language (Bahasa indonesia) within One year thereafter he joined Masters program in department of informatics engineering with his level of expertise in Network Centric computing (NCC). The author has successfully completed his graduate studies in March 2018.