Dynamic Key Based Approaches for Security Amelioration in Spatial Domain Image Steganography

Thesis submitted to Pondicherry University in partial fulfillment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

in

COMPUTER SCIENCE AND ENGINEERING

by

P.THIYAGARAJAN

DEPARTMENT OF COMPUTER SCIENCE
SCHOOL OF ENGINEERING AND TECHNOLOGY
PONDICHERRY UNIVERSITY
PUDUCHERRY – 605014

AUGUST 2013

DEDICATED

To

My beloved Parents

Mr.V.S.Paramasivan and Mrs.P.Kamala

and to the soul of

My Grandparents

Mr.T.Sivagurunathan and Mrs.S.Thamaraichelvi

CERTIFICATE

This is to certify that this thesis titled "**Dynamic Key Based Approaches for Security Amelioration in Spatial Domain Image Steganography"** submitted by **Mr.P.Thiyagarajan**, to the Department of Computer Science, School of Engineering and Technology, Pondicherry University, Puducherry, India for the award of the degree of **Doctor of Philosophy** in **Computer Science and Engineering** is a record of bonafide research work carried out by him under my guidance and supervision.

This work is original and has not been submitted, in part or full to this or any other University / Institution for the award of any other degree.

Place :Puducherry
Date :

Prof. G. Aghila., B.E.(Hons)., M.E., Ph.D.
(Guide & Supervisor)
Department of Computer Science
School of Engineering and Technology
Pondicherry University
Puducherry – 605 014
India.

DECLARATION

I hereby declare that this thesis titled "**Dynamic Key Based Approaches for Security Amelioration in Spatial Domain Image Steganography"** submitted to the Department of Computer Science, School of Engineering and Technology, Pondicherry University, Puducherry, India for the award of the degree of **Doctor of Philosophy** in **Computer Science and Engineering** is a record of bonafide research work carried out by me under the guidance and supervision of **Prof. G. Aghila.** This work is original and has not been submitted, in part or full to this or any other University / Institution for the award of any other degree.

Place: Puducherry **P.Thiyagarajan**

Date:

ACKNOWLEDGEMENTS

The journey to my Ph.D. embarked upon in the year 2010 with anxiety; a journey to the realm unknown and foreign. Yet it was a journey filled with knowledge and wisdom. It marks a period in my life that has given me a vision to tread upon many more such ventures and strength to dare aspire for more.

"Ideal teachers are those who use themselves as bridges over which they invite their students to cross, then having facilitated their crossing, joyfully collapse, encouraging them to create bridges of their own."

– Nikos Kazantzakis

The above statement perfectly suits for my Ph.D. research supervisor and SSE Project Joint Investigator, ***Prof. G. Aghila,*** Department of Computer Science, School of Engineering and Technology, Pondicherry University. I would like to express her my deep and sincere gratitude. She initiated me into this challenging field by providing me with essential knowledge and grounding. Sustaining and developing my interest in it by her constant examination of my work, she also enriched it with her valuable comments and suggestions. With her perceptiveness, intelligence, erudition and most of all, her patience, she has been always a source of inspiration and guidance at every step of my research work. I would have been lost without her.

Also I would like to thank my doctoral committee members ***Dr. V. Prasanna Venkatesan***, Associate Professor and SSE Project Joint Investigator, Department of Banking Technology, Pondicherry University and ***Dr. G. Ayyappan***, Professor, Department of Mathematics, Pondicherry Engineering College for their critical suggestions and support which made possible the completion of my thesis.

I thank ***Prof. S. V. Raghavan,*** Chief Investigator of the Collaborative Directed Basic Research on Smart and Secure Environment Project (CDBR-SSE) sponsored by National Technical Research Organisation (NTRO), New Delhi, for providing me an opportunity to work in this project. Many thanks to SSE Joint project investigators, Pondicherry University, for recognizing my potential by providing timely promotion, computing facilities and generous funding to present my research work in various International and National Conferences across India. I would also like to thank all the

SSE Project Investigators from various nodes of this project for their vital comments and evaluation during my research presentations in various SSE Workshops.

I express my sincere thanks to ***Dr. P. Dhavachelvan***, Head, Department of Computer Science, Pondicherry University and ***Dr. R. Subramanian,*** Dean, School of Engineering and Technology for permitting me to do this research work.

I am indebted to ***Dr. K. Saruladha***, Senior Assistant Professor, Pondicherry Engineering College, for her volunteered support, encouragement and prayers for me. I am also thankful to my contemporary research scholars ***Ms. R. Sunitha, Dr. K. S. Kuppusamy, Ms. V. Uma, Ms. P. ShanthiBala*** and ***Mr. Ajit Kumar*** with whom I was able to discuss about my research and personal happenings and share all the frustrations and joys which were encountered during my Ph.D. journey.

I am beholden to my parents, whom without a second thought supported my decision to resign the job and to pursue research. I strongly believe that only with the showers of blessings from my grandfather and grandmother, who are in now in their heavenly abode, I came up to this stage in research. I owe a great deal to my brother-in-law ***Mr. S. Udayakumar***, and my sister ***Mrs. U. Kalaiselvi*** for their unbounded love and affection. Special mention to my loving nephews ***U. Aadhish*** and ***U. Mahatru*** with whom, due to my research work, I didn't spend much time during their stay in India.

My thanks are due to unmentioned many others, who rendered their help during this research. Last but not least, I thank the ***Almighty*** for bestowing me with good health and favoring me with supportive environment to carry out this research work.

P.Thiyagarajan

ABSTRACT

The secure transmission of information is the need of the hour in “Information world”. Cryptography and Information hiding are the techniques which transmit information securely to remote places. Steganography is an information hiding technique where the information to be transmitted is hidden in a digital medium like image, audio or video. The medium which contains the secret message is known as stego-medium. This thesis focuses on the spatial domain image steganography algorithms for 2D and 3D images.

A detailed literature review has been carried out on the existing spatial domain 2D and 3D image steganography algorithms. The existing spatial domain image steganography algorithms are classified and the important methods from these classifications are discussed. The objectives of this research have been framed based on the careful and detailed analysis of the pros and cons of these existing methods.

This thesis is focused on strengthening the spatial domain image steganography algorithms using the dynamic key. Three new algorithms namely Dynamic Pattern based Image Steganography (DPIS), Reversible Dynamic NROI based Steganography algorithm using graph coloring (RDS) and Pattern Based 3D Image Steganography (PBIS-3D) algorithms are proposed in this research to strengthen the security in spatial domain image steganography algorithms.

DPIS algorithm is proposed for 2D images and the dynamicity is ensured using the random color string generated for every embedding process. RDS algorithm is also proposed for 2D images and dynamicity is encompassed using the graph which is assigned for cover-image. The assigned graph is solved for graph 3-coloring to get the key. PBIS-3D algorithm is proposed for 3D images and the dynamicity is introduced using the triangle mesh which is formed using the secret message. The developed DPIS algorithm is applied to Internet banking domain to enhance the transaction level security and to prevent the phishing attack. Both RDS algorithm and PBIS-3D algorithm are applied to the medical domain to hide the patient details in the medical image. RDS algorithm is also applied to GIS domain to hide the metadata of the map in the NROI of the image.

The three proposed DPIS, RDS and PBIS-3D algorithms are implemented using Matlab and tested with capacity, invisibility and statistical parameters. All these parameters are tested by conducting experiments and the average of the results was projected. The capacity parameter calculates the number of pixels used for embedding secret message bits of different lengths. The invisibility parameter is tested with the help of histogram analysis.

Three statistical parameters Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER) are calculated to find the quality of the stego-image generated by the DPIS, RDS and PBIS-3D algorithms. Chi-square test is also performed to find the relation between the cover-image and the stego-image generated by the three proposed algorithms. The robustness of the proposed algorithms is tested by exposing the stego-images to various attacks such as scaling, cropping, rotation, noise and filtering attacks. The empirical results obtained using the parameters capacity, invisibility, statistical tests and robustness for the proposed algorithms DPIS, RDS and PBIS-3D are encouraging.

The conclusion derived out of this thesis is that the introduction of dynamicity in the key, pixel selection and in the number of bits embedded in the pixels strengthens the security in spatial domain image steganography and it is proved through various experimental results. The future direction of this research work includes the introduction of dynamicity in the frequency domain image steganography, exploration of the statistical property of the image to introduce dynamicity and to revert the complete cover-image from the stego-image in the extraction part.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Expansion
2D	2-Dimension
3D	3-Dimension
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
ASP	Active Server Pages
ATM	Automated Teller Machine
B	Blue Color
BC	Before Christ
BER	Bit Error Rate
CI	Cover-image
CT	Computed Tomography
DM	Digital Medium
DNS	Domain Name System
DPIS	Dynamic Pattern based Image Steganography
EPR	Electronic Patient Record
G	Green Color
GIS	Geographical Information System
HVS	Human Visual System
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
K	Key
LCD	Liquid Crystal Display
LSB	Least Significant Bit
MATLAB	Matrix Laboratory
MD5	Message Digest
MEP	Macro Embedding Primitive
MKA	Modified Kekre's Algorithm
MSE	Mean Square Error
MST	Minimum Spanning Tree

NC	Normalized Correlation
NROI	Non Region of Interest
OPAP	Optimal Pixel Adjustment Process
P	Pixel
PBIS-3D	Pattern Based 3D Image Steganography
PCA	Principal Component Analysis
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Differencing
R	Red Color
RCI	Reversed Cover-image
RDS	Reversible Dynamic NROI based Steganography Algorithm using graph coloring
RGB	Red, Green and Blue color
RIM	Repetitive Index Modulation
ROI	Region of Interest
RRP	Representation Rearrangement Procedure
RS	Regular Singular
RSA	Ron Rivest, Adi Shamir and Leonard Adleman
SHA	Secure Hash Algorithm
SI	Stego-image
SM	Secret Message
SMB	Secret Message Bits
SSL	Secure Socket Layer
URL	Uniform Resource Locator
W	Watermark
WDM	Watermarked Digital Medium
XOR	Exclusive Or

CHAPTER 1

INTRODUCTION

"Information is wealth" is profoundly known statement. The advancement in information and communication technology has facilitated the storage and transmission of information globally. This mobility of information helps business to operate from different geographical locations. As information is crucial for any business, the safe transmission of information in the digital world is the most challenging task. The three primary goals for secure transmission of information are Confidentiality, Integrity and Availability (Pieprzyk et al., 2003).

Confidentiality makes sure that only the intended recipient will receive and will be able to interpret the communicated message. Integrity enables the receiver to check whether outsiders tampered with the information transmitted. It also detects the changes in the order of the message transmitted, deleting or adding some parts of the message. Availability makes sure that the information is available when the user needs it. The techniques that information security systems adopt to protect the information from unintended recipients, are explained in the following sections.

1.1. INFORMATION SECURITY SYSTEMS

Information security systems guarantee the security of information through cryptography and information hiding techniques (Pieprzyk et al., 2003). Cryptography is the study of mathematical techniques which transform the secret message into unintelligible form. The information hiding techniques are classified broadly into watermarking and steganography techniques. The broad classification of information hiding techniques is shown in Figure 1.1 and the bold in the Figure 1.1 indicates the focus of our research.

1.1.1. Cryptography

Cryptography is the study of converting messages from readable format to scrambled format ensuring that only the communicating parties will be able to understand the message (William and Stallings, 2006). The information is secured in cryptography through encryption and decryption algorithms. Encryption is the first step in

cryptography and it accepts plain text (P) and the encryption key (E_k) as input and produce cipher text (C) as output. This cipher text is transmitted through the communication channel to the receiver. The received cipher text is decrypted using the corresponding decryption algorithm.

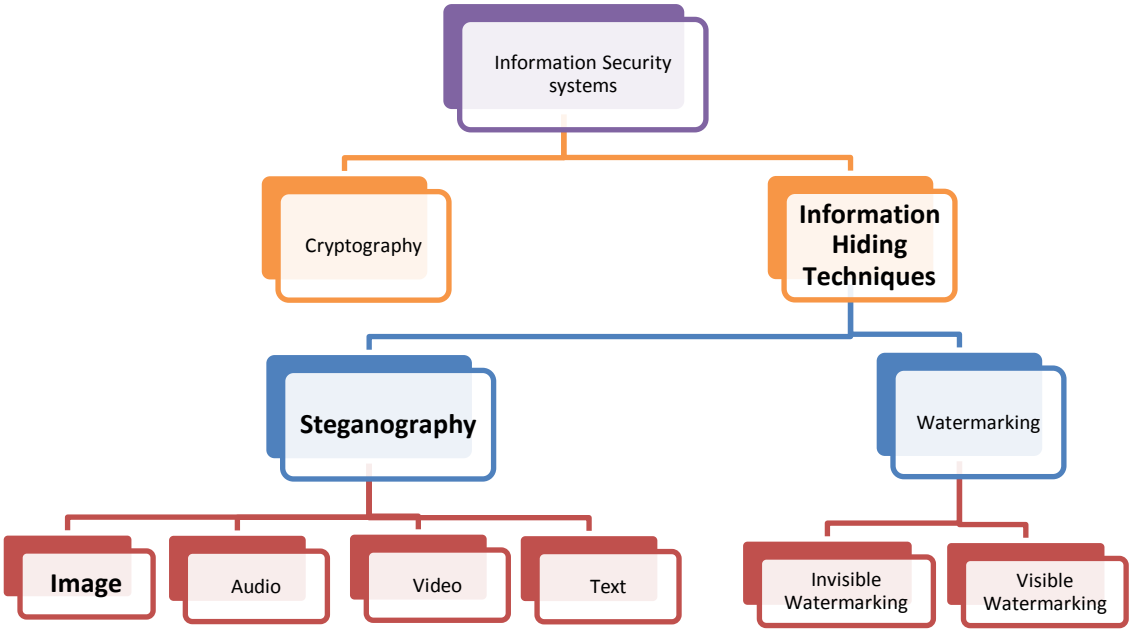


Figure.1.1. Information security system classification

The input to the decryption algorithm is the cipher text (C) and the decryption key (D_k). The output of the decryption algorithm is the plain text (P). The encryption and decryption keys used in cryptography algorithms may be the same or different for encrypting and decrypting messages.

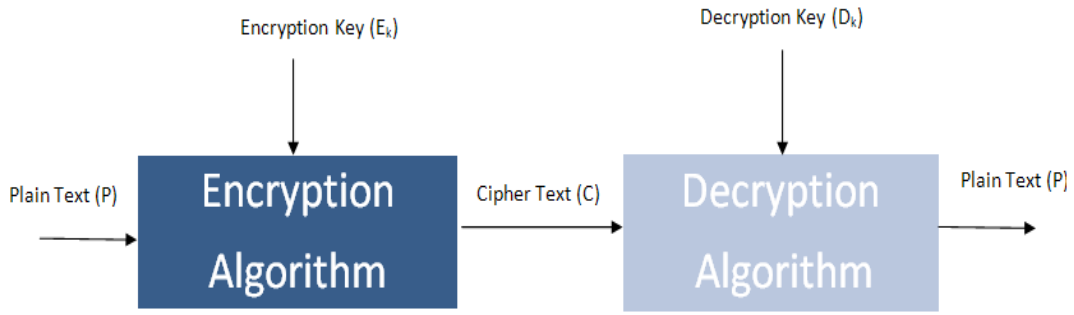


Figure.1.2. Asymmetric key cryptography – Diagrammatic representation

If the same key is used both in encryption and decryption part, then the algorithm is called as symmetric-key cryptographic algorithm otherwise it is called as asymmetric-

key cryptographic algorithm. Figure 1.2 shows the diagrammatic representation of asymmetric-key cryptographic algorithm.

1.1.2. Information Hiding Techniques

Apart from cryptography, information hiding techniques such as watermarking and steganography are also used to provide information security. An overview of the watermarking and the steganography techniques is given in the following section.

1.1.2.1.Watermarking

Watermarking is a technique which is used to place a piece of data either visibly or invisibly in digital medium such as image, audio or video. Watermarking is mainly used to identify the owner, source and distributor of the digital medium (Shih, 2007). Watermarking can also be used to detect the tampering, if any, done to the digital medium. Watermarking is further classified into invisible and visible watermarking. In visible watermarking the owner name or logo of the digital medium (Watermark (W)) is embedded into the Digital Medium (DM) visibly providing copy right protection to the digital medium.

In invisible watermarking the watermark is embedded to the digital medium such that it is not visible in the digital medium. In both visible and invisible watermarking, the embedding of watermark should not introduce any noticeable changes in the original digital medium. Figure 1.3 depicts the overall process involved in invisible watermarking.

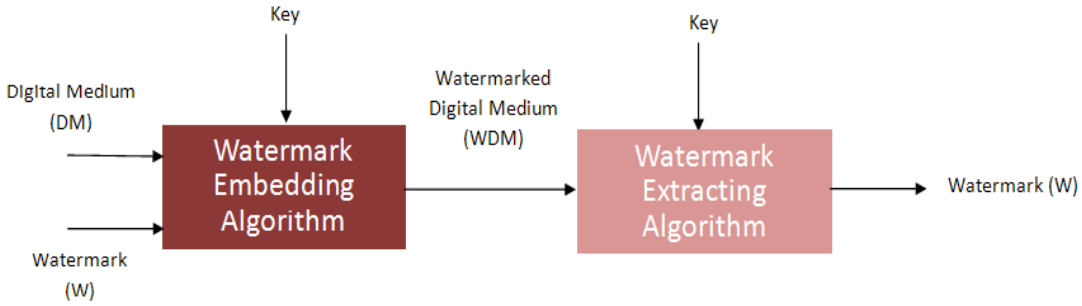


Figure.1.3. Invisible watermarking – Diagrammatic representation

1.1.2.2. Steganography

Steganography is the art and science of hiding information in digital medium (Shih, 2007). The digital media used to hide information in steganography are text, video,

audio and image. This thesis work mainly focuses on image steganography. **"***A Picture speaks more than words*" is absolutely true in image steganography. Apart from the content in the image which is detected by Human Visual System (HVS) it also contains information which is hidden in the image. Steganography is a form of invisible watermarking (Marvel et al., 1998). The art of secret communication has been a practice since ages and the section below explains the art of secret communication in ancient days.

1.1.2.2.1. Ancient Steganography Methods

The word steganography originated from the two Greek words 'stegos' meaning 'cover' and 'graphia' meaning 'writing'. The art of secret communication steganography has its origin in 5th century BC (Before Christ). Since then it has been practiced by military and political leaders for secret communications. Histiaeus in 5th century BC shaved the head of a slave and tattooed the secret message on his scalp (Provos and Honeyman, 2003) (Moulin and Koetter, 2005). Once the hair grew on the slave's head, the slave was sent to the recipient. In World War II, invisible ink was used to write secret messages on paper (Johnson and Jajodia, 1998). These papers when examined by non-intended recipient will appear to be blank. Once the paper reaches the recipient, it will be heated to reveal the secret message written on it. The advanced version of this technique uses chemical substances instead of heating at the recipient side to know the secret message.

Chinese mathematicians around 500 years ago devised a method in which paper with holes is shared between communicating parties (Kahn, 1996). Sender places the sheet with holes on the plain paper and writes the message on the holes. Sheet with holes is removed and the remaining spaces are filled with characters so that the original message appears innocuous. Null cipher (Kahn, 1996) (Johnson and Jajodia, 1998) is another interesting information hiding technique developed during World War II, which is explained through an example.

The following text was send to the receiver "*Big rumble in New Guinea. The war on celebrity acts should end soon. Over four big ecstatic elephants replicated"*. First characters from each word are taken to form the secret message, which is "*Bring two cases of beer*". The following section explains the digital era steganography.

1.1.2.2.2. Digital Era Steganography

The advancement in Internet, computing facility and Digital Signal Processing (DSP) techniques enabled steganography techniques on digital medium (Gribunin et al., 2002). The secret message, which is to be transmitted to the recipient, is embedded in the digital medium such as text, image, audio and video. The diagrammatic representation of image steganography is represented in Figure 1.4.

This research is focused on image steganography and it can be done in spatial domain and frequency domain. As in watermarking technique, image steganography (Chandramouli et al., 2004) also involves embedding and extracting algorithms. The original image (cover-image) and the secret message are the inputs to the embedding algorithm. With the help of the key, the secret message is embedded in the cover-image and the output will be the stego-image. This stego-image is given as input to the extracting algorithm and the same key used in embedding algorithm will be used to extract the secret message from the stego-image.

Steganography is applied in several domains (Bahi et al., 2012) such as military for secret communication, telemedicine for transferring patient information etc. Like two sides of a coin, steganography can also be used for destructive purposes.

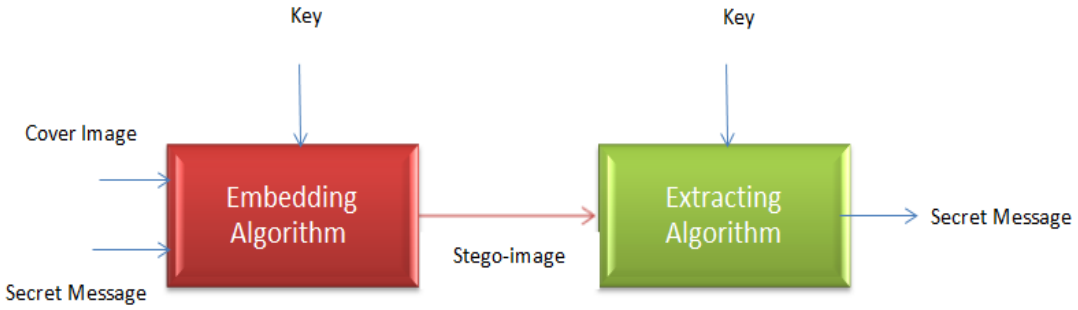


Figure.1.4. Image steganography – Diagrammatic representation

From the article in USA TODAY[1], it is evident that steganography was used to plan 9-11-2001 twin tower attack. Steganography was also used to launch botnet cyber attack (Nagaraja et al., 2011). To prevent the illegitimate use of steganography, steganalysis techniques are used. Steganalysis is the art and science of detecting and extracting the secret message in the digital medium (Cheddad et al., 2010).

[1] "Researchers: No secret bin Laden messages on sites" http://usatoday30.usatoday.com/tech/news/2001/10/17/bin-laden-site.htm#more Retrieved on: 6th April 2013

Steganalysis is done on the digital medium by applying image processing attacks such as cropping, scaling, rotation and translation. Statistical techniques (Amin et al., 2007) such as correlation, first order statistics (histogram) are also used to detect the presence of message in the digital medium. All these techniques cryptography, steganography and watermarking are interlinked. To differentiate between these techniques the purpose of these techniques is shown in Table 1.1. In this research, the steganography is focused and motivations to choose steganography are discussed in the following section.

Table.1.1. Purpose of cryptography, watermarking and steganography

Techniques	**Purpose**
Cryptography	To ensure security during communication by scrambling the readable data format to meaningless sequence of words using cryptographic algorithms (William and Stallings, 2006)
Water marking	To protect copy right violation in digital medium (Shih, 2007)
Steganography	To conceal the existence of information in digital medium so that apart from communicating parties none will able to detect the presence of data in the digital medium (Gribunin et al., 2002)

1.2. MOTIVATION

With the existing computational facilities even the toughest cryptographic algorithms such as Rivest-Shamir-Adleman (RSA[2]) is cracked which clearly portrays that it is not only enough to keep the content of the message secret but also necessary for us to keep the existence of the message secret. As keeping the existence of message secret in digital medium is a challenge, this work has been focused on steganography. This thesis emphasizes spatial domain 2-Dimensional (2D) and 3-Dimensional (3D) image steganography algorithms.

In recent years, many 2D and 3D spatial image domain image steganography algorithms were proposed (Cheddad et al., 2010). In this thesis, these 2D and 3D spatial domain image steganography algorithms were classified based on their scheme. On analyzing these spatial domain image steganography algorithms carefully it was found that many of the existing spatial domain image steganography algorithms

[2] "Researchers crack RSA encryption algorithm" http://www.slashgear.com/researchers-crack-rsa-encryption-algorithm-0977193/ Retrieved on: 03rd January 2011

are static in nature and they use same position of pixels and static number of bits for embedding different secret messages in different images.

Though the spatial domain image steganography algorithms are inexpensive and can embed very large amount of data compared to frequency domain image steganography algorithms (Kanzariya Nitin and Nimavat Ashish, 2013), due to their static nature they cannot withstand major image processing and statistical attacks. This static nature of existing spatial domain image steganography algorithms was the motivation to work towards dynamic key spatial domain image steganography approaches for 2D and 3D images. The important phases of this research work are explained in the next section.

1.3. PHASES OF RESEARCH

The different phases of this research work titled "Dynamic Key Based Approaches for Security Amelioration in Spatial Domain Image Steganography" are shown in Figure 1.5. The phases include literature survey, design, implementation and experimental analysis. Contribution of this research in nutshell is outlined in the next section.

1.4. CONTRIBUTIONS OF THE THESIS

In this research, two spatial domain image steganography algorithms for 2D images and one spatial domain image steganography algorithm for 3D images are proposed and implemented. The steganography algorithms proposed for 2D images are Dynamic pattern based image steganography (DPIS) algorithm and Reversible Dynamic (Non Region of Interest) NROI based Steganography algorithm using Graph Coloring (RDS). Further for 3D images, Pattern based 3D Image Steganography (PBIS-3D) algorithm is proposed.

These three proposed algorithms were implemented and evaluated with capacity, invisibility, statistical and robustness parameters. DPIS algorithm is applied to Internet banking domain and RDS and PBIS-3D algorithms are applied to medical domain. The overall research contribution is depicted in Figure 1.6.

1.5. ORGANISATION OF THE THESIS

This thesis is organized into nine chapters. They are

- Chapter 2 presents a thorough literature survey on spatial domain 2D and 3D image steganography algorithms. The existing spatial domain 2D and 3D image steganography algorithms are grouped based on their methods. A brief survey is also provided for the Internet banking transaction level security mechanisms and anti-phishing browser plug-ins.

- Chapter 3 discusses the problem statement, objective of the research, scope of the research and research methodology followed in this research work.

- Chapter 4 elaborates the proposed Dynamic Pattern based Image Steganography (DPIS) algorithm for 2D images. This chapter covers the need for dynamic 2D image steganography algorithm. The three important phases of the DPIS algorithm, dynamic key generation, DPIS embedding algorithm and DPIS extraction algorithm, are explored in this chapter.

- Chapter 5 delves into the details of how the key is generated dynamically from the cover-image in the proposed Reversible Dynamic NROI based Steganography algorithm using graph coloring (RDS). This chapter also discusses the RDS embedding and extraction algorithm in detail.

- Chapter 6 deals with the proposed Pattern Based 3D Image Steganography (PBIS-3D) algorithm. This chapter starts with the need for dynamic 3D spatial domain image steganography algorithm. Dynamic key generation from secret message, PBIS-3D embedding algorithm and PBIS-3D extraction algorithm are elaborated in this chapter.

- Chapter 7 provides details about the implementations and the parameters, which are used to evaluate the proposed algorithms. The broad categories which are used to evaluate these proposed algorithms are capacity, invisibility, statistical test and robustness against various attacks. This chapter also compares these three proposed algorithms with similar existing algorithms against various parameters.

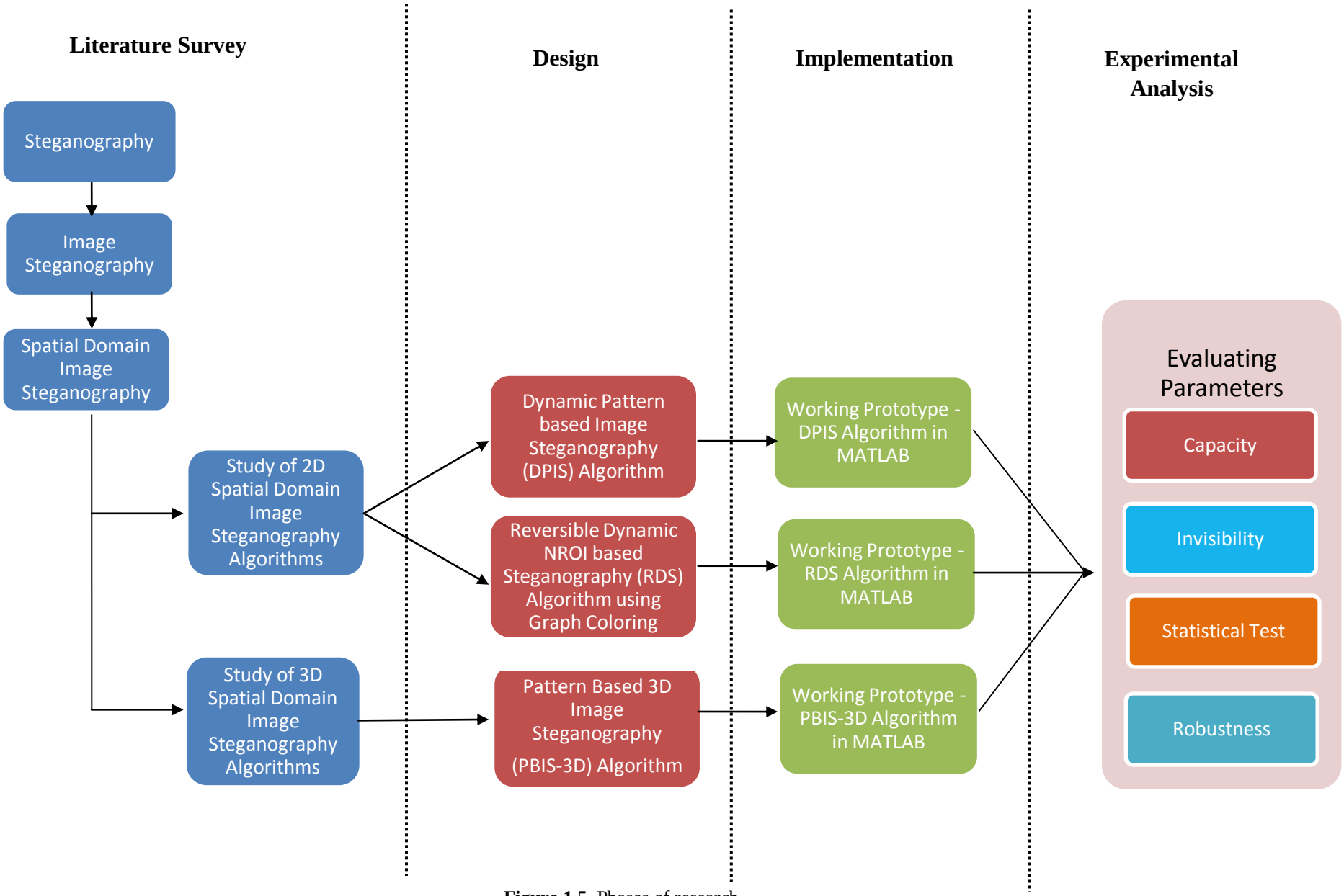


Figure.1.5. Phases of research

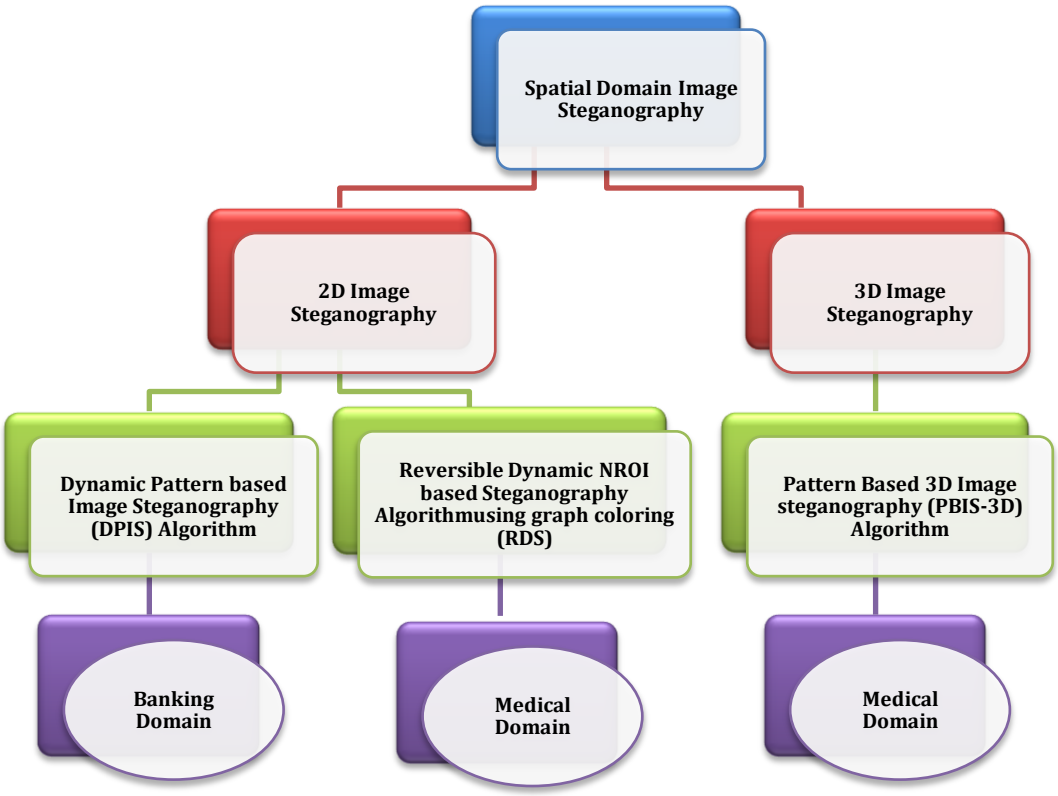


Figure.1.6. Research contributions

- Chapter 8 illustrates the applications of these three proposed algorithms. DPIS algorithm is applied to Internet banking domain to enhance transaction security and to prevent phishing attack. RDS and PBIS-3D algorithms are applied in medical domain for secure transfer of patient information.

- Chapter 9 concludes by summarizing the findings of the thesis and indicating possible future avenues for this research.

CHAPTER 2

LITERATURE SURVEY

This chapter provides a detailed literature review on the various 2D and 3D spatial domain image steganography algorithms. The existing 2D and 3D spatial domain image steganography algorithms are classified into various methods based on their embedding and extraction procedure and its pros and cons were analyzed. In order to overcome the limitations noticed in the literature survey, three dynamic spatial domain image steganography algorithms were proposed in this research. These proposed algorithms were applied to Internet banking and medical domain. In Internet banking domain the proposed algorithm is applied to enhance the transaction security and to prevent the phishing attack. In medical domain, the proposed algorithm is applied to hide the patient information in the medical image.

The existing methods, which provide transaction level security in Internet banking domain and the plug-in methods, which prevent phishing attacks, are also discussed in this chapter. The existing steganography algorithms which were applied to medical domain are discussed as part of survey of 2D and 3D spatial domain image steganography algorithms.

2.1. LITERATURE SURVEY – 2D IMAGE STEGANOGRAPHY

Image steganography is usually carried out in two domains viz., spatial domain and frequency domain. In frequency domain, the cover-image is transformed to frequency domain coefficients by mathematical tools such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) and Contourlet Transform (CT). In frequency domain, the secret message is embedded into the coefficient of the insignificant bits such that it doesn't affect the quality of the stego-image. The transformations that are used in frequency domain image steganography algorithm are listed below:

a) Discrete Cosine Transform (DCT) (Malakooti and Khederzdeh, 2012, Song et al., 2012, Behbahani et al., 2011)
b) Discrete Fourier Transform (DFT) (Bhattacharyya et al., 2009a, McKeon, 2006, Keshari and Modani, 2011)

c) Discrete Wavelet Transform (DWT) (Prabakaran and Bhavani, 2012, Seyedi et al., 2011, Sarreshtedari and Ghaemmaghami, 2010)

d) Contourlet Transform (CT) (Mohan and Anurenjan, 2011, Sajedi and Jamzad, 2008)

Since the research work in this thesis is based on spatial domain, a brief introduction is given above to frequency domain image steganography algorithm and detailed literature review is provided on spatial domain image steganography algorithm in the next section.

2.1.1. Spatial Domain Image Steganography

Spatial domain 2D image steganography algorithms are grouped into four main categories. They are pixel based steganography, random steganography, texture based steganography and reversible steganography. Pixel based steganography is further classified into pixel channel based algorithm, pixel value difference algorithm and pixel intensity based algorithm. Random steganography is further classified into random number based algorithm, chaotic algorithm and fibonacci, prime and natural number based algorithm. Texture based algorithm is classified into texture analyzing algorithm, edge based algorithm, and labeling algorithm. This broad classification of spatial domain 2D image steganography algorithm is depicted in Figure 2.1.

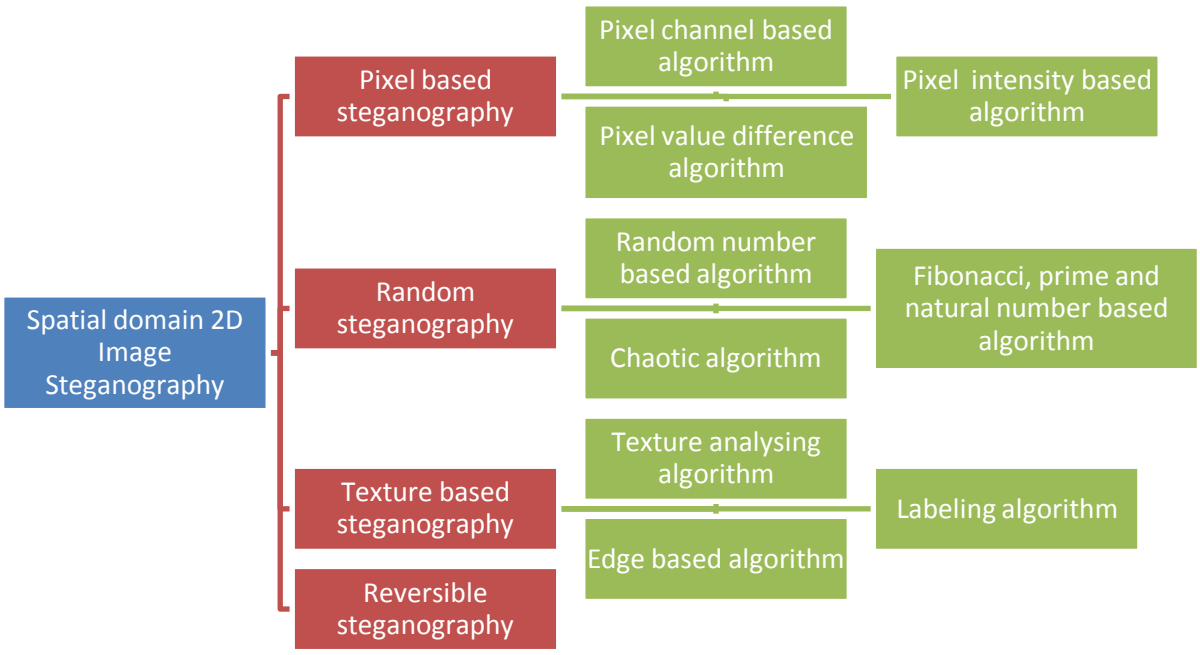


Figure.2.1. Classification of spatial domain 2D image steganography algorithm

2.1.1.1. Pixel Based Steganography

The characteristics of the pixel such as its value, color and intensity are taken into consideration in pixel based 2D steganography algorithms. The major existing algorithms in the pixel based steganography are pixel value difference algorithm, pixel channel based algorithm and pixel intensity based algorithm are discussed in detail in the following section.

2.1.1.1.1. Pixel Value Difference Algorithm

Optimal Pixel Adjustment Process (OPAP) and the Pixel Value Differencing (PVD) are the major techniques used in pixel value difference algorithm. The algorithms such as (Chan and Cheng, 2004, Ulutas et al., 2011, Wu et al., 2011 and Mandal and Das, 2012) are discussed briefly in this section. All the discussed algorithms are generic except (Ulutas et al., 2011) which focuses on medical domain.

In (Chan and Cheng, 2004) Least Significant Bit (LSB) method is used by applying Optimal Pixel Adjustment Process (OPAP). In OPAP authors check whether the channel of embedded pixel modify k+1 bits, where k is the number of bits embedded to reduce the Mean Square Error (MSE) in the channel. The quality of resultant stego-image is greatly improved by OPAP techniques and it also reduces the computational complexity.

(Ulutas et al., 2011) proposed a (k,n) secret sharing method in which the medical image and patient record information is shared among ‘n’ different clinicians. In order to reconstruct the medical image at least ‘k’ number of clinicians should gather. This Shamir’s secret sharing scheme is used to address all the security parameters such as authentication, integrity and confidentiality. The two components of this method are partitioning and retrieving. In partitioning component, the medical image and patient information are divided into shares by sharing algorithms. LSB based embedding is done with the help of OPAP (Optimal Pixel Adjusting Process). In the retrieving component, the shares of medical image are checked for their integrity and the reconstruction of image is done. From the experimental results it was shown that this method had produced high embedding capacity with low distortion.

OPAP LSB technique is used in (Wu et al., 2011) method in order to enhance the quality of the stego-image. The cover-image is divided into non- overlapping blocks

and variable message bits are embedded in the cover-image. This method uses the Shamir's secret sharing scheme as its base. This method has been compared with other information hiding techniques and from the results it was shown that this method produces good quality stego-images.

Each pixel in (Mandal and Das, 2012) method is split into 8 bits of red, 8 bits of blue and 8 bits of green color. Each color from all pixels in the image is grouped and is represented as matrices. Pixel Value Differencing (PVD) method is applied to all the three matrices in a sequential way. The problem of overflowing of values beyond 255 is prevented in this method. From the experimental results it is observed that this method outperforms the original PVD method. Another classification of pixel based steganography algorithm is pixel channel based algorithm which is discussed in the next section.

2.1.1.1.2. Pixel Channel Based Algorithm

Pixel channel based algorithm uses color channel of the pixel for embedding and extraction process. (Lim et al., 2001, Acharya et al., 2003, Gutub et al., 2008, Bhattacharyya et al., 2009b, Nergui et al., 2009 and Nikoukar, 2010) are the few major algorithms discussed briefly for pixel channel based algorithm. Out of the six algorithms discussed in this section, three algorithms (Lim et al., 2001, Acharya et al., 2003 and Nergui et al., 2009) were focused on medical domain.

Channel based spatial domain information hiding technique is proposed in (Lim et al., 2001) method. Integrity and authenticity security parameters are achieved in this method. This method is web based client server model and it uses Computed Tomography (CT) scan images for experiments. In embedding algorithm, the 7-bit plane information is passed as input to the hash function. The resultant from hash function is embedded in LSB of pixel.

The detection algorithm is in server side, which checks the integrity. In detection algorithm LSB is extracted first and then the 7 bits are given as input to the hash function. The obtained information in detected part is compared with the embedded information. If there is an error, warning is given to the user about the change in the image.

(Acharya et al., 2003) proposed an algorithm in which medical images are used for

experiments and it encrypts the American Standard Code for Information Interchange (ASCII) characters of patient information using Advanced Encryption Standard (AES) algorithm. During transmission of medical image there is a probability of noise added to it. To manage the transmission effect channel coding technique has been used. Each bit from the encrypted message is embedded with the LSB of each pixel. It has been proved that the execution speed of the method is high and it is resistant to noise and cropping attacks.

In (Gutub et al., 2008) method indicator channel is fixed in each pixel. The 2 Least Significant Bit (LSB) of the indicator channel is analyzed to embed the secret message bits in the remaining channel. If the LSB of the indicator channel is '0' then no bit is embedded in the pixel. If the LSB of the indicator channel is '1' then secret message bits are embedded in the pixel. This method is tested with the parameters such as capacity, robustness and histogram analysis.

Keyless steganography algorithm is presented in (Bhattacharyya et al., 2009b). The number of 0's and 1's in the data to be embedded is counted and stored in the variables i_0 and i_1. The number of 0's and 1's in the blue color channel of the cover-image is stored in the variables c_0 and c_1. If c_0 greater c_1 and i_0 greater i_1 or c_1 greater c_0 and greater i_0 then the integer variable flag is set to 0 otherwise integer variable flag is set to1 in the fixed position of the stego-image file. If the flag is 0 then secret message bits are embedded in the LSB of the blue channel. Otherwise the last bit is inverted and the secret message bits are embedded in the LSB of the blue channel. This algorithm alters very less number of pixels in the cover-image and thus the stego-image obtained will be of high quality.

(Nergui et al., 2009) proposed a method which encrypts patient information using AES algorithm. This encrypted message is embedded inside the medical image using LSB algorithm. There are possibilities that during transmission the medical image transmitted may be prone to noise. In order to mitigate this noise, Error Correcting Codes are introduced. Interleaving is a technique that is applied to increase the error correcting capability of Error Correcting Code. This method is tested for various channel conditions and error correcting codes.

(Nikoukar, 2010) in his method took pixels and split them into R, G and B channels. New value of the pixel is obtained by making the 3 LSB of Red, Green and Blue

(RGB) channels to zero. The obtained new values are compared and the minimum values of RGB channel are obtained to embed 2 bits of secret message. This method produced good quality stego-images. The intensity based steganography algorithm which is classification of pixel based algorithm is discussed in the next section.

2.1.1.1.3. Pixel Intensity Based Algorithm

The intensity value of the pixel is considered in this pixel intensity based algorithms. (Parvez and Gutub, 2008, Upreti et al., 2010, Hussain, 2010 and Dharwadkar et al., 2010) are the algorithms discussed in this section. Out of the four algorithms discussed (Dharwadkar et al., 2010) is targeted for medical domain.

Based on the intensity of the pixel secret message bits are embedded in (Parvez and Gutub, 2008) method. Indicator channel is shared between both the embedding and extracting part. The lowest value channel is chosen for embedding. Partition scheme decides the number of secret message bits to be embedded in each pixel. This method results in a very high capacity with low visual distortion.

Combination of cryptography and steganography are used in (Upreti et al., 2010) method. Rivest-Shamir-Adleman (RSA) and International Data Encryption Algorithm (IDEA) algorithms are applied on the plain text and the cipher text. Embedding is done based on the intensity of the pixel. From the experimental results it was obvious that this method utilizes very less number of pixels for embedding large data.

(Hussain, 2010) in his method uses Modified Kekre's Algorithm (MKA) which is based on LSB method. Secret message, which is to be embedded, is operated with Exclusive Or (XOR) with the 8-bit key to destroy the original characteristic of the message. Based on the intensity, pixels which can embed 5, 3 and 2 bits are grouped together and represented as matrix. Experimental results show that this method has high capacity and produces good quality stego-images.

In (Dharwadkar et al., 2010) method intensity of the pixel is chosen as deciding criteria for embedding. This method is experimented with medical images. The information, which is to be embedded, is converted into bits. These bits are compared with the bits plane. If the match occurs then these locations are stored in the array. These array values are used in the extraction part to extract the bits. Thus the authentication of the image is checked without making any change in the cover

medical image.

The above discussed pixel based steganography algorithms concentrate on the pixel characteristic for embedding and extracting. Static pixel selection and static number of secret message bits embedded in the pixel chosen for embedding are the limitations of pixel based steganography algorithms.

2.1.1.2. Random Steganography

Random steganography algorithm is classified into Fibonacci, prime and natural number based algorithm, chaotic based algorithm and random number based algorithm. In random steganography algorithm, the secret messages are embedded in the pixels, which are selected by the random mechanism. The details about these random mechanisms are discussed below.

2.1.1.2.1. Fibonacci, Prime and Natural Number Based Algorithm

This section discusses the algorithms, which use prime number, natural number and Fibonacci series for their embedding process. (Picione et al., 2006, Dey et al., 2007, Younes and Jantan, 2008 and Al-Husainy, 2011) are the few algorithms briefly discussed below.

In (Picione et al., 2006) method fibonacci series is used for embedding process. This method uses different bit-planes decomposition based on Fibonacci series which increases the number of embedding bit planes. The experimental results have been compared with normal LSB method, which shows that this method achieves good quality stego-images.

(Dey et al., 2007) proposed an improved Fibonacci LSB data hiding technique using prime numbers. Embedding is done in higher bit planes which results in robust and good quality stego-image. Through theoretical and experimental results authors have shown that this method out performs Fibonacci LSB data hiding technique.

(Younes and Jantan, 2008) proposed an algorithm using natural number decomposition, which is an improved version of Fibonacci and prime number LSB method. Secret message bits are embedded in different sets of bit planes. The comparative study with Fibonacci and prime number LSB methods shows that this method is robust and produces stego-image of good quality.

The standard ASCII value of the alphabets is mapped to the decimal value in the range 0 to 25 in (Al-Husainy, 2011) method. The secret message, which is to be embedded, is mapped to the new ASCII value and is stored in an array M. The pixel byte value of the cover-image is represented as three decimal digits and is stored in an array D.

The frequency for the elements in both the array M and D is calculated. The core of this method is finding the match list L by matching each element in the list M with the elements in the list D. If match is found it is represented as 1 otherwise as 0. After creating the matching list L, it creates a new list B from list L, such that each element in B represents the number of continuous values of 0s or 1s in the list L. The list B is compressed and embedded in the unused bytes of the cover-image. This method produces good quality stego-images. Another classification of random based steganography algorithm is chaotic based algorithm which is discussed in the next section.

2.1.1.2.2. Chaotic Based Algorithm

In this algorithm, the randomness is achieved by the chaotic sequence or mapping procedure. (Gang and Ni-ni, 2005, Luo et al., 2007 and Yang and Zhou, 2009) are the algorithms discussed briefly in this section. Among the algorithms discussed (Luo et al., 2007) is focused on medical domain.

(Gang and Ni-ni, 2005) proposed a fragile information hiding technique. LSB method is combined with chaotic sequence and it is applied for medical images. Security of the method is ensured by the chaotic sequence and it produces good quality stego-images.

(Luo et al., 2007) proposed a method on LSB Steganography. This method adopts random embedding through chaotic system which is robust to sample pair steganalysis technique (a technique used to detect the presence of secret message inside the digital medium). Robustness of this method depends on initial value of chaotic system and parameter of the compensation.

(Yang and Zhou, 2009) in their novel technique hides the image inside the image. The image, which is to be hidden, is first compressed to reduce the amount of bits embedded. Chaotic mapping procedure is followed during embedding. This method

uses minimum number of pixels for embedding as the secret image is compressed. Robustness of this method is also improved because of the chaotic mapping. The random number based algorithm which is another classification of random based steganography is discussed in the next section.

2.1.1.2.3. Random Number Based Algorithm

In this algorithm, the random number is generated which is used for embedding and extraction procedures. (Abraham and Paprzycki, 2004, Lee et al., 2009 and Viswanatham and Manikonda, 2010) are the algorithms discussed in brief in this section for random number based steganography algorithm.

In (Abraham and Paprzycki, 2004) method random key is generated which is used for both embedding and extracting processes. Seed value is generated from the stego-key from which the pseudo random numbers are obtained. These random numbers are nothing but the pixels in the image in which the secret message are embedded.

(Lee et al., 2009) in their proposal uses pseudo random number for both embedding and extraction. Every bit from the secret message is assigned to the pixel in the cover-image and it checks for the LSB, if it matches nothing is done to the pixel. If it does not match, random number is generated between the range of 0 to 1. If the random number is less than or equal to 0.5 the original pixel value is reduced by 1 or if the random number is greater than 0.5 the original pixel value is increased by 1. This steganography method is resistant to chi-square attack.

In (Viswanatham and Manikonda, 2010) method random numbers are generated and these numbers are mapped to pixels in Region of Interest (ROI) of the cover-image. This method makes it tough for the intruder to hack as it selects the pixels randomly from the cover-image for embedding.

The above discussed random steganography algorithms select random pixel for embedding secret message. The limitations of random steganography algorithms are static secret message bits embedding and failure to check the integrity of the secret message at the extraction part.

2.1.1.3. Texture Based Steganography

In this section, the algorithms which exploit the texture of the cover-image for

embedding and extraction procedures are discussed. Texture based algorithm is classified into texture analyzing algorithm, edge based algorithm and labeling algorithm. Major algorithms belonging to this classification are briefly discussed below.

2.1.1.3.1. Edge Based Algorithm

In edge based algorithm, the edges are detected in the cover-image using segmentation or edge detection techniques. Generally the edge technique is used to separate the Region of Interest (ROI) from Non Region of Interest (NROI). The algorithms discussed in brief here are (Tirandaz et al., 2009, Li and Li, 2009, Chen et al., 2010, Luo et al., 2010, Zaz, 2010 and Hussain and Hussain, 2011). Among these algorithms (Li and Li, 2009 and Zaz, 2010) are deliberately proposed for medical domain.

In (Tirandaz et al., 2009) technique the message is embedded in the edge pixel of the binary text images. Text image boundaries are detected and message bits are embedded in it by applying flipping technique in edge pixels. In flipping technique, the distortion caused by embedding message in the edge pixels are calculated and based on the distortion value, message bits are embedded. Flipping is applied carefully on embeddable edge lines to avoid the easy detection of any changes by Human Visual System (HVS).

Repetitive Index Modulation (RIM) method is used to check the authentication and integrity of medical image in (Li and Li, 2009) method. Segmentation technique is used to separate the Region of Interest (ROI) and background portion of medical image. This background portion of the image is used to embed the ROI based content dependent message. Any error occurring during transmission in the ROI portion of the image, is easily identified at the receiver side by comparing the extracted message with the ROI. This method can embed secret message of large length.

(Chen et al., 2010) in his proposed method uses canny edge detector along with fuzzy edge detector. The edges in the image is divided into small blocks and data are embedded using LSB technique. Due to the hybrid edge detector used in this method, it achieves high payload and it produces good quality stego-images. This method also resists statistical steganalysis method.

In (Luo et al., 2010) the author revisited the LSB method by proposing adaptive edge scheme, which determines the embedding pixel according to the difference between continuous pixel values. Taken HVS into consideration bits were embedded in the sharp regions and smooth regions were free from embedding. The proposed LSB revisited method achieves good stego-image quality when compared with other LSB techniques. Message bits are embedded according to the threshold obtained from the secret message size and content edge.

(Zaz, 2010) in his method hides the patient record information into the medical image. El Gamal public key cryptosystem and Diffie-Helman Key distribution is modified and it is used in this method to enhance the security. From the cover medical image the Region of interest (ROI) and Non region of interest (NROI) are spotted out. The Electronic Patient Record (EPR) information is converted into bits and it is encrypted. From the cover medical image Least Significant Bit (LSB) plane is obtained and it is embedded with the encrypted EPR in NROI region. In the extraction part, the LSB plane is constructed from stego-image and the message embedded is extracted and decrypted. Apart from enhancing the security the computational cost of this method is low.

In general, the edge based method exploits the region around the edge of the given image for hiding information. (Hussain and Hussain, 2011) in their method used Canny or Sobel edge detection method. From the edge detected, certain length of horizontal edges are found. Based on the absolute difference of the edge pixel and the upper pixel with threshold of the image, LSB method is used for embedding. This method results in good quality stego-images with minimum number of bits used for embedding. The texture analyzing algorithm which is another classification of texture based algorithm is discussed in detail in the section below.

2.1.1.3.2. Texture Analyzing Algorithm

In texture based steganography algorithm, the cover-image is divided into hard and smooth texture area based on the sensitiveness of Human Visual System (HVS) and embedding and extraction processes are carried out. (Othman et al., 2009 and Majeed et al., 2009) are discussed in brief for texture analyzing steganography algorithm.

Human Visual System (HVS) characteristic is exploited in (Othman et al., 2009)

method for embedding message in the pixels. HVS can easily detect the minor changes in the blue color. Hence 2 bits are embedded in blue color while 3 bits are embedded in both red and green color and this approach is called as 3-3-2 (3 bits in red, 3 bits in green and 2 bits in blue channel) approach. Thus 1 byte of data is embedded in single pixel in 3-3-2 approach. In this work the 4-4-4 approach is also discussed which produces stego-image poorer in quality compared to the stego-image produced by 3-3-2 approach.

In (Majeed et al., 2009) method, range flit method for texture analysis is used which identifies the regions in the image where more data would be embedded. In complex texture 4-4-4 method embedding is applied. In smooth and simple texture 3-3-2 embedding is used. Texture based algorithm is further classified into labeling algorithm which is discussed in the following section.

2.1.1.3.3. Labeling Algorithm

In this method, the dark area of the cover-image is identified and the image is converted to binary. Then the objects are labeled with connectivity schemes. (Motameni et al., 2007 and Yang, 2007) algorithms based on this labeling method are briefly discussed below.

(Motameni et al., 2007) proposed a novel method to hide text message inside grey scale images. A group of pixels is called as connected pixels if their edges touch each other. This method discusses 4-connectivity and 8-connectivity. This method presents a way for labeling different colors to identify dark area of image and then hide the message in 2-LSB of pixels.

(Yang, 2007) in his method proposed steganography method based on module substitution. Variable secret message bits are embedded into pixel with the help of three module substitutions. In order to achieve good capacity and reduce color distortion, the Red, Green and Blue components are encoded by Mod u, Mod u-v and Mod u-v-w substitution. From the experimental results it is evident that good visual quality of stego-image is generated with high embedding capacity.

In texture based steganography algorithm, the characteristic of cover-image is taken care while embedding and extracting the secret message in it. The limitations of texture based steganography algorithm are similar to that of pixel based

steganography algorithms as pixel selection and embedding of secret message bits are static.

2.1.1.4. Reversible Steganography

Reversible algorithm is also known as lossless steganography algorithm. In reversible algorithm, the cover-image is retrieved at the extraction part after extracting the secret message from the stego-image. (Ni et al., 2006, Chang et al., 2008, Zeng et al., 2009, Ulutas et al., 2010 and Abd-Eldayem, M.M., 2013) are some of the reversible steganography algorithm discussed in this section.

(Ni et al., 2006) proposed a reversible data hiding technique based on histogram shifting. It is based upon a selection point of peak pixel value P from histogram and simply adding or subtracting 1 from all pixel values which are lesser or greater than P value. This algorithm utilizes the minimum points of the histogram of the cover-image and modifies the pixel grayscale values to embed data into the image using Least Significant Bit embedding procedure.

(Chang et al., 2008) in his proposal discussed a new histogram shifting method. It takes the adjacent pixels instead of histogram peak point value for embedding. This technique increases the embedding capacity, as the local area is highly correlated and it becomes the advantage to achieve high capacity.

(Zeng et al., 2009) proposed a new lossless data hiding method, which is also based on histogram shifting method. The modified version of histogram shifting is given by calculating the differences between adjacent pixels in different scan paths. The author also discusses nine different scan paths and the best path is chosen for embedding. Multi-layer data embedding is used to increase the hiding capacity. This method achieves high embedding capacity and keeps low distortion by choosing the best scan path.

(Ulutas et al., 2010) in his method has two algorithms involved in it, they are sharing and retrieving algorithms. The cover-image is divided into small images and it is shared among ‘n’ participants. Secret message values are embedded in the ‘n’ shared cover-images. In retrieving the algorithm the embedded message is extracted along with cover-image.

(Abd-Eldayem, M.M., 2013) in his method proposed a novel reversible information hiding method along with encryption algorithm. In embedding process, the medical image is divided into groups where each group has four pixels. Flipping method is applied to the pixel groups and RS (Regular-Singular) vector is created. Lossless compression technique is applied to the RS vector. The hash value of the medical image is obtained from Message Digest (MD5) algorithm. This hash value is concatenated with patient id to get the message. The concatenated message is encrypted using AES cryptographic function. The extraction is the reverse process of embedding. From the experimental results, it is shown that this method produces good quality stego-images. The advantage of the reversible steganography is that the cover-image is reversed from the stego-image with no loss or minimum loss. The shortcomings of the reversible steganography are static pixel selection, static embedding of bits and lack of dynamic key mechanism.

This section classifies the spatial domain 2D image steganography algorithms into four major algorithms based on pixel value, randomness, image texture and reversible property. Based on this classification, the literature review of the spatial domain 2D image steganography algorithms are discussed in this section. The next section explains the classification of 3D image steganography algorithms. The literature review carried out on the spatial domain 3D image steganography algorithms are discussed in the next section.

2.2. LITERATURE SURVEY – 3D IMAGE STEGANOGRAPHY

In recent days, three-dimensional (3D) geometric models are becoming a vital part of the multimedia content. 3D geometric models are in use in many fields such as architecture, computer aided design, video games, science, medical imaging, archaeological artifacts, and many more. The advancements of distributed engineering environment and virtual space construction technology open up the opportunities globally to distribute and exchange 3D geometrical models through computer network. Such background has prompted researchers to extend the realm of steganography from the traditional media such as images and videos to 3D geometric models.

3D information hiding techniques is first introduced in (Ohbuchi et al., 1997) and since then it has been a hot research topics in information security field. As the

structure and properties of the 2D and 3D image are entirely different, the information hiding algorithms of 2D digital images cannot be directly applied to 3D digital images.

The classification of the 3D image steganography algorithm is shown in Figure 2.2. 3D steganography algorithm has been classified into two types namely spatial domain and frequency domain. Frequency domain is further classified into spectral methods and multi resolution methods. In this chapter, a brief introduction of frequency domain techniques is provided. Since the research in this thesis focuses on spatial domain, the detailed literature review is provided on spatial domain 3D image steganography algorithms.

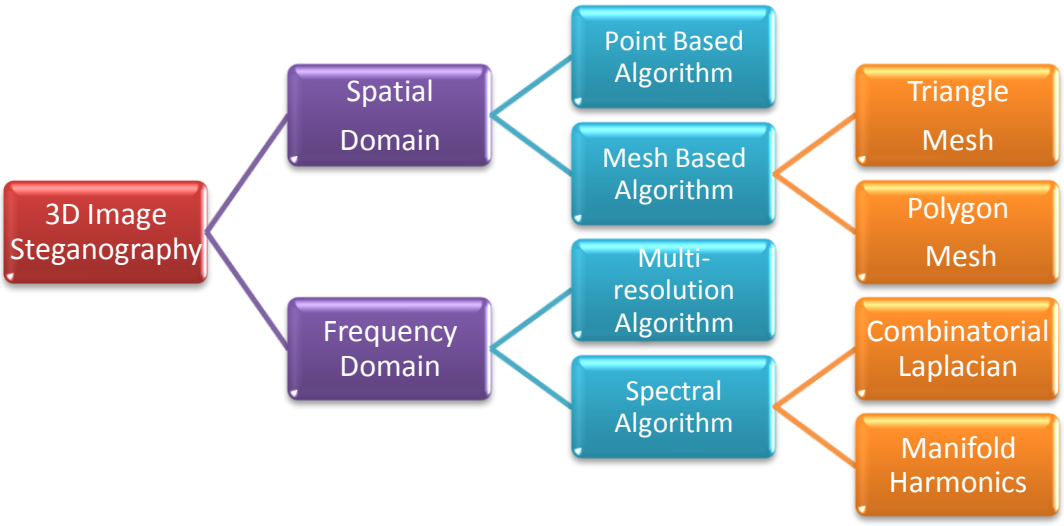


Figure.2.2. Classification of spatial domain 3D image steganography algorithm

2.2.1. Frequency Domain 3D Image Steganography

The basic idea behind the 3D frequency domain steganography is that to modify the cover-image using transformation techniques, and to embed the data in the frequency coefficient. In 3D steganography, the frequency domain steganography is classified into spectral algorithm and multi-resolution algorithm.

2.2.1.1. Spectral Algorithm

Spectral graph theory (Beineke et al., 2004) and signal processing are the areas that have influenced the spectral algorithm based information hiding technique. In spectral

algorithm, the secret message is added to the polygon mesh, which is formed in the cover-image. Mesh spectra is computed from a laplacian matrix derived from the connectivity of a polygonal mesh. Mesh spectral analysis was first proposed by (Karni and Gotsman, 2000) for lossy compression of vertices of polygonal meshes. Eigen value and eigen vector of laplace transform contain information about the shape of the mesh and their connectivity. Spectral algorithm is broadly classified into combinatorial laplacian and manifold harmonics algorithm.

2.2.1.1.1. Combinatorial Laplacian Algorithm

3D information hiding techniques proposed by (Alface and Macq, 2005, Karni and Gotsman, 2000, Ohbuchi et al., 2002, Taubin, 1995, Zhang, 2004) follow combinatorial laplacian method. There are two types of combinatorial laplacian method: non-blind and blind methods. The method which require the cover object while extracting secret message from stego object are called as non-blind method and the method which does not require cover object are called as blind method. Few non-blind methods by the authors namely (Cotting et al., 2004, Ohbuchi et al., 2001, Lavoué et al., 2006, Lavoué et al., 2007, Ohbuchi et al., 2004) have been reported in the literature.

In non-blind methods, the secret message bits are embedded in the low frequency and medium frequency coefficients. The main strength of these methods is the relatively high robustness. The disadvantages of the method are its computational cost and the distortion caused by this method in the cover-image is high.

(Cayre and Macq, 2003) and (Alface and Macq, 2005) proposed a blind method in which the embedding is done in coefficient triplet. In order to make the method secure, more attention is given to preprocessing, parameterization, patch generation and remeshing. Manifold harmonics, another classification of spectral method, is discussed in the following section.

2.2.1.1.2. Manifold Harmonics Method

Though combinatorial laplacian implementation is simple and it's reversible, lack of geometry information fails to describe the characteristics of an object. Manifold Harmonics is one such discrete laplacian proposed by (Vallet and Lévy, 2008) which

describes geometric characteristics. (Liu et al., 2008, Wang et al., 2009 and Lavoué, 2009) are some of the manifold harmonics methods reported in the literature.

2.2.1.2. Multi-resolution Algorithm

In the multi-resolution algorithm, the complicated function is broken into simple part called wavelet coefficients. In 3D mesh object, the original 3D mesh is analyzed using wavelet transform. (Uccheddu et al., 2004, Wang et al., 2007 and Wang et al., 2008) are some of the methods which uses multi-resolution method for information hiding. The basic idea is to adjust the wavelet coefficient norms to hide the secret message. Lookup table or quantization methods are used to control the weight of the modulation. The merits of the multi-resolution techniques are secret message can be embedded at different levels and secret message can also be embedded in wavelet coefficients base mesh. The demerit of the multi-resolution methods is that it is not resist to cropping and remeshing attacks.

This section provides a brief introduction of 3D frequency domain image steganography algorithm. The detailed literature review of the spatial domain 3D image steganography algorithms are explained in the next section.

2.2.2. Spatial Domain 3D Image Steganography

Spatial domain 3D image steganography is classified into point based algorithm and mesh based algorithm. Mesh based algorithm is further classified into triangle and polygon mesh method. The important algorithms of spatial domain 3D image steganography reported in the literature are discussed in this section.

2.2.2.1. Point Based Algorithm

In point based 3D image steganography algorithm, the secret message bits are embedded in the points distributed in the 3D images rather than forming meshes. The algorithms proposed by (Wang and Wang, 2006, Qi et al., 2010, Amat et al., 2010 and Tan et al., 2009) are discussed in this section.

(Wang and Wang 2006) proposed a point based spatial domain method for 3D images. This method discusses two methods namely Principal Component Analysis (PCA) and Macro Embedding Primitives (MEP) method. The point coordinate system is translated to new coordinate system. Further, the list of intervals is assigned for

each axis according to the secret key. Secret message bits are embedded into each interval by changing the point position. In the second method, Macro Embedding Primitives (MEP) is identified and then 2 to 6 secret message bits are embedded in each MEP. The robustness is tested by conducting different experiments and it is quantified in terms of capacity, computational complexity, visibility, and security.

(Qi et al., 2010) in his work uses Self-Similarity Position Matching procedure in spatial domain steganography. This method partitions the 3D point cloud to message patches and generates codebook. Every message point in similar message patch can embed maximum up to four bits. The shape description of the message patch and the similarity measures are used to improve codebook performance. From the experimental results, it is obvious that this method has high capacity with low distortion.

(Amat et al., 2010) in his research discusses a method to embed data without changing the position of the vertices of 3D spaces. This method is based on the 3D model given by cloud of vertices and a list of edges in the formation of triangle meshes. Initially a Minimum Spanning Tree (MST) is constructed covering all the points in the 3D model. Then in order to find the region of embedding the MST is scanned for which the starting point has to be decided by the key. This method is resistant to rotation, translation and scaling attacks but it is very sensitive to noise.

(Tan et al., 2009) in his research devised a point based method, which considers the vertex index as message block. The given message is represented as three types of message blocks namely unique, repeated and 1 or 0 bit repeated blocks. Each message block chooses the best embedding methods from vertex index, length bit string mapping and repeated bits embedding. The computation cost for this method is very less and capacity of this method is very high compared to the other methods.

In the above discussed algorithms the secret messages are embedded in the points in the 3D image which is distributed throughout the image. The limitation of the method are lack of dynamic key for embedding and extracting and lack of variable bits embedding in the pixel chosen in 3D image.

2.2.2.2. Mesh Based Algorithm

Mesh based algorithm is classified into triangle mesh and polygon mesh model algorithm. The secret message is embedded in the vertices and in the edges of the mesh formed. Some of the methods reported in the literature for triangle mesh and polygon mesh are discussed in this section.

2.2.2.2.1. Triangle Mesh Based Algorithm

In this method, triangle mesh is formed in the given 3D cover-image and the secret message bits are embedded in the edges or along with the vertices of the triangle mesh formed. The following triangle mesh based algorithms (Mao et al., 2001, Yu et al., 2003 and Chou and Tseng, 2006) are discussed in this section.

(Mao et al., 2001) is his work introduces triangle mesh for embedding. The triangle meshes are formed by dividing the edge of the triangle. The embedding ratio is decided by the ratio of the triangle edge and bits are embedded on the edges. At most 2 bits of the secret message per triangle is embedded. The major disadvantage of this method is that it cannot embed secret messages of large length.

(Yu et al., 2003) proposed a robust triangular non-blind mesh model. Vertices are grouped and each vertex is divided into many sections. Each bit is added to the section by modifying the length from its member vertices to the center of the mesh. Additive method is followed with an adaptive intensity from local geometrical mesh analysis. To ensure the robustness of the method preprocessing and resampling are done. The messages which are to be hidden are distributed throughout the image and it is resistant against many attacks such as cropping and addition of noise.

(Chou and Tseng, 2006) in their method, used triangle mesh vertices, to address two problems such as causality problem and convergence problem. Multi-function vertex embedding method and an adjusting-vertex method are introduced in this method to overcome the above said problem. In order to embed many bits in a vertex different functions are defined for the coordinates of the vertices. This method can also detect the small changes done to the models.

Apart from triangle meshes, polygon meshes can also be formed in cover-image to embed secret message, and the algorithms which uses polygon meshes to embed secret messages are discussed in the next section.

2.2.2.2.2. Polygon Mesh Based Algorithm

Instead of triangle meshes, polygon meshes are formed in the given 3D cover-image. In the polygon mesh formed, the secret messages are embedded in the vertices or on the edges of the polygon. The polygon mesh based methods proposed by the authors namely (Aspert et al., 2002, Cheng and Wang, 2006, Cho et al., 2007, Tu et al., 2010, Tu and Tai, 2012 and Garg et al., 2012) are discussed in this section.

(Aspert et al., 2002) in their work proposed a method in 3D polygon meshes. Small displacements of the vertices in the 3D polygon meshes along with the length of approximation of the normal to the surface are used for embedding. This method is robust to simple geometric transformations and less complexity in computation. The embedding procedure doesn't introduce any major visual distortion to the cover-image.

(Cheng and Wang, 2006) in his research uses polygon meshes for hiding data. This method uses spatial domain along with Representation Rearrangement Procedure (RRP). Spatial domain multi level embedding procedure is used to embed data in the vertices of the polygon and RRP is used to rearrange vertices order, rearrange polygon order and polygon indexes order. From the experimental results it is shown that the proposed method is efficient and secure.

Two data hiding methods for 3D polygon mesh models are proposed in (Cho et al., 2007) method. According to the message bits embedded, this method modifies the distribution of vertex norms. The cover-image is converted into spherical coordinates and the vector norms are divided into bin which is mapped to the normalized range of [0,1]. In the first method, the mean value of the distribution is shifted and in the second method variance of this method is changed. This method also employs histogram mapping function to enhance the quality of the stego-image. Robustness of this method is proved through similarity transforms.

(Tu et al., 2010) in his work describes a left-skewed binary coding tree for embedding in polygon meshes. The coding tree with skew property helps in lengthening the

embedding bit stream. The time complexity of this work is O(nlogn) with the maximum capacity of 72 bits per vertex. The reference ordering from polygonal mesh traversal is based on mesh connectivity thus making the method robust against affine transformations.

Message probability model based polygon mesh data hiding technique is proposed in (Tu and Tai, 2012) method. The embedding procedure has the following components such as computation of reference ordering, message probability model, construction of coding tree based on probability model and embedding. In the extraction part, the reference order is computed and the message is extracted. The time complexity of the algorithm ranges from O(nlogn) to $O(n^2)$. The capacity of this approach depends on the run-length histograms of a given embedding message.

(Garg et al., 2012) proposed a data hiding technique for 3D polygonal models using berry distance. In order to maintain visual quality data is hidden in vertices chosen by the Secure Hash Algorithm (SHA) cryptographic function. Data hiding in this method is based on the floating point arithmetic method. In embedding process, the normal distance of each vertex from center of mass is calculated and the marked vertices are converted to Institute of Electrical and Electronics Engineers-754 (IEEE-754) floating point representation in double precision. Apart from producing good visual quality of stego-image, this method also detects any tampering in the stego-image.

In the above discussed algorithms, either triangle meshes or polygon meshes are formed. The limitation of the existing polygon and triangle mesh based 3D spatial domain image steganography algorithms is that the mesh formation is static for each embedding process. Since the mesh formation is static, same location of pixels are selected for embedding process.

This section discussed the classification of 3D image steganography algorithms. Using the classification, the overview of the 3D frequency domain image steganography algorithms and a detailed outlined of 3D spatial domain image steganography algorithms are discussed in this section. In this thesis, three new spatial domain image steganography algorithms have been proposed and these proposed algorithms are applied to medical domain and Internet banking domain. The medical domain steganography algorithms are discussed as part of 2D spatial domain image steganography algorithm.

The next section discusses the overview and the security issues of Internet banking. It also briefs on some of the methods which provide transaction security and anti-phishing browser plug-in methods as reported in the literature.

2.3. INTERNET BANKING – SECURITY ISSUES

Nowadays Internet has become one of the basic needs for human life. Many day to day activities of human are carried out easily with the help of Internet. Banking domain is greatly benefitted by the Internet as the cost involved in Internet transaction is very less when compared to Automated Teller Machine (ATM), a phone call, a human teller transaction (Reserve Bank of India, 2003). This is depicted through the Figure 2.3.

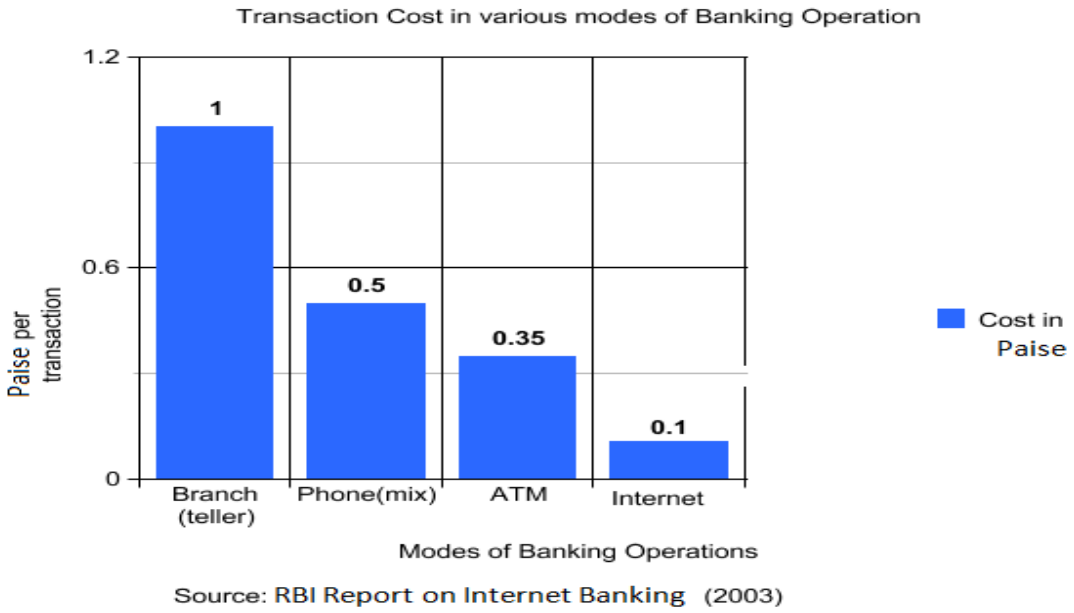


Figure.2.3. Various mode of banking Vs Cost per transaction

Though there are lots of advantages in Internet banking, it has the following threats too they are:

a) Transaction Security
b) Phishing attack
c) Session Hijacking
d) SQL Injection
e) Cross-site scripting

One of the proposed algorithms in this thesis, Dynamic Pattern based Image

Steganography Algorithm (DPIS), is applied to Internet banking to enhance the transaction security and to prevent phishing attack. Hence a brief survey of the existing techniques, which provides transaction security and existing anti-phishing browser plug-ins are discussed here.

2.3.1. Internet Banking – Transaction Security

Banks which offer Internet banking should ensure reliable and secure transactions for their customers. This section explains some of the important techniques in literature which address transaction security.

Secure Socket Layer (SSL) is the security system, which transmits sensitive information like online banking username and password, credit card details over the Internet. SSL is used to encrypt and decrypt the information that is passed on between client and the server. SSL performs 40 bits or 128 bits encryption on the message transmitted in the Internet. The length of the SSL key is directly proportional to security. SSL protocol is analyzed in the (Wagner and Schneider, 1996) and it clearly lists out the issues such as key exchange roll back attack, anonymous key exchange issue and version rollback attack.

In (Hiltgen et al., 2006) proposed a short time password as solution to transaction security – Man in the middle attack. This method is based on Challenge Response procedure where the bank server generates the challenge and the response is generated by the Liquid Crystal Display (LCD) hardware token device such as Verisign or Actividentity or RSA's SecurID solution. The limitations of this method are that it is costly and the user has to carry the extra device and should be trained about the usage of the extra hardware token device.

Advanced Encryption Standard (AES) is the cryptographic algorithm, which is commonly used to encrypt and decrypt messages. Recently hackers have cracked AES algorithm (Biryukov et al., 2010).

This survey clearly points out the need for a technique, which ensures secure online transaction. This research work, proposes an algorithm to enhance the transaction security by combining the cryptography along with steganography. The combined proposed work is explained in the chapter 8. This section explains about some of the existing methods, which are used to enhance the transaction level security. In the next

section, phishing attacks are dealt with and also it discusses various mechanisms which are used to prevent phishing attacks.

2.3.2. Phishing

In Phishing, the attacker tries to imitate legitimate site and gather vital information from the user, which in turn will be used to make control of the user's account. Phishing is the most alarming threat to Internet banking (Fette et al., 2007) and the graph shown in Figure 2.4 shows the number of phishing sites detected in various countries in 2012.

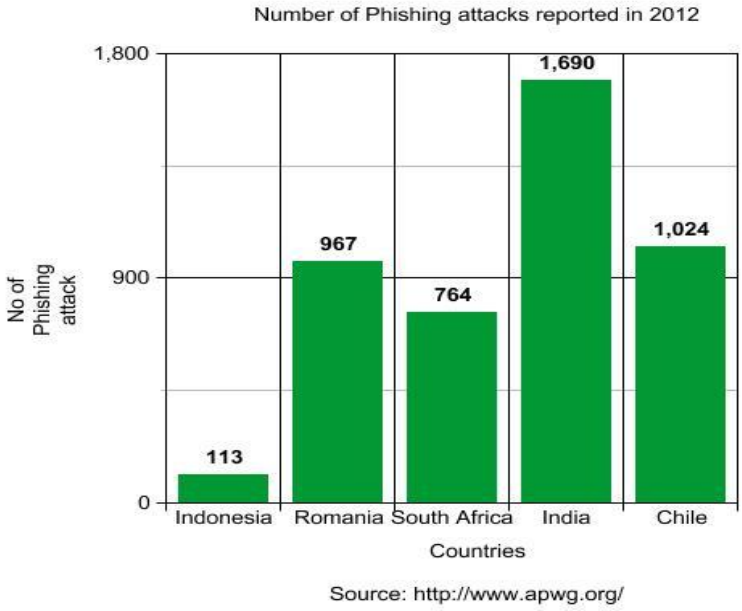


Figure.2.4. Number of phishing site detected in various countries in 2012

2.3.2.1. Anti-phishing Methods

There are number of methods available to prevent phishing attack and these methods are classified into four groups. They are

a) Analyzing Emails (Bergholz et al., 2008, Fette et al., 2007, Wei-Chih and Yu, 2009)
b) Website Content Analysis (Soman et al., 2008, Ma et al., 2009a, Ma et al., 2009b, Garera et al., 2007)
c) Authentication method (Dhamija and Tygar, 2005a, Dhamija and Tygar, 2005b)

d) Anti-Phishing Browser Plug-in (Netcraft [3], TrustWatch [4], Spoofstick [5], ScamBlocker[6])

Since this research focuses on steganography based anti-phishing browser plug-in, a brief survey about these browser plug-ins are given below.

2.3.2.2. Anti-phishing Browser Plug-in

A browser plug-in is a specific component, which is added to the browser for performing some tasks. In this section, the browser plug-ins, which is used to prevent phishing attacks, are discussed.

2.3.2.2.1. Netcraft Plug-in

Netcraft plug-in is introduced for Mozilla browser in the year 2005. This plug-in will display the host location of the website and its risk rating. From the host location and the risk rating, the user can find the authenticity of the website. If the website accessed by the user appears to be suspicious then the user can report it to Netcraft. Netcraft will validate the site and if it is a phished site then it will be stored in blacklisted database so that rest of the user will not fall prey to phished site. The limitation of the Netcraft plug-in is that user should be aware of the host place from where the website is launched.

2.3.2.2.2. TrustWatch Plug-in

TrustWatch is the plug-in for Internet explorer which verifies the identity of the website by displaying the domain name and also checks the Uniform Resource Locator (URL) blacklisted database. If the user accessed URL matches with the blacklisted database then a warning message is displayed to the user about the website authenticity. The limitation of TrustWatch is that it is time consuming since it needs to check all the entries in the black listed database and it falls prey to the new phishing link until it is entered to the blacklisted database.

---

[3] "NetCraft Anti-Phishing Extension" http://toolbar.netcraft.com/ Retrieved on: 01st April 2013
[4] "Firefox Plugin Review: TrustWatch Search" http://www.brighthub.com/computing/smb-security/reviews/50866.aspx Retrieved on: 01st April 2013
[5] "SpoofStick for Internet Explorer" http://spoofstick-for-internet-explorer.software.informer.com/ Retrieved on: 01st April 2013
[6] "Introducing ScamBlocker" http://www.earthlink.net/elink/issue95/security_archive.html Retrieved on: 01st April 2013

2.3.2.2.3. Spoof Stick

In spoof stick installed browser the domain name of the user accessed website is displayed. Pre-requisite to use this plug-in is that the user should have knowledge about the domain name of the site which he/she is accessing. While using the spoof stick, user should check the validity of the domain related information before entering their credentials. The limitation of this plug-in is that user should be aware of the website domain name of the site which he/she is accessing.

2.3.2.2.4. Scam Blocker

ScamBlocker spots the phished site in email by using the eleven tips. These tips will check the entire email for false urgency, spelling mistake, grammar mistake and the validity of any link provided in the mail. ScamBlocker is incorporated with Earthlink mailbox. Hence a person email account in Earthlink will be scanned for phishing threat and if only found legitimate will be displayed in inbox. Scam Blocker limitation is that if the hacker follows a new pattern in the email, which contains the phished link, then the Scam Blocker fails to detect such mail.

The above survey on anti-phishing browser plug-ins clearly portrays that the limitations of the existing anti-phishing browser plug-ins. It also emphasizes the need for anti-phishing browser plug-in which addresses the limitations discussed in this section.

2.4. SUMMARY

In this chapter, the spatial domain 2D image steganography algorithms are classified and the brief descriptions about these classifications are provided. 3D image steganography algorithms are also classified and a brief discussion is provided on the spatial domain 3D image steganography algorithms. The merits and demerits of the 2D and 3D spatial domain image steganography algorithms are also presented in this chapter. It has also outlined the overview and threats of Internet banking. A brief literature study is provided on Internet banking transaction level security mechanisms and anti-phishing plug-in methods.

CHAPTER 3

PROBLEM STATEMENT AND RESEARCH METHODOLOGY

The objective of this research work is to enhance the security of spatial domain 2D and 3D image steganography algorithm using dynamic key. The proposed image steganography algorithms are applied to Internet banking domain and medical domain. This chapter starts with highlighting the problem statement of this research. Section 3.2 focuses on the scope of this research and section 3.3 elaborates on the research methodology followed in this research. The brief summary of this chapter is provided in section 3.4.

3.1. PROBLEM STATEMENT

From the literature survey provided in the previous chapter it is observed that spatial domain 2D and 3D image steganography algorithms have the following shortcomings

- Static key mechanisms for embedding and extraction
- Static pixel selection for embedding secret message
- Static number of bits embedding in the pixel
- Lack of mechanism to check the integrity of the transmitted message

The primary limitation of these static image steganography algorithms is that it can be easily detected by any steganalysis technique (a technique which detects the presence of secret message inside the digital medium). This has led to the research question of "*How to strengthen the spatial domain 2D and 3D image steganography algorithms*?" and this has directed to focus the research towards ameliorating the security of spatial domain image steganography algorithms. Based on the above listed limitations the research problem is formulated. To define the research problem the following research objectives were framed:

- To design and develop dynamic key based spatial domain steganography approaches for 2D and 3D images

- To ameliorate the security aspects of 2D and 3D spatial domain image steganography algorithms using dynamic key
- To explore the applications of dynamic key based image steganography algorithms in various domains

These research objectives helped us to frame the research problem as stated below:

> ***"To design and develop dynamic key based approaches for security amelioration in spatial domain image steganography and to explore its applications"***

This thesis explores the above specified research problem with the help of the following research questions:

Question 1: *How is dynamicity encompassed in spatial domain image steganography?*

Answer: Three different algorithms were proposed in this thesis for ensuring dynamicity in the spatial domain image steganography. The dynamic spatial domain image steganography algorithms proposed in this research for 2D images are, Dynamic Pattern based Image Steganography algorithm (DPIS) and Reversible Dynamic NROI based Steganography algorithm using graph coloring (RDS). Pattern Based 3D Image Steganography (PBIS-3D) algorithm is proposed for encompassing dynamicity in spatial domain 3D image steganography.

In DPIS, the dynamic key is generated using the random color sequence for each embedding process whereas in RDS algorithm, the dynamic key is generated using the cover-image. Based on the cover-image, the graph is assigned to it and the graph is solved for graph 3-coloring problem to obtain the key. In PBIS-3D algorithm, the dynamic key is generated using the secret message. The secret messages are used to form the triangle mesh and the vertices of the triangle mesh are used for embedding and extracting. The diagrammatic representation of how dynamicity is encompassed in the proposed algorithm is shown in Figure 3.1.

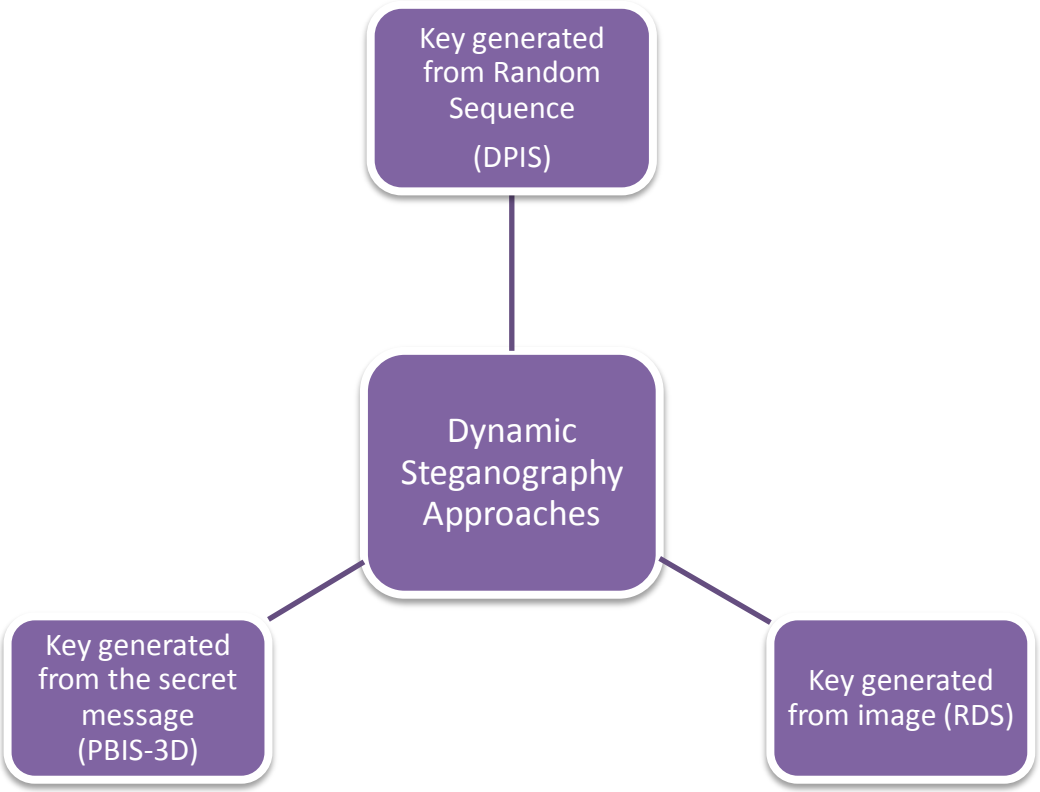


Figure.3.1. Diagrammatic representation of the proposed dynamic steganography approaches

Question 2: *How is security strengthened in spatial domain image steganography using the dynamic key?*

Answer: This thesis uses the dynamic key generated in the DPIS, RDS and PBIS-3D algorithms for ameliorating security in spatial domain image steganography. These dynamic keys are used to select pixels for embedding secret message bits and it is also used to determine the number of secret message bits to be embedded in the selected pixels. This thesis also tests the stego-images generated by the three proposed dynamic spatial domain image steganography algorithms by exposing them to different attacks and their behaviors were analyzed to understand its stamina against the attacks.

Question 3: *What are all the domains where the proposed 2D and 3D dynamic image spatial domain image steganography algorithms are applied?*

Answer: The proposed DPIS algorithm is applied to Internet banking domain to enhance the transactional level security and to prevent phishing attack. RDS and

PBIS-3D algorithms are applied to the medical domain for hiding patient record information in medical images.

3.2. SCOPE OF RESEARCH

This research is focused on the design and implementation of robust dynamic spatial domain image steganography algorithms. In the proposed spatial domain 2D image steganography algorithms the dynamicity is ensured by the dynamic key generated using the color sequence and the cover-image. In spatial domain 3D image steganography algorithm the dynamicity in generating the key is ensured by the secret message. These proposed algorithms were implemented and the research findings are depicted as Tables and Figures. Internet banking domain is chosen for applying the DPIS algorithm and medical domain is chosen for applying the RDS and PBIS-3D image steganography algorithms.

3.3. RESEARCH METHODOLOGY

The research commenced with an exhaustive survey with classification of 2D and 3D spatial domain image steganography algorithms. Performance analysis of the steganography algorithms reveals that spatial domain steganography algorithms can embed large amount of message bits but robustness and imperceptibility properties of this domain are weak, where as in frequency domain, embedding capacity is less but robustness and imperceptibility properties are high compared to spatial domain.

This research is an attempt to strengthen the spatial domain image steganography algorithm through dynamic key generation thereby enhancing the security. The research methodology followed in this work is algorithmic and experimental approach (Panneerselvam, 2004). As an outcome of the algorithmic approach robust dynamic and secure 2D and 3D spatial domain image steganography algorithms were devised. Following an experimental research methodology, the proposed algorithm Dynamic Pattern based Image Steganography (DPIS), Reversible Dynamic NROI based Steganography algorithm using graph coloring (RDS) and Pattern Based 3D Image Steganography (PBIS-3D) algorithm were implemented and tested for robustness, capacity, invisibility and statistical parameters. The proposed algorithms were compared with similar algorithms against various parameters. The overall framework

of this research, which is depicted in Figure 3.2, contains three main components namely,

- Dynamic steganography algorithms
- Domains where these dynamic steganography algorithms are applied
- Metrics which are used to evaluate the dynamic steganography algorithms

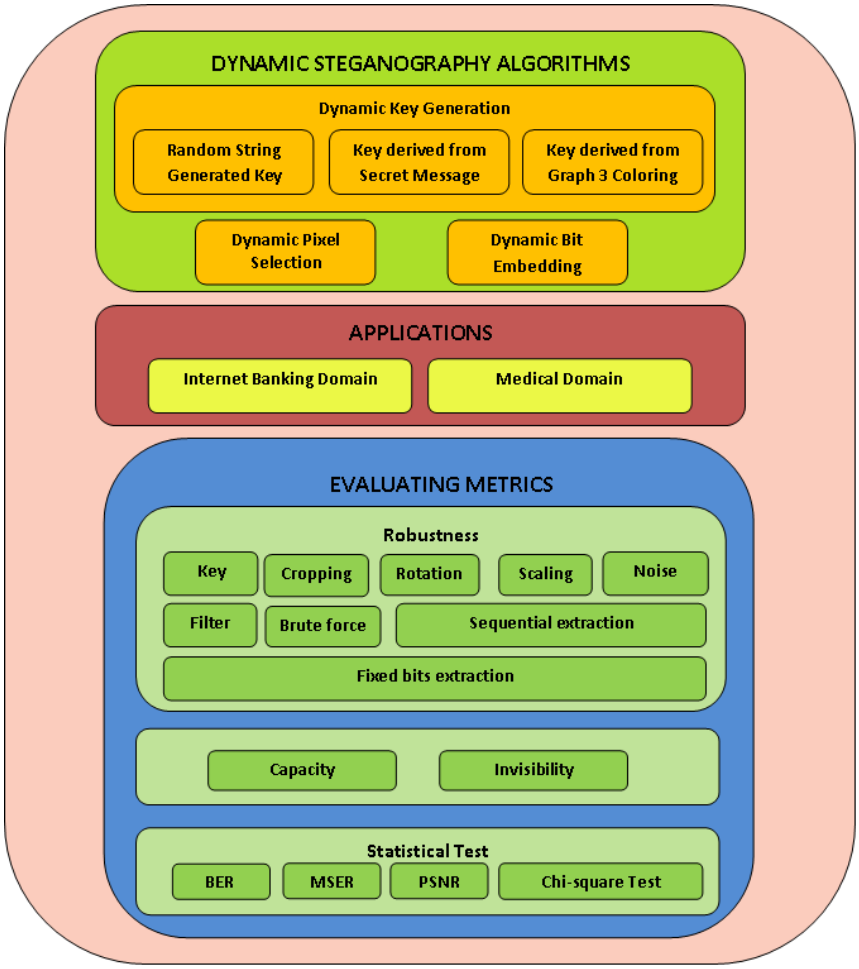


Figure.3.2. Research framework

Robustness of the three proposed algorithms is tested by analyzing the strength of the key and the algorithms behavior are analyzed with the attacks such as cropping, scaling, rotation, median filter, Gaussian filter, resistance with noise , brute force attack, sequential extraction attack and fixed bits extraction attack. The invisibility of the proposed algorithms was tested with the histogram analysis. Capacity metric is used to find the number of pixels used for embedding various lengths of secret messages.

Peak Signal to the Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER) and Chi-square test are the parameters, which are used to test the statistical property of the stego-image generated by the proposed algorithms.

The proposed DPIS, RDS and PBIS-3D algorithms are applied to real time applications. DPIS algorithm is applied in Internet banking to enhance transaction level security and to prevent phishing attack. RDS and PBIS-3D algorithms are applied in medical domain to hide the patient information inside the medical images.

3.4. SUMMARY

This chapter has brought out the problem definition that is being attempted upon in this research. It has highlighted the objectives of research and outlined the scope of the research. The methodology that is followed in this research work and the parameters used to evaluate the proposed algorithms are also portrayed in this chapter.

CHAPTER 4

DYNAMIC PATTERN BASED IMAGE STEGANOGRAPHY ALGORITHM

This research work aims to develop spatial domain image steganography algorithms which include dynamic pixel selection and embedding variable bits in the pixel chosen. The dynamic pixel selection is achieved by the generation of random string with combinations of red, green and blue channels. The traditional way of sequential embedding is eradicated in this algorithm by analyzing the color value of the pixel. This chapter starts with explaining the need for the dynamic spatial domain image steganography algorithm. The three main components of Dynamic Pattern based Image Steganography (DPIS) algorithm namely key generation, embedding algorithm and extraction algorithm are elaborated in detail.

4.1. NEED FOR DYNAMIC IMAGE STEGANOGRAPHY ALGORITHM

In spatial domain image steganography, the secret message bits are embedded in the Least Significant Bit (LSB) of each pixel in the cover-image which is known as LSB technique. As most of the spatial domain image steganography algorithms are static in nature it paves way for attackers to predict the presence as well as extract the secret message from the stego-image. In order to make the detection of secret message in the stego-image as a hard process, dynamicity needs to be introduced in spatial domain image steganography algorithm.

In this direction, this section presents the DPIS algorithm which incorporates dynamicity in the selection of pixels and dynamicity in the number of bits to be embedded in each pixel. The dynamicity is ensured by the key generated for each embedding process. The dynamic pixel selection and dynamic embedding of bits in the pixel strengthens the security of the spatial domain image steganography algorithm.

4.2. DYNAMIC PATTERN BASED IMAGE STEGANOGRAPHY (DPIS) ALGORITHM

Each pixel in the color image consists of red, green and blue colors. Each color in the pixel is represented as eight bits and they are called as color channels. DPIS algorithm is based on the concept that secret messages are embedded in the color channel which contributes less to the pixel color. The goal of the DPIS algorithm is to select the pixel dynamically for embedding and to embed variable number of bits in the pixel. The detailed description of the DPIS algorithm is discussed in this section and it contains five tuples as shown in Eq. 4.1.

$$DPIS = \{CI, SM_i, K_s, Embedding\ (CI, SM_i, K_s), Extraction\ (SI, K_s)\} \quad (4.1)$$

where

CI – Cover-image
SM_i – Secret Message
K_s – Key
SI – Stego-image
Embedding (CI, SM_i, K_s) – DPIS Embedding algorithm
Extraction (SI, K_s) – DPIS Extracting algorithm

Generation of key, Embedding algorithm and Extracting algorithm are the three main phases of the DPIS algorithm and it is described below.

4.2.1. Generation of Key

The DPIS algorithm starts with the generation of the key K_s which contains Red (R), Green (G) and Blue (B) colors and it is represented in Eq. 4.2.

$$K_s = K_1K_2K_3 \ldots K_q\ ;\quad K_s \in \{R, G, B\} \quad (4.2)$$

The length (q) of the generated key should be greater or equal to 20 and it is shown in Eq. 4.3. As the length of the key is directly proportional to the security of the DPIS algorithm, K_s generated here is of large length and the details of the key length is given in the section 7.6.1.1.

$$q = \text{Len}(K_s); \quad 20 <= q <= \infty \tag{4.3}$$

The mandatory condition for generation of key is that it should contain at least one R, one G and one B in it. The generation of the key is the crucial part in DPIS algorithm as the key is the basis for embedding the message in the cover-image. For every embedding process different keys of different lengths will be generated which ensure dynamicity and security. The following section explains the DPIS embedding algorithm using the key generated in this section.

4.2.2. DPIS Embedding Algorithm

DPIS embedding algorithm takes the cover-image, secret message and the key as input and it embeds the secret message in the cover-image. The output of the DPIS embedding algorithm is the stego-image where the secret message has been embedded. Each pixel in the cover-image contains red, green and blue channels which are depicted in Eq. 4.4.

$$P_i = \{P_1, P_2, P_3, \ldots, P_N\} \tag{4.4}$$

where P_i contains R,G and B colors and $i=1,2,\ldots,N$

P_i is the pixel in the cover-image and

N is the total number of pixels in the cover-image

Each character in the secret message (SM) which is to be embedded in cover-image is converted into binary (SMB) and it is represented in Eq. 4.5 and Eq. 4.6.

$$SM = S_1S_2S_3\ldots S_z \quad \text{where } 1<=Z<=\text{Length (SM)} \tag{4.5}$$

$$SMB = b_1b_2b_3\ldots b_{(Z*7)} \tag{4.6}$$

where $SMB \in \{0, 1\}$ and $1<=Z<=\text{Length (SM)}$

Each color K_1 to K_q from K_s, which is generated in the previous section, is assigned to each pixel in the cover-image in rotation fashion and it is represented in Eq. 4.7

$$\text{Assigning color in Key } K_s \text{ to } P_i = \{ K_1P_1, K_2P_2, \ldots, K_qP_q, K_1P_{q+1}, K_2P_{q+2}, \ldots, K_{1\ldots q}P_N\} \tag{4.7}$$

In Eq. 4.7 ‘q’ indicates the length of the key K_s generated and ‘N’ indicates the total number of pixels in the cover-image. Each pixel P_i contains R, G and B color channels. The color that is assigned for the pixel in the cover-image from K_s is named as indicator channel. The remaining two unnamed channels in the pixel are compared for the lowest value and the channel with lowest value is termed as data channel. The left out unnamed channel is termed as the third channel.

Indicator channel value is compared with the other two channel values. If the indicator channel is the lowest value compared to the other two values then that pixel is skipped from embedding. This part of the embedding algorithm gets rid of the sequential pixel embedding. The Least Significant Bit (LSB) of data channel is checked for zero. If LSB of data channel is zero then two bits of the secret message are embedded in the data channel. If the LSB of the data channel is one then three bits of secret message are embedded in it. This part of the embedding algorithm ensures that the channel with more contribution to the pixel color does not suffer from embedding.

Based on the number of bits embedded in the data channel, the Least Significant Bit (LSB) of the third channel is modified. If two bits are embedded in the data channel then LSB of the third channel is made zero. Otherwise if three bits are embedded in the data channel then LSB of the third channel is made one.

In the extraction part, from among the three channels in a pixel, indicator channel is identified from the secret key. To identify the location of the data channel in the pixel, indication is provided in the LSB of the indicator channel. If the data channel follows immediately the indicator channel then the LSB of indicator channel is assigned zero else the LSB of indicator channel is assigned one. The pseudo code of the embedding algorithm (DPIS_Embedding) is depicted in the Figure 4.1.

The output of the DPIS embedding algorithm is the stego-image (SI) which contains the secret message. The stego-image is transmitted to the intended recipient who extracts the secret message from stego-image using extraction algorithm which is explained in the next section.

Algorithm for DPIS Embedding

Input: *Cover-image CI, Secret Message SM, Key K_s*
Output: *Stego-image SI*

DPIS_Embedding (CI, SM, K_s)
Begin
Assign color from K_s to $\forall P_i$ in CI in rotation fashion;
While (all SM bits are not embedded)
{
$\forall P_i$ the assigned color from K_s is Indicator channel
if (low(R_i , G_i , B_i)) matches with Indicator channel
*Skip; /*Skipping pixel from embedding */*
else if (K_s = R_i)
{
Data channel = low (G_i , B_i);
Left out channel is Third channel;
New_P_i = Function_Embed(P_i , Indicator channel ,Data channel , Third channel, SM);
}
else if (K_s = G_i)
{
Data channel = low (R_i,B_i);
Left out channel is Third Channel;
New_P_i = Function_Embed(P_i , Indicator channel ,Data channel , Third channel, SM);
}
else if (K_s = B_i)
{
Data channel = low (R_i,G_i);
Left out channel is Third Channel;
New_P_i = Function_Embed(P_i , Indicator channel ,Data channel , Third channel, SM);
}
stego_image=New_P_i;
Move to next P_i ;
}
return stego_image;
End

Function in DPIS embedding process

Input: *P_i , Indicator channel ,Data channel , Third channel, SM*
Output: *Stego_Pixel P_i*

Function_Embed (P_i , Indicator channel ,Data channel , Third channel, SM)
Begin
If ((Data channel mod 2) = 0)
{
New_DC = Embed 2 bits of SM in the LSB of Data channel
If ((Third channel mod 2) =1)
{
New_TC = Assign Third channel LSB '0'
}
If (Data channel follows immediately the Indicator channel)
{
New_IC =Assign Indicator channel LSB '0'
}

```
    }
     If ( (Data channel mod 2) = 1)
    {
          New_DC = Embed 3 bits of SM in LSB of  Data channel

        If ( ( Third channel mod 2) =0)
        {
          New_TC = Assign Third channel LSB '1'
        }
        If (Data channel not follow immediately the  Indicator channel )
        {
           New_IC = Assign Indicator channel LSB '1'
        }
    }

Stegopixel_Pi = ( New_IC , New_DC , New_TC )
return Stegopixel_Pi ;
End
```

Figure.4.1. DPIS Embedding Algorithm

4.2.3. DPIS Extracting Algorithm

In DPIS extraction algorithm, stego-image and the key are given as input. The key K_s generated in embedding algorithm is transmitted to the extraction part. The stego-image is represented as set of pixels in Eq. 4.8.

$$SI = \{P_1, P_2, P_3, \ldots, P_N\} \quad (4.8)$$

where $P_i \in \{ R,G,B\}$; $i=1,2,\ldots,N$

SI is the stego-image and

N is the number of pixels in the stego-image

Each color K_1 to K_q from K_s, which is obtained from embedding algorithm, is assigned to each pixel in the stego-image in rotation fashion and is shown in Eq. 4.9.

$$\text{Assigning color in Key } K_s \text{ to } SI = \{ K_1P_1, K_2P_2, \ldots, K_qP_q, K_1P_{q+1}, \ldots, K_{1\ldots q}P_N\} \quad (4.9)$$

In Eq. 4.9 'q' indicates the length of the key and 'N' indicates the number of pixel in the stego-image. The color which is assigned from K_s to a pixel is called as indicator channel. If the indicator channel has the lowest value from other colors in the pixel then the pixel is skipped from extraction. If the indicator channel is not the lowest then the extraction continues. Apart from the indicator channel, the data channel has to be identified to extract the secret message bits. To identify the location of data channel in a pixel, the LSB of indicator channel is examined. If the LSB of indicator channel is '0' then the channel which follows the indicator channel immediately is named as the data channel.

If the LSB of indicator channel is '1' then the channel which is before the indicator channel is named as the data channel. Out of the three channels in the pixel, two channels are named as the indicator channel and data channel. The left out unnamed channel is termed as the third channel. Before extracting the secret message bits from the data channel, the number of bits embedded in each pixel needs to be determined. To find this, the channel apart from indicator and data channel, which is named as third channel, is examined. If the LSB of third channel is zero then two bits of secret message is extracted from data channel. Otherwise if LSB of third channel is one then three bits of secret message are extracted from data channel.

Algorithm for DPIS Extraction

Input: *Stego-image SI, Key* K_s
Output: *Secret Message SM*

DPIS_Extraction (SI, K_s ***)***
Begin
Assign color from K_s *to* $\forall P_i$ *in SI in rotation fashion;*
While (all SM bits are not extracted)
{
$\forall P_i$ *the assigned color from* K_s *is Indicator channel;*
if (low(R_i*,* G_i *,*B_i*)) matches with Indicator channel*
*Skip; /*Skipping pixel from extraction */*
*else if (LSB of Indicator channel is '0') /*To fetch the data channel*/*
{
Channel which follows immediately the Indicator channel is the Data channel
Channel apart from Indicator and Data channel is named as Third channel
}
else if (LSB of Indicator channel is '1')
{
Channel which is before the Indicator channel is the Data channel
Channel apart from Indicator and Data channel is named as Third channel
}
*if (LSB of Third channel is '0') /*To get the number of bits embedded in data channel*/*
{
SM=Extract two bits of secret message from LSB of Data channel
}
else if (LSB of Third channel is '1')
{
SM=Extract three bits of secret message from LSB of Data channel
}
Move to next P_i *;*
} return SM;
End

Figure.4.2. DPIS Extraction Algorithm

The pseudo code of the extracting algorithm (DPIS_Extraction) is explained in Figure.4.2. Figure 4.3, Figure 4.4 and Figure 4.5 shown are sample categories of cover-image and stego-images generated by DPIS algorithm with various lengths of secret message embedded in it. The implementation and the experimental results of

the DPIS algorithms have been dealt with Chapter 7. The application of DPIS algorithm is discussed in Chapter 8.

Figure.4.3. Mona Lisa Cover-image (left) and Stego-image (right) with 60,000 bits embedded by DPIS algorithm Image Size: 300 x 266

Figure.4.4. Flower Cover-image (left) and Stego-image (right) with 80,000 bits embedded by DPIS algorithm Image Size: 323 x 429

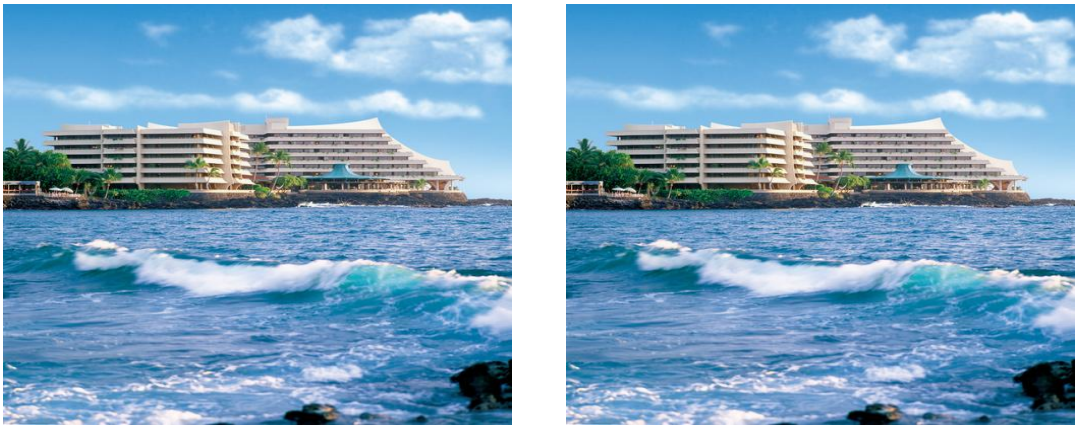


Figure.4.5. Sea Cover-image (left) and Stego-image (right) with 1, 00, 000 bits embedded by DPIS algorithm Image Size: 375 x 480

4.3. SUMMARY

This chapter elaborates the need for the dynamic spatial domain image steganography algorithm. The three main phases of the DPIS algorithm such as generation of key, embedding algorithm and extraction algorithm are discussed in detail. This chapter discusses DPIS algorithm in which the dynamicity is ensured by the random key generation where as the next chapter discusses a spatial domain image steganography algorithm in which the dynamicity is ensured by the cover-image.

CHAPTER 5

REVERSIBLE DYNAMIC NROI BASED STEGANOGRAPHY ALGORITHM USING GRAPH COLORING

The development of Dynamic Pattern based Image Steganography (DPIS) algorithm leads to the design of an algorithm considering dynamicity and reversibility. In this perspective, this research work aims to develop a reversible dynamic spatial domain image steganography algorithm. In this approach the given image is spilt into Region of Interest (ROI) and Non Region of Interest (NROI) and the secret message is embedded in the NROI using the key generated by the graph 3-coloring problem. This chapter starts with explaining the need of Reversible Dynamic NROI based Steganography Algorithm using Graph Coloring (RDS). The main phases of RDS algorithm which are discussed in this chapter are identification of ROI, deriving key from ROI, RDS embedding and extraction algorithm.

5.1. NEED FOR RDS ALGORITHM

Generally in the extraction part of the steganography algorithm the secret message bits alone are extracted from stego-image. As discussed in section 2.1.1.4 the extraction algorithm which tries to revert the cover-image from stego-image apart from extracting the secret message is called as reversible image steganography algorithm. Moreover most of the spatial domain steganography algorithms are static in their nature and this feature easily reveals the presence of secret message inside the digital medium. In this chapter, a novel spatial domain steganography algorithm is proposed which addresses dynamicity and reversible property.

The dynamic key is generated with the help of cover-image and for different cover-image different keys will be generated. The dynamic key is used in RDS algorithm as it strengthens the security of embedding and extraction algorithm. The reversible property is achieved in the proposed RDS algorithm by exploiting the background color of the image. In the next section the important phases of RDS algorithm are discussed.

5.2. REVERSIBLE DYNAMIC NROI BASED STEGANOGRAPHY ALGORITHM USING GRAPH COLORING

Reversible dynamic steganography algorithm using graph coloring generates key from the cover-image. Each time when a new cover-image is chosen for embedding different keys will be generated. RDS algorithm consists of six tuples which are shown in Eq. 5.1.

RDS = {CI, SM, GK(CI), Embedding (CI, K_s, SM), GK(SI), Extraction (SI, K_s) }(5.1)

where

CI – Cover-image

SM – Secret Message

GK(CI) – Key generation procedure from cover-image (CI) where the generated key is denoted by K_s

Embedding (CI, K_s, SM) – RDS Embedding algorithm

GK(SI) – Key generation procedure from stego-image (SI) where the generated key is denoted by K_s

Extraction (SI, K_s) – RDS Extracting algorithm

The important phases of RDS algorithm are embedding and extraction. These phases are explained in detail in the below section. The overall architecture of the proposed RDS algorithm is shown in Figure 5.1.

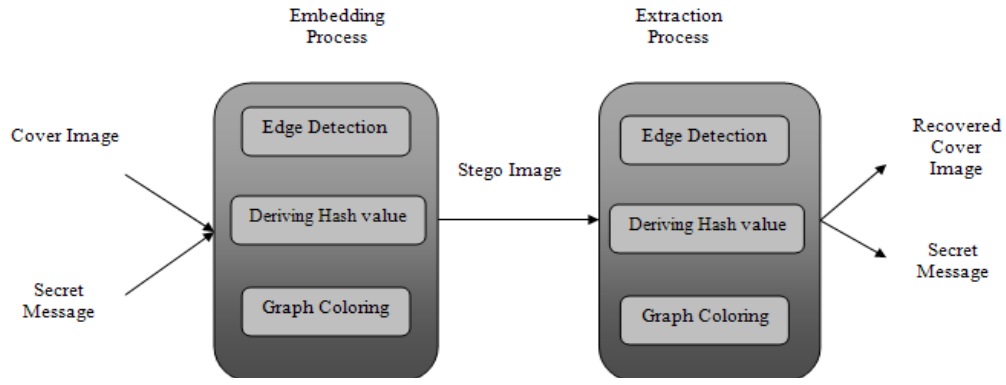


Figure.5.1. Architecture of RDS algorithm

Embedding and extracting algorithm has the following sub-components:

a) Identification of Region of Interest (ROI) and Non Region of Interest (NROI) in the image through edge detection technique

b) Deriving hash value from ROI of the image to get the graph
c) Solving the graph for 3-coloring to get the key.

Each subcomponent is elaborately discussed in the following section.

5.2.1. Identification of ROI and NROI in the Image

The image content is divided into two regions, Region of Interest (ROI) and Non Region of Interest (NROI). The significant part of the image which is of user's interest is termed as ROI and rest of the portion of the image is termed as NROI. Edge detection technique is used to distinguish ROI from NROI in an image. There are many edge detection techniques (Nadernejad et al., 2008) such as Marr-Hildreth edge detector, canny edge detector, local threshold and boolean function based edge detection. These edge detection techniques identify the points in the image at which the brightness changes and separate ROI and NROI. The performance of the edge detection techniques are analyzed in (Nadernejad et al., 2008) based on the two important metrics such as probability of false positive and false negative. Based on the performance (Nadernejad et al., 2008), canny edge detection is employed in the proposed RDS algorithm. Canny edge detection method is applied on the brain image and it is shown in Figure 5.2.

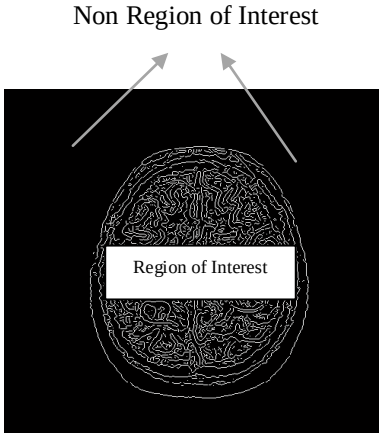


Figure.5.2. Canny edge detection technique applied on brain image

Among the many white lines shown in Figure.5.2, the outer white line is taken as boundary which separates the ROI from NROI. The region inside the outer white line irrespective of the background is termed as ROI and portion outside the outer white boundary is termed as NROI. RDS algorithm is proposed for images which are split

into single ROI and NROI .The next section describes how the hash value is derived from the ROI of the image.

5.2.2. Deriving Hash Value from the ROI of Image

Using the canny edge detection technique, the ROI in the image is identified. As mentioned in the architecture in Figure 5.1, after identifying the NROI and ROI region using canny edge detection technique, the next step is to derive the hash value from the ROI.

a) All the pixels in ROI are taken into consideration to derive the hash value which is represented by the Eq. 5.2.

$$ROI = \{ P_1, P_2 , P_3 \ldots P_n \} \quad (5.2)$$

where P_i is the pixel in ROI and n is the total number of pixels in ROI.

b) MD5 hash function is applied on the sum of all pixels in ROI and it is shown in Eq. 5.3.

$$\text{Hash value} = MD5\left(\sum_{i=1}^{n} Pi\right) \quad (5.3)$$

The key is obtained from the sum of all pixel values in ROI, hence to provide confidentiality MD5 hash function is applied to it (Todorov, 2010). The sum of all pixel value from ROI region is used to identify the graph for the given image. The identification of the graph and how it is solved for graph 3-coloring problem to get the key is explained in the next section.

5.2.3. Identification of Graph and Deriving its Coloring Sequence

The next step in the embedding process is to identify the graph based on the ROI hash value and derive coloring sequence for each image. The procedure that is used to identify the graph and to derive the key from the graph for the image is explained in this section. The first step in this process is to obtain the graph index from the hash value and it is shown in Eq. 5.4.

$$\text{Graph index} = (\text{Hash value}) \bmod \text{`n'} \quad (5.4)$$

where 'n' is the number of entries in the shared Table 5.1.

In order to map the hash value generated in the previous section to the graph index in the Table 5.1, modulo operation is performed on the sum of ROI pixel values with the number of entries in the shared table (n). The graph index thus obtained is used to get the graph for the image from the Table 5.1 which is shared between the embedding and the extraction part. The shared table contains two entities, graph index and the graph and the sample is shown in Table 5.1.

Table.5.1. Shared table between embedding and extraction part

Graph Index	Graph $K_{r,n}$
0	$K_{2,25}$
1	$K_{3,30}$
2	$K_{2,30}$
3	$K_{3,25}$
4	$K_{2,28}$
…	…
…	…
n-1	$K_{2,24}$

Graph indices varies from 0 to n-1 and tree graphs are taken for the experiments and it is represented by the symbol $K_{(r,n)}$ where ‘r’ represents the number of root vertices and ‘n’ represents the number of leaf nodes in the graph. The number of root vertices ‘r’ in the tree graph taken for the experiments varies among 1, 2 and 3 where as number of leaf nodes are taken above 20. The image taken for RDS embedding is assigned with one of tree graph from Table 5.1 based on their ROI values.

Generally Table 5.1 contains large number of entries and there may be rare cases where for two different images the hash value and graph index may be the same. In such rare cases the same tree graph is assigned to the image which will result in same key for two different images. The graph entries in Table 5.1 are static but they can be changed for obtaining different keys which make the behavior of RDS algorithm unpredictable to the attacker.

The graph obtained for the image is solved for graph 3-coloring problem and the resultant color sequence is used as the key for both the embedding and the extraction process. The reason for choosing graph 3-coloring problem to derive the key are mentioned below:

a) Key need not be transmitted from embedding part to the extraction part as the key is derived from the graph which is assigned for the cover-image and the stego-image using the procedure discussed in Figure 5.4.

b) As the key is derived from the stego-image it need not be stored in the database

c) Toughness in solving the graph 3-coloring problem

The rule for coloring the vertices of the graph in 3-coloring problem is that, the vertices which are connected by edges should not have the same color. There are many ways to solve graph 3-coloring problem. In order to obtain the same key at the embedding and extracting part the same coloring procedure has to be followed.

The pseudo code of the method which is used to solve graph 3-coloring problem in RDS algorithm is given in Figure 5.4. Three colors 0, 1 and 2 are used in RDS algorithm to color the vertices of the tree graph from top to bottom in clock wise direction and it is shown in Figure 5.3. The resultant coloring sequence is used as the key in both the embedding and extraction algorithm. With the help of color sequence (key) obtained from the graph 3-coloring problem secret message bits are embedded in the cover-image with the help of embedding algorithm which is explained in next section.

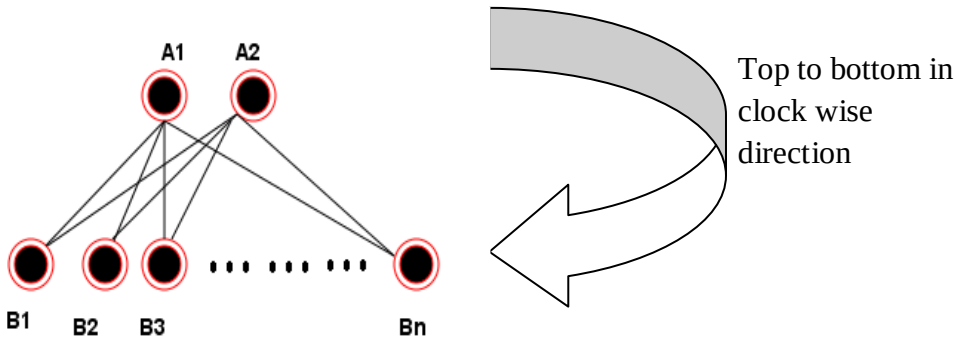


Figure.5.3. Graph 3-coloring from top to bottom in clock wise direction

Algorithm to obtain the coloring sequence of the graph

Input: *Graph* $K_{r,n}$
Output: *Coloring Sequence of the vertices (key)* K_s

RDS_3 coloring sequence (graph)

Begin

Color $(V_i) \in \{0, 1, 2\}$ $1 \leq i \leq n$ *where 'v' is the vertices in the Graph and 'n' is the number of vertices in the graph*
Vertex coloring is done from top to bottom in clock wise direction of the graph
While(all vertices are not colored)
{
$\forall V_i$ *get the vertices it is connected and it is denoted by* Con_V_i
$\forall V_i$ *Color*(V_i) *should be assigned in order of {0,1,2} such that* $color(V_i) \neq color(Con\_V_i)$
}
K_s *= Arrange the Color*(V_i) *from top to bottom in clock wise direction*

End

Figure.5.4. RDS Graph 3-coloring algorithm

5.2.4. RDS Embedding Algorithm

As discussed in section 5.2.1, canny edge detection technique is used to segregate the cover-image into ROI and NROI. As ROI part of the cover-image is very crucial it is not affordable for embedding secret message. Hence NROI portion of the cover-image is chosen for embedding the secret message. Apart from this, the process of transmission of stego-image needs to maintain the integrity of the ROI pixels. In order to achieve the integrity, ROI hash value is embedded in preselected pixels of NROI region. ROI hash value is embedded in NROI pixels when the count of the pixel in NROI region matches with the number in the series which is given by the Eq. 5.5.

NROI pixels for embedding ROI hash value = k, k+d, k+2d, … , k+ (n-1)*d (5.5)
where

'k' is any number within the count of NROI pixels
'd' is the difference between two consecutive numbers in the series
'n' is the total count of NROI pixels in which the hash value of ROI is embedded

As the above pixels in the series shown in Eq. 5.5 are embedded with the hash value of ROI, these pixels are free from embedding the secret message bits. Each color in the key which is obtained in the previous section is assigned sequentially to NROI pixels except for those pixels in Eq. 5.5.

The secret message will not be embedded in the pixels which are assigned with color '0'. One bit and two bits of secret message are embedded in the pixels which are assigned with color '1' and '2' respectively. Figure 5.5 explains the overview of RDS embedding algorithm. The pseudo code of RDS embedding algorithm is explained in the Figure 5.6. RDS embedding process has the following properties:

a) Eradicates sequential embedding of the secret message by not considering the pixels which is assigned with color zero and the pixels in the NROI pixel series given in Eq. 5.5.
b) Embeds variable numbers of bits to the pixel based on the color (key) assigned to it.

The stego-image obtained from the embedding procedure is taken as input for the extraction algorithm. In RDS algorithm the stego-key need not be transmitted to the extraction part and it is computed at the extraction process. The detailed extraction algorithm is explained in the following section.

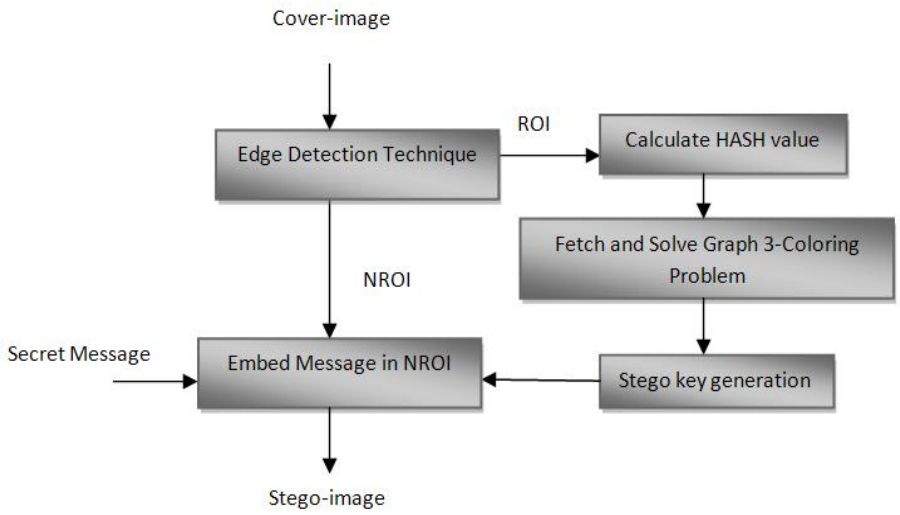


Figure.5.5. Overview of RDS embedding algorithm

Algorithm for RDS Embedding

Input: *Cover-image CI , Key K_s , Secret Message SM*
Output: *Stego-image*

Embedding (CI, K_s ,SM)
Begin

*Embed the hash value of ROI in the series k, k+d, …,k+ (n-1)*d where 'k' is number within the count of NROI pixel, 'd' is the difference between two number in the series and 'n' is total number of NROI pixels in which the hash value of ROI is embedded*

Convert SM to bits
*$\forall$ pixel P_i in NROI assign each color in the K_s in rotation fashion except for those NROI pixel who's count are in the series k, k+d, k+2d, …, k+ (n-1)*d*

```
While (all SM bits are not embedded in NROI region)
{
    if (Pi assigned Ks = 0)
        // do nothing;
    else if (Pi assigned Ks = 1)
    {
        Stego_Pixel=embed '1' bit of SM in LSB of Pi
    }
    else if (Pi assigned Ks = 2)
    {
        Stego_Pixel=embed '2' bits of SM in LSB of Pi
    }
    Move to next Pi ;
}
Stego-image = Stego_Pixel;
return Stego-image;
```

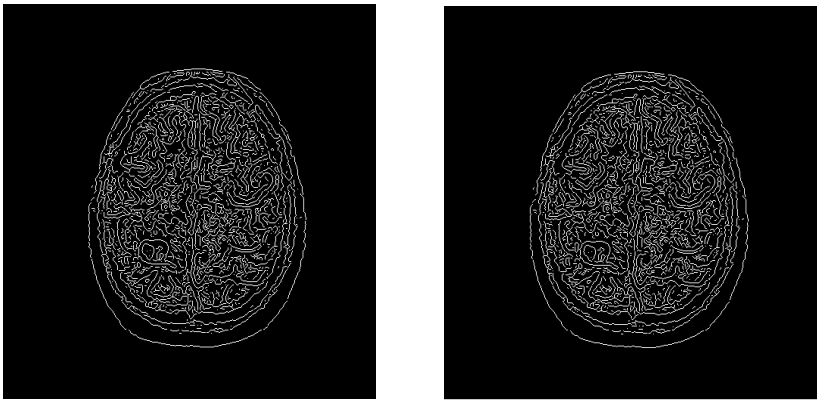
End

Figure.5.6. RDS embedding algorithm

5.2.5. RDS Extraction Algorithm

The first step in RDS extraction algorithm is to identify ROI and NROI in the stego-image using the canny edge detection technique. Though secret message is embedded in stego-image, the edge detected in stego-image is identical to the cover-image and it is shown in Figure.5.7.

The second step in RDS extraction procedure is deriving hash value from ROI. With the help of the hash value the graph is obtained for the particular stego-image from the shared table and it is solved for graph 3-coloring problem. The resulting color sequence for the assigned graph is used as the key for extraction. Before extraction, the transmitted stego-image needs to be checked for its integrity.



(a) (b)

Figure.5.7. Canny edge detection of (a) Cover-image (b) Stego-image which contains the secret message of about 1500 bits

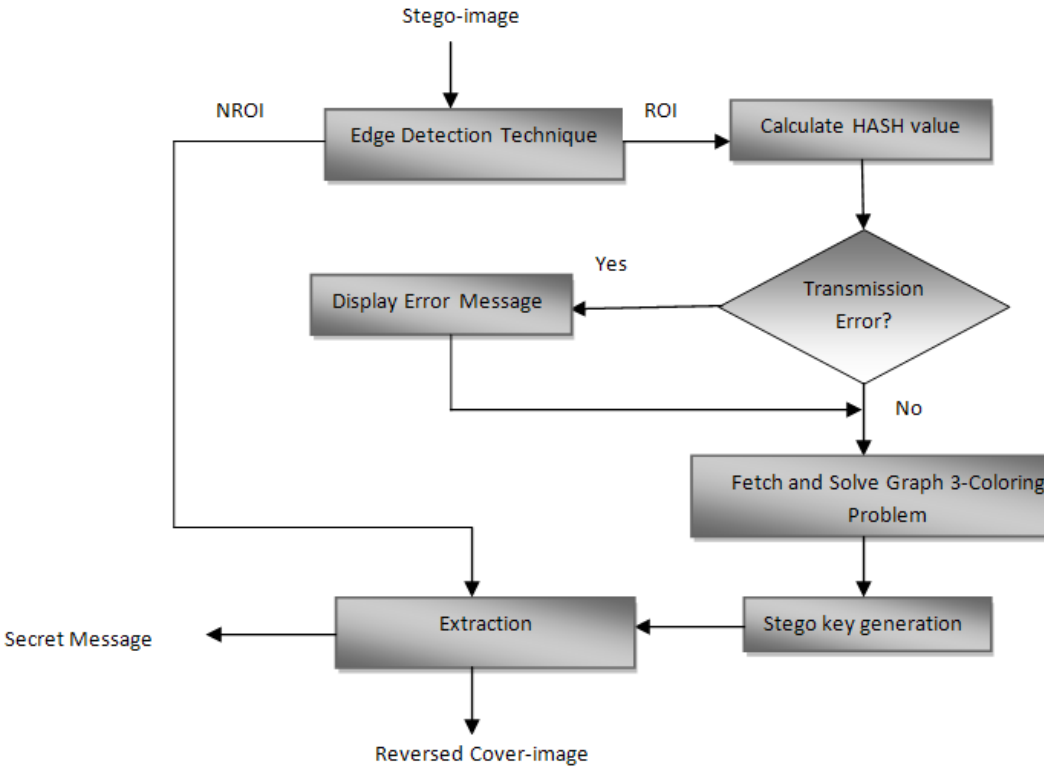


Figure.5.8. Overview of RDS extraction algorithm

The integrity of the transmitted stego-image is checked by comparing the hash value of ROI with the NROI pixel in the series. The possibilities that occur while comparing the hash value of ROI with the NROI series pixel are given below:

a) If more than half of the extracted value from NROI series matches with the ROI hash value then it can be concluded that there will be negligible transmission error and the extraction procedure continues.

b) If there are less than or equal to half of the extracted value from NROI series matches with the ROI hash value then there are two possibilities
   - Transmission error in ROI of stego-image
   - Transmission error in NROI of stego-image

In both cases error message is displayed to the user about the integrity of the stego-image and the extraction continues. If error occurs in ROI then the key generated will not be correct and hence junk secret message will be extracted from the stego-image. If error occurs in NROI then the embedded secret message bits will be altered.

From the stego-image ROI hash value, graph index and the graph are obtained. The obtained graph is solved for 3-coloring problem and the solution is used as extraction key. In the RDS extraction algorithm the key is not transmitted from the embedding part, rather it is generated in extraction part itself. Each color from the key is assigned to the NROI pixels sequentially. If color '0' is assigned to the pixel then that pixel is free from extraction. If color '1' is assigned to the pixel then one bit of secret message is extracted from the pixel. If color '2' is assigned then two bits of secret message are extracted from the stego-image pixels.

To achieve reversibility property, the predominant color in the NROI region is identified. This predominant color in the NROI region is used to replace the pixel value from where the secret message bits are extracted. Figure 5.8 illustrates the overview of RDS extraction procedure. The pseudo code of the extraction procedure is given in Figure 5.9.

The two advantages of the RDS algorithm are non transmission of key from embedding part to extraction part and recovering of the cover-image from the stego-image in the extraction part. The implementation and experimental results of the RDS algorithm are discussed in Chapter 7 and RDS algorithm application in medical domain is explained in Chapter 8.

Algorithm for RDS Extraction
Input: *Stego-image*
Output: *Secret Message SM , Reversed Cover-image RCI*

Extracting (Stego-image)

Begin

Identify ROI and NROI in the stego-image
Calculate hash value of ROI
If (hash value of ROI doesn't match with more than half of the NROI pixel series value)
{
Display warning message regarding transmission error
}
Calculate graph index from ROI hash value
Fetch graph for this stego-image
Derive graph 3 coloring ' K_s ' for the graph which is the key for extraction
$\forall$ pixel P_i in NROI assign each color in the K_s in rotation fashion except for those pixels in NROI series
While (until all bits are not extracted)
{
if (P_i assigned K_s == 0)
; // do nothing
else if (P_i assigned K_s == 1)
{
SM=extract '1' bit of SM
RCI = replace the extracted bits with background color
}
else if (P_i assigned K_s == 2)
{
SM=extract '2' bits of SM
RCI = replace the extracted bits with background color
}
}
return SM and RCI;
End

Figure.5.9. RDS extraction algorithm

5.3. SUMMARY

This chapter discussed the reversible dynamic NROI based steganography algorithm using graph coloring. In RDS algorithm the following important phases, identification of ROI and NROI in the cover-image, deriving hash value from ROI, identification of graph and deriving its coloring sequence, RDS embedding algorithm and RDS extraction algorithm are discussed in detail. Dynamicity is ensured in RDS algorithm using the image. The next chapter explains how the dynamicity is guaranteed using the secret message which is to be embedded in the 3D images.

CHAPTER 6

PATTERN BASED 3D IMAGE STEGANOGRAPHY ALGORITHM

This research work aims to develop dynamic embedding and extraction algorithm for 3D images. The dynamicity is ensured by the secret key which is obtained from the secret message. The selection of the pixels to embed the secret message bits is carried out with the help of triangle mesh. This chapter starts with explaining the need for dynamic 3D image steganography algorithm. The four main components of the Pattern based 3D Image Steganography (PBIS-3D) algorithm namely generation of the key, triangle mesh formation, embedding and extraction procedures are elaborated in this chapter.

6.1. NEED FOR PATTERN BASED 3D IMAGE STEGANOGRAPHY ALGORITHM

With the increase in the development of Internet technologies and network bandwidth the usage of multimedia content in the Internet has increased dramatically. This development in technologies prompted user to shift from 2D images to 3D images. In digital world, 3D images became one of the indispensable parts as it provides good quality and finer details of image with an additional dimension compared to 2D image. This extra dimension and quality of 3D images attracted the diversion of the information hiding researchers to extend the 2D image steganography to 3D images. 2D image steganography algorithms cannot be directly applied to 3D images as they differ in properties such as dimension, image size etc. From the literature survey it is observed that most of the spatial domain 3D image steganography algorithms are static in nature.

Hence in the proposed PBIS-3D algorithm dynamicity is introduced using the secret message. The following section covers the details of the Pattern Based 3D Image Steganography (PBIS-3D) algorithm.

6.2. PATTERN BASED 3D IMAGE STEGANOGRAPHY (PBIS-3D) ALGORITHM

The main goal of PBIS-3D algorithm is to induct randomization in the selection of the pixel for embedding and to utilize the minimum number of pixels for embedding the secret message. PBIS-3D algorithm is formulated using the tuples as shown in Eq. 6.1.

PBIS-3D = {CI, SM, GK (SM), Embedding(CI, SM, K), Extraction (SI, K)} (6.1)

where

CI- Cover-image
SM – Secret message
GK (SM) –Key generation procedure from SM where the generated key is denoted by K
Embedding(CI, SM, K) – Embedding procedure
Extraction (SI, K) – Extraction procedure where SI is stego-image

Key generation, Triangle mesh formation, Embedding and Extracting procedure are the four important phases in PBIS-3D algorithm. The following section explains each of the phases in detail.

6.2.1. Generation of Stego-Key from Secret Message

In PBIS-3D algorithm the key is generated from the secret message which is to be embedded in the cover-image. Thus different keys will be generated for each different message to be embedded in the same cover-image. Apart from this, the novelty of the algorithm depends in choosing the pixel for embedding and the number of message bits embedded in each pixel. The detailed steps involved in stego-key generation are explained in the following steps:

a) Input to the stego-key generation algorithm is the secret message and it is represented in Eq. 6.2.

$$SM = S_1S_2S_3\ldots S_z;\ 1<=z<=Length\ (SM) \quad (6.2)$$

Each character in secret message is converted to ASCII and from ASCII it is converted to binary and it is shown in Eq. 6.3.

$$SMB = b_1b_2b_3...b_{(Z*7)} \text{ ; } SMB \in: \{0, 1\}; 1<=Z<=Length(SM) \quad (6.3)$$

b) Secret message bits (SMB) in binary are divided into three bits per message block (MB) as depicted in Eq. 6.4. If SMB is not divisible by three then last portion of the SMB is padded with zeros to make size of last block size as three.

$$SMB = MB_1, MB_2, MB_3, \ldots, MB_k \quad (6.4)$$

where

Length of any MB = 3

'k' is number of blocks

c) Each block of the binary message (MB) is converted into decimal value (MBD). Since each block in binary is of length three the decimal value of each block will lie in the range of 0 and 7 and it is shown in Eq. 6.5.

$$\forall (MBD_{1,2,\ldots,k}) \in: \{0,1,2,3,4,5,6,7\} \quad (6.5)$$

d) The minimum (Min) and maximum (Max) of each MBD_i are calculated where 1<=i<=k and it is represented in the Eq. 6.6.

$$Min = Minimum(MBD_{1,2,\ldots,k}) \text{ and } Max = Maximum(MBD_{1,2,\ldots,k}) \quad (6.6)$$

e) Each message block in decimal value (MBD) is normalized using Eq. 6.7.

$$NMBD_i = \frac{MBD - Min}{Max - Min} \quad (6.7)$$

f) The median λ of the normalized value $NMBD_i$ is computed where 1<=i<=k

g) Median λ which is computed in step f is used as decomposition ratio. The stego-key (K) is generated by the product of decomposition ratio λ and the size of the cover-image N and it is shown in Eq. 6.8.

$$K = \lambda * N \quad (6.8)$$

The stego-key generated will be highly unpredictable as it depends on the secret message. Even a very minor change in the secret message will result in drastic change in the stego-key. The decomposition ratio λ is used to form a triangle mesh from the

initial triangle and the details about the triangle mesh and the initial triangle are explained in the following section.

6.2.2. Triangle Mesh Formation

In triangle mesh formation, the initial triangle which is formed in the cover-image is divided into number of smaller triangles with the edges shared and it is shown in Figure 6.1. The detailed steps involved in triangle mesh formation are given below:

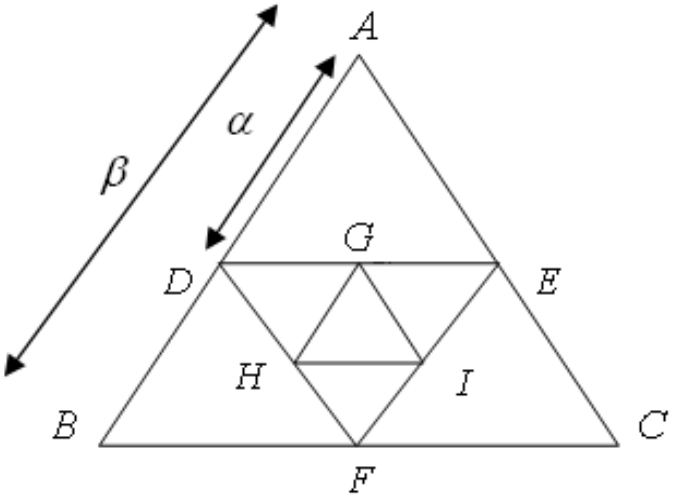


Figure.6.1. Triangle Mesh Formation

a) The maximum of A, maximum of B and maximum of C where A, B and C are the three different points in three different axes of the 3D image is calculated. These maximum points are joined to form the initial triangle T_i where i=0.

b) The edges of the initial triangle T_0 are bifurcated in the clock wise direction. The bifurcation is done on the initial triangle edge and the point where this bifurcation needs to be done is decided based on the Eq. 6.9.

$$\alpha = \beta * \lambda \tag{6.9}$$

where β is the length of the any edge of the initial triangle and

λ is the decomposition ratio obtained from the stego-key generation procedure.

By joining the bifurcation points, which are spotted in the initial triangle using the Eq. 6.9, the triangle T_i is formed where i = i+1.

c) Step b is repeated until the minimum number of triangle meshes are formed which is given in the Eq. 6.10.

$$Minimum\,number\,of\,triangle\,mesh = t = \left\lceil \frac{l(M)}{3*n} \right\rceil \tag{6.10}$$

where l(M) is the length of the binary message in bits,

n is the minimum bits to be embedded in the vertices of the triangle

Denominator has '3' as the triangle has 3 vertices. In order to make the above formulae generalized '3' can be replaced by number of vertices of the mesh formed.

d) The vertices of the triangles formed is denoted by V_{ij} where 1<=i<=t and 1<=j<=3 and 't' represents the number of triangles formed.

In stego-key generation, the median λ is calculated in order to bifurcate the initial triangle edges around the midpoint. This λ is also called as decomposition ratio since it is used to decompose the initial triangle edge. In PBIS-3D algorithm the number of bits to be embedded in the vertices of the triangle is varied.

To find the approximate number of triangle meshes't' to be formed the minimum number of bits to be embedded in vertices of the triangle is taken in to account while arriving the formulae in Eq. 6.10. The pictorial representation of the triangle mesh formed is shown in Figure. 6.1.

Triangle mesh formation is dynamic and it is different for different messages to be embedded in the same cover-image. Table 6.1 shows the stego-key and the triangle mesh formation values, portraying that stego-key and the pixel positions are different for each different secret message to be embedded in the same cover-image. The vertices obtained from the triangle mesh are used for embedding the secret message bits in it.

Table: 6.1. Dynamicity of stego-key and triangle mesh formation for same cover-image with different secret messages

S.No	Secret Message	Normalized Median Value λ	Stego-key	Sample triangle vertices in the car cover-image where secret message to be embedded
1.	Hi Kumar, This is MALIK. Tomorrow at University gate will meet at 12AM. Malik	0.4286	822857	(513,2) (515,2) (519,2) (527,2) (543,2) (575,2) (639,2) (767,2) (1023,2) (512,2) (514,2) (518,2) (526,2)
2.	Bring the materials with complete package in red color package.	0.5714	1097142	(685,2) (687,2) (691,2) (693,2) (695,2) (701,2) (703,2) (723,2) (727,2) (733,2) (735,2) (749,2) (751,2) (755,2) (757,2)

6.2.3. PBIS-3D Embedding Procedure

The outline of the embedding procedure is explained in the Figure 6.2. The inputs to the embedding procedure are cover-image and secret message. The output of the embedding procedure is the stego-image.

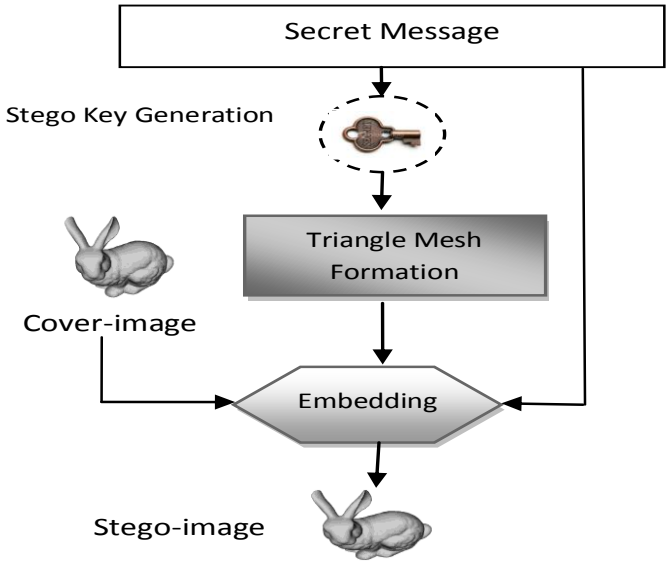


Figure.6.2. PBIS-3D embedding procedure

The main steps of PBIS-3D embedding procedure are:

a) The vertices of the triangle mesh formed V_{ij} are collected where 1<=i<=t and i<=j<=3, t is the number of triangle mesh formed

b) The stego-key obtained from the key generation part is converted in to its binary form

c) Each bit from the stego-key is assigned to the each vertex V_{ij} in the rotation fashion. The first 3t bits of the stego-key are assigned to the 3t vertices of the triangle in clock wise direction where 't' is minimum number of triangle mesh formed.

d) Based on the stego-key assigned to the vertices of the triangle the variable number of bits are embedded in the vertices using Least Significant Bit (LSB) method.

   - If '0' is assigned to the triangle vertex then two bits of secret message are embedded to the triangle vertex.
   - If '1' is assigned to the triangle vertex then three bits of the secret message are embedded to the triangle vertex.

e) The steps (a-d) are repeated until all the message bits are embedded.

The output of the embedding procedure is the stego-image. The secret message which is embedded in the stego-image is extracted using extraction procedure.

6.2.4. PBIS-3D Extracting Procedure

The extraction procedure takes the stego-image generated in the embedding procedure as input. The key K which is generated in the embedding part is transmitted to the extraction part. With the help of stego-image and the key, the extraction procedure extracts the embedded secret message. Figure.6.3 gives the overview of extraction procedure. The major steps involved in the extraction procedure are discussed below:

a) The stego-key K is obtained from the embedding procedure

b) From the stego-key 'K' the decomposition ratio λ which is used to bifurcate the edges of the triangle is obtained and it is given in the Eq. 6.11.

$$\lambda = \frac{K}{N} \tag{6.11}$$

where ‘’K’ is the stego-key

‘N’ is the size of the stego-image

Even after embedding the secret message bits in the cover-image the size of the stego-image remains same.

c) The stego-key is converted to its binary form

d) The initial triangle is constructed as described in the embedding procedure and the bifurcation of the initial triangle is done using the decomposition ratio λ which is obtained in step b

e) The vertices of the triangle mesh formed are collected in clock wise direction and it is represented as V_{ij}.

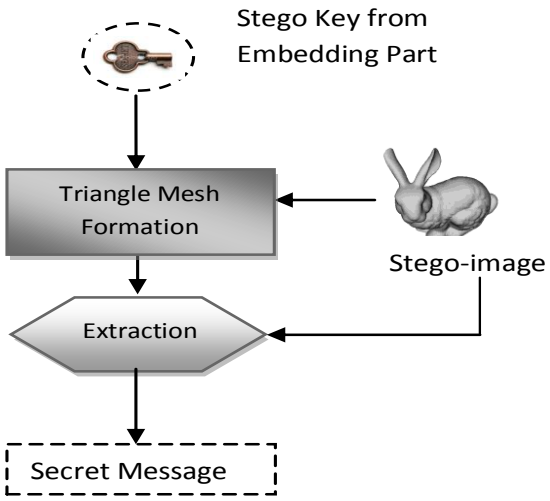


Figure.6.3. PBIS-3D extracting procedure

f) The stego-key is converted into its binary and each bit from the key is assigned to the triangle’s vertex. Based on the stego-key bit assigned the secret message bits are extracted from the vertices of the triangle.

- If ‘0’ is assigned to the vertex of the triangle then two bits of secret message are extracted
- If ‘1’ is assigned to the vertex of the triangle then three bits of secret message are extracted

Figure 6.4, Figure 6.5 and Figure 6.6 show sample categories of cover-image and stego-images generated by PBIS-3D algorithm with different lengths of secret messages embedded in it. The implementation and the experimental results of PBIS-3D algorithm are discussed in Chapter 7 and the application of PBIS-3D algorithm on medical domain is described in Chapter 8.

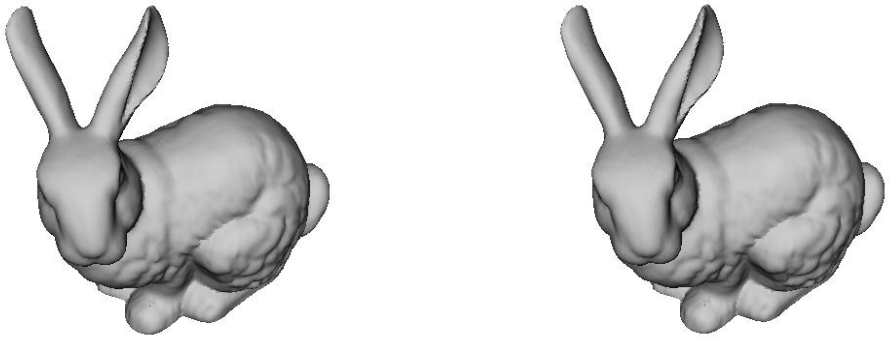


Figure.6.4. Bunny Cover-image (left) and Stego-image (right) with 60,000 bits embedded by PBIS-3D algorithm Image Size: 461 x 373

Figure.6.5. Car Cover-image (left) and Stego-image (right) with 60,000 bits embedded by PBIS-3D algorithm Image Size: 1600 x 1200

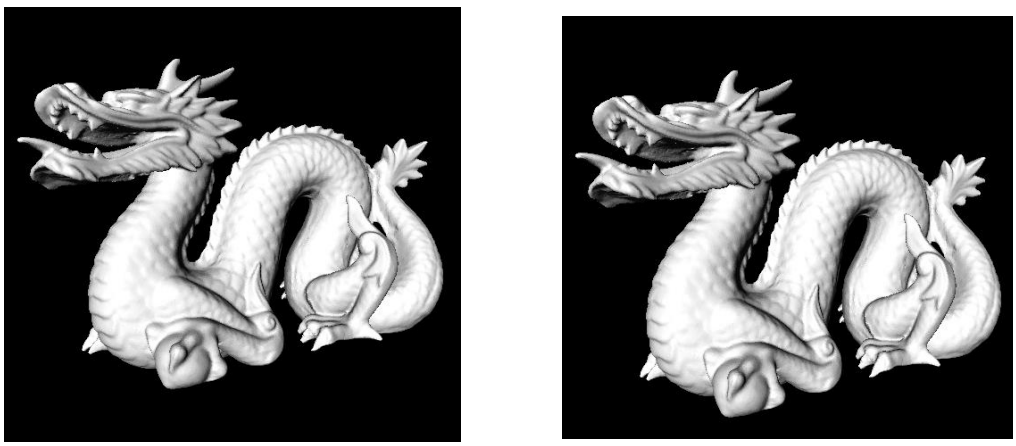


Figure.6.6. Dragon Cover-image (left) and Stego-image (right) with 60,000 bits embedded by PBIS-3D algorithm Image Size: 512 x 512

6.3. SUMMARY

This chapter discussed the need for 3D image steganography algorithm. Generation of key from the secret message, triangle mesh formation using the key, PBIS-3D embedding procedure and extraction procedure are discussed elaborately in this chapter. The following chapter discusses the implementation of the DPIS, RDS and PBIS-3D algorithms and it also deals with the different parameters which are used to evaluate the three proposed algorithms.

CHAPTER 7

RESULTS AND DISCUSSIONS

Any work proposed and developed must be scientifically proved for its acceptance. This chapter discusses the implementation details and the evaluation methodologies that are used to test the three proposed algorithms namely Dynamic Pattern based Image Steganography (DPIS), Reversible Dynamic NROI based Steganography using Graph Coloring (RDS) and Pattern based 3D Image Steganography (PBIS-3D) algorithm. The details of the DPIS, RDS and PBIS-3D algorithm are discussed in detail in chapter 4, chapter 5 and chapter 6 respectively.

The rest of this chapter is arranged as follows: Section 7.1 explains the experiment setup. Section 7.2 list the metrics used for evaluating the proposed algorithms. Section 7.3 presents the results of the capacity and originality retention parameters tested for DPIS and PBIS-3D algorithms. In Section 7.4 the invisibility parameter for all the three algorithms DPIS, RDS and PBIS-3D are evaluated through histogram analysis. The qualities of the stego-image produced by the three proposed algorithms are analyzed in section 7.5 through various statistical parameters such as PSNR, MSE and BER.

Chi-square statistical test is also performed on the stego-images generated by three proposed algorithms to check whether the stego-image is related to the cover-image. Various attacks are experimented on the stego-images generated by DPIS, RDS and PBIS-3D algorithm to prove the robustness of the algorithms which are discussed in the section 7.6. In section 7.7 the proposed algorithms are compared with similar other existing algorithms against various parameters and section 7.8 summarizes the chapter.

7.1. EXPERIMENTAL SETUP

The proposed algorithms DPIS, RDS and PBIS-3D have been developed using Matlab 7.6.0.324 R2008a version. The snapshot of the prototypes developed for DPIS, RDS and PBIS-3D algorithms are shown in Figure 7.1, Figure 7.2 and Figure 7.3 respectively.

The rich and essential image processing capability with inbuilt functions of Matlab apart from its simplicity and user friendliness have made us to choose Matlab as the implementation platform. As the three proposed algorithms deal with the pixels in spatial domain, uncompressed image formats such as bmp, png, gif and tiff are considered for experiments.

The behavior of the three proposed algorithms is tested with images from different categories and sizes. The secret messages of different lengths are embedded in the cover-image to test the quality of the stego-images generated by the proposed algorithms. The proposed algorithms are also compared with other algorithms against various parameters to prove its efficiency. The metrics used for evaluation for the three proposed algorithms are described in the next section.

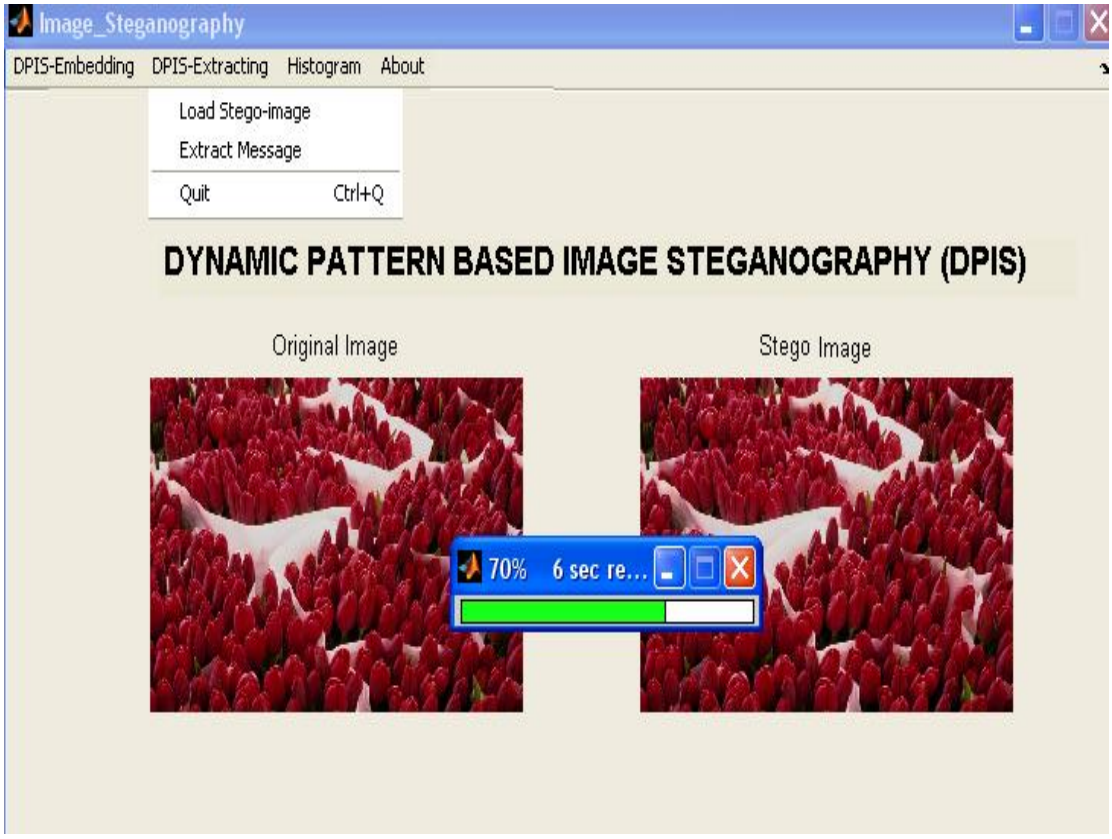


Figure.7.1. Dynamic Pattern based Image Steganography (DPIS) algorithm prototype - screen shot

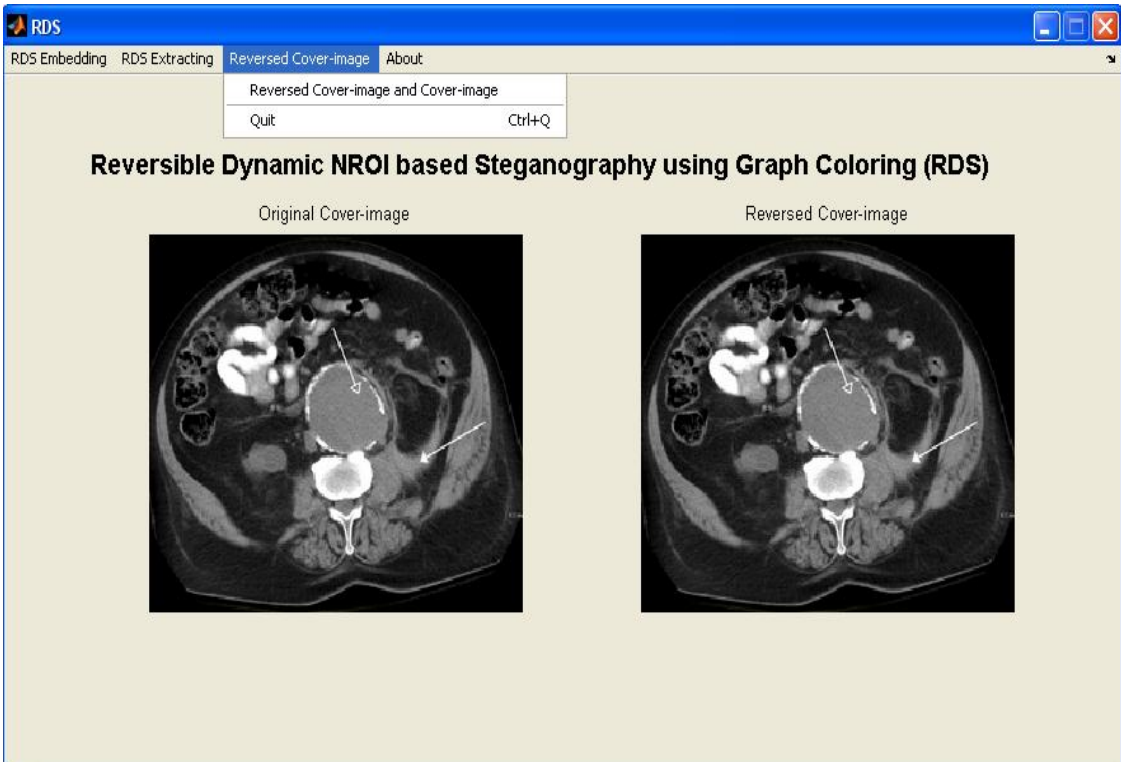


Figure.7.2. Reversible Dynamic NROI based Steganography algorithm using Graph Coloring (RDS) prototype - screen shot

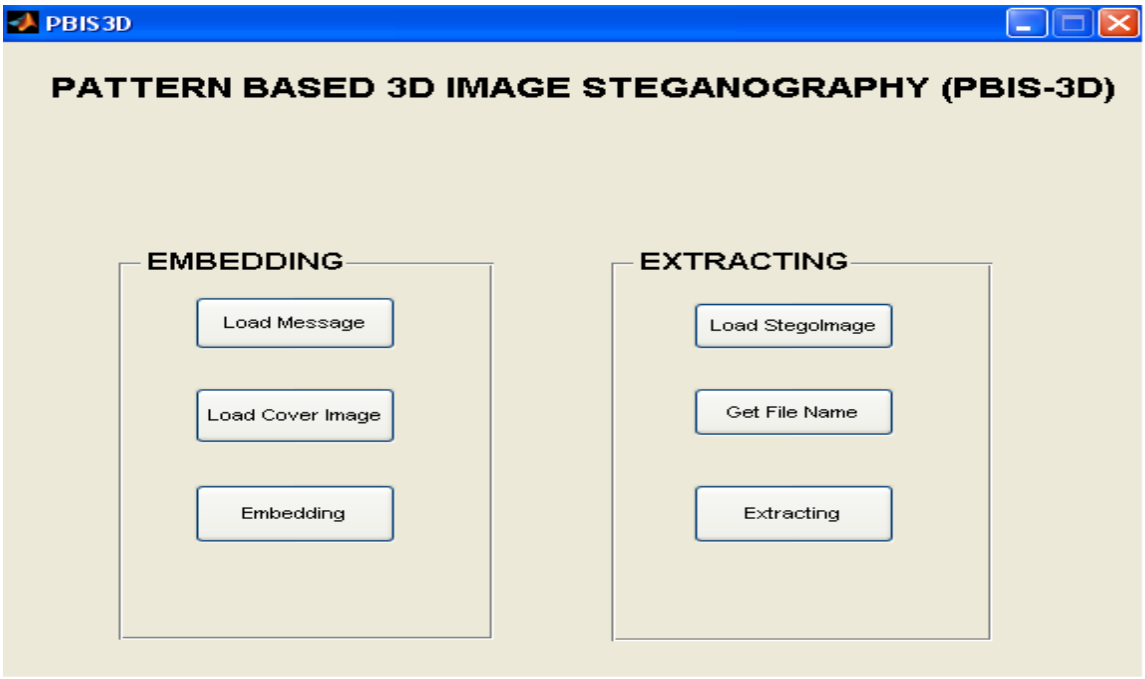


Figure.7.3. Pattern Based 3D Image Steganography (PBIS-3D) algorithm prototype – screen shot

7.2. EVALUATION METRICS

The level of competence of the proposed algorithms is evaluated through a set of experiments using the following metrics:

- Capacity
- Invisibility
- Statistical test
- Robustness

The spatial domain image steganography algorithm uses pixels to embed the secret message. An efficient steganography algorithm should use minimum number of pixels for embedding secret message. Thus in this research, the capacity metric is used to evaluate the efficiency of the proposed algorithms in terms of the number of pixels used for embedding secret messages. The embedding part of the steganography algorithm should not introduce any noticeable change to the cover-image. To find whether there is any difference between cover-image and the stego-image generated by the proposed algorithms the invisibility metric is taken for evaluation. The stego-image generated by the proposed algorithms should be of high quality and this quality is evaluated through statistical metrics. The stego-images generated by image steganography algorithms should resist against steganalysis attacks. Hence the robustness of the stego-images generated by the three proposed algorithms are tested with scaling, rotation, cropping, filtering and noise attacks.

7.3. CAPACITY

Capacity is the key metric in evaluating the image steganography algorithm. Capacity is defined as the ratio of total number of pixels used in the cover-image for embedding the secret message to the total number of pixels in the cover-image and it is represented as in Eq. 7.1

$$\text{Capacity} = \left(\frac{Total number of\ pixels\ used\ for embedding}{Total number of\ pixels\ in\ Cover image} \right) \tag{7.1}$$

Originality retention is the ratio of total number of pixels which are not used for embedding to the total number of pixels in the cover-image. Originality retention is a modified version of capacity and it is shown in Eq. 7.2

$$\text{Originality retention} = \left(\frac{Total number pixels not used for\ embedding}{Total number of\ pixels in\ Cover\ image} \right) \quad (7.2)$$

Capacity and originality retention are closely related but their objectives are different. In originality retention, the originality retained by the cover-image even after embedding the secret message is calculated. The capacity and the originality retention are calculated for the DPIS and PBIS-3D algorithms and the results are tabulated in the following section.

7.3.1. Evaluation of DPIS Algorithm Using Capacity Metric

Table.7.1. Capacity and Originality Retention of DPIS algorithm

Images	**Image Size (Width * Height)**	**Message Size (Bits)**	**Average number of pixels used for embedding**	**Average number of unused pixels**	**Average Capacity (%)**	**Average Originality Retention (%)**
Apple	450*540	10,000 – 20,000	5791.50	237208.50	2.38	97.62
Bird	550*367	20,000 - 30,000	10121.45	191728.55	5.01	94.99
Dosa	512*384	30,000 – 40,000	13409.96	183198.04	6.82	93.18
Flower	336*429	40,000 – 50,000	19396.55	124747.45	13.46	86.54
Lena	512*512	50,000 – 60,000	23109.24	239034.76	8.82	91.18
Portrait	450*570	60,000 – 70,000	23722.62	232777.38	9.25	90.75
Sea	500*500	70,000 - 80,000	32751.09	217248.91	13.10	86.90
Baboon	512*512	80,000 - 90,000	34552.84	227591.16	13.18	86.82
Zebra	540*518	90,000 - 10,0000	35849.05	243870.95	12.82	87.18

Table.7.2. Capacity and Originality Retention of Lena image with different message size - DPIS algorithm

Image and Image Size (Width * Height)	Message Size (Bits)	Average number of pixels used for embedding	Average number of unused pixels	Average Capacity (%)	Average Originality Retention (%)
Lena 512*512	10,000 – 20,000	6971.85	255172.15	2.66	97.34
	20,000 - 30,000	11225.41	250918.59	4.28	95.72
	30,000 – 40,000	14726.78	247417.22	5.62	94.38
	40,000 – 50,000	18943.15	243200.85	7.23	92.77
	50,000 – 60,000	23109.24	239034.76	8.82	91.18
	60,000 – 70,000	26986.95	235157.05	10.29	89.71
	70,000 - 80,000	31261.63	230882.37	11.93	88.07
	80,000 - 90,000	35021.72	227122.28	13.36	86.64
	90,000 - 10,0000	38427.63	223716.37	14.66	85.34

DPIS algorithm was tested for capacity metric by conducting various experiments. In each of the experiments the length of the secret message was varied from 10,000 bits to 1,00,000 bits. Generally short messages are communicated message through steganography techniques. Hence for all experiments message length is restricted to 1,00,000 bits (approximately 14,000 characters).

The performance of the DPIS algorithm is analyzed for various categories and different size of cover-images such as Lena, baboon, fruits, flower, nature, portrait, birds, sea and animals. The experiments were repeated in each range and the average of the results were taken and it is tabulated in Table 7.1. From the results shown in Table 7.1 it is observed that the DPIS algorithm maintains around 87% originality even after embedding around 1 lakh bits in the zebra cover- image. The value of capacity and originality retention of the same cover-image with different message range is experimented and the results are shown in Table 7.2. From the results shown

in Table 7.2 it is observed that for same cover-image as the size of the message increases the originality retention decreases.

The capacity and originality retention metrics are also compared with (Parvez and Gutub, 2008) and (Gutub et al., 2008) algorithms. These two algorithms are taken for comparison as they analyze the color channel for embedding which is similar to DPIS algorithm. The experimental results were tabulated in Table 7.3 and the same has been depicted in the Figure 7.4.

Three different message groups of different size in the range 100 to 1,000 bits, 1,000 to 10,000 bits and 10,000 to 15,000 bits were taken for comparison. For embedding message in the group 10,000 to 15,000 bits, (Parvez and Gutub, 2008) algorithm retains 91.81 % of originality in the flower cover-image, (Gutub et al., 2008) algorithm retains 90.37% of originality in the flower cover-image and DPIS algorithm retains 93.21% of originality in the flower cover-image.

Table 7.3 clearly portrays that compared to (Parvez and Gutub, 2008) and (Gutub et al., 2008) algorithm, DPIS algorithm retains high originality in the flower cover-image even after embedding different lengths of secret message in it.

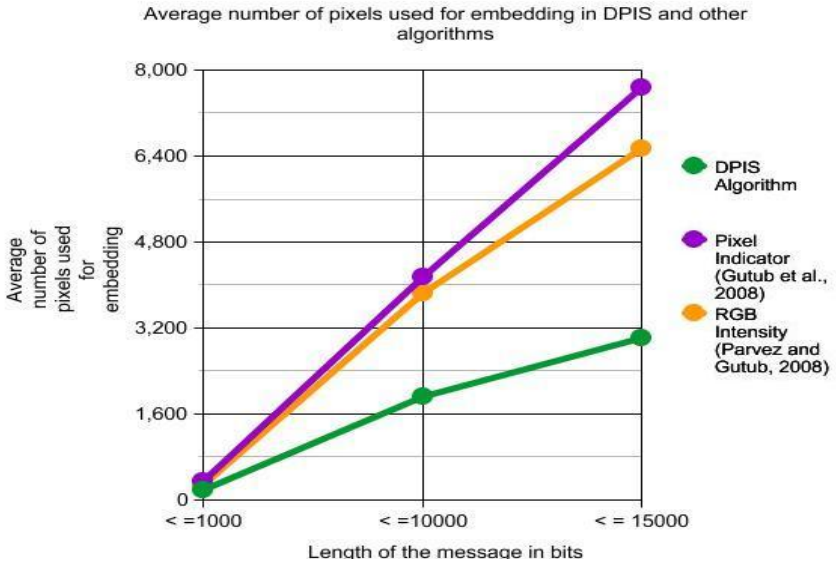


Figure.7.4. DPIS Vs Existing algorithms - Average pixels used for embedding

Table.7.3. Comparison of Capacity and Originality Retention between DPIS Vs Existing Algorithm

Image name and Size	Methods	Message Size (bits)	Average Pixels used for embedding (round off value)	Average Pixels not used for embedding (round off value)	Average Capacity (%)	Average Originality Retention (%)
Flower image 300*266	Parvez and Gutub, 2008	100 to1,000	284	79516	0.36	99.64
		1,000 to10,000	3841	75959	4.81	95.19
		10,000 to15,000	6536	73264	8.19	91.81
	Gutub et al., 2008	100 to 1,000	342	79458	0.43	99.57
		1,000 to10,000	4157	75643	5.21	94.79
		10,000 to15,000	7684	72116	9.63	90.37
	DPIS Algorithm	100 to 1,000	**231**	**79569**	**0.29**	**99.71**
		1,000 to10,000	**2453**	**77347**	**3.07**	**96.93**
		10,000 to15,000	**5417**	**74383**	**6.79**	**93.21**

7.3.2. Evaluation of RDS Algorithm Using Capacity Metric

As discussed in section 5.2.1, RDS algorithm separates the image into ROI and NROI region. The secret message is embedded in the NROI portion of the image. The space available to embed the secret message in the NROI region based steganography algorithms is less compared to other algorithms where the whole image is available for embedding.

As the number of pixels available for embedding in the NROI region based image steganography algorithm is less it can embed only short message which results in good originality retention. From the above analysis, it is obvious that the RDS algorithm has only less number of pixels available for embedding which results in good originality retention.

7.3.3. Evaluation of PBIS-3D Algorithm Using Capacity Metric

The evaluation of PBIS-3D algorithm was iterated for different lengths of secret message in the range between 10,000 bits and 1,00,000 bits in the 3D cover-image. The average originality retention and average capacity were calculated and it is tabulated in Table 7.4.

Different images of various sizes were taken and embedded with secret message of varying lengths. The results are shown in Table 7.4. On embedding around 1, 00, 000 bits in the bunny cover-image of size 461*373 (width * height) it uses 21.25 % of pixels for embedding and maintains 78.75% of originality.

The behavior of capacity and originality retention of PBIS-3D algorithm on single cover-image by embedding with various lengths of secret message is experimented and the results are shown in Table 7.5. From the results it is obvious that as the size of the secret message increases the originality retention decreases.

Table.7.4. Capacity and Originality Retention of PBIS-3D algorithm

Images	Image Size (Width * Height)	Message Size (Bits)	Average number of pixels used for embedding	Average number of unused pixels	Average Capacity (%)	Average originality Retention (%)
Car	1600* 1200	10,000 – 20,000	9154.78	1910845.22	0.48	99.52
Dragon	512* 512	20,000 - 30,000	10425.33	251718.67	3.98	96.02
Horse	467* 528	30,000 – 40,000	14583.41	231992.59	5.91	94.09
Flower	1280* 1280	40,000 – 50,000	16745.33	1621654.67	1.02	98.98
Elephant	300* 300	50,000 – 60,000	22471.78	67528.22	24.97	75.03
Teeth	400* 400	60,000 – 70,000	27028.41	132971.59	16.89	83.11
Bone	391* 366	70,000 - 80,000	27777.54	115328.46	19.41	80.59
Dinosaur	2560* 1600	80,000 - 90,000	32692.96	4063307.04	0.8	99.2
Bunny	461* 373	90,000 - 10,0000	36538.47	135414.53	21.25	78.75

PBIS-3D is compared for capacity and originality retention with (Cheng and Wang, 2006) and (Agarwal and Prabhakaran, 2009) algorithms. Table 7.6 shows the values obtained by comparing PBIS-3D algorithm and (Cheng and Wang, 2006) algorithm by embedding secret message of length of 17320 bits and 1480 bits. (Cheng and Wang, 2006) uses an average of 48.18 % and 49.33% of pixels for embedding message length of 17320 and 1480 bits where as PBIS-3D algorithm uses only 15.75% and 18.75% of pixels for embedding the message of same size.

Secret message of length in bits 14841and 20060 is embedded in the bunny and horse cover-image by using (Agarwal and Prabhakaran, 2009) and PBIS-3D algorithm. The results obtained are tabulated in Table 7.7. (Agarwal and Prabhakaran, 2009) uses 41.2 % and 41.5 % of pixels for embedding the secret message of 14841 and 20060 bits in length but PBIS-3D uses only 13.53 % and 36.83 % of pixels. The graphical representation of the Table 7.6 and Table 7.7 are illustrated in the Figure 7.5.

Table.7.5. Capacity and Originality Retention of Car image with different message size - PBIS-3D algorithm

Images	**Message Size (Bits)**	**Average number of pixels used for embedding**	**Average number of unused pixels**	**Average Capacity (%)**	**Average Originality Retention (%)**
Car 1600*1200	10,000 – 20,000	9154.78	1910845.22	0.48	99.52
	20,000 - 30,000	11821.13	1908178.87	0.62	99.38
	30,000 – 40,000	14625.65	1905374.35	0.76	99.24
	40,000 – 50,000	19360.42	1900639.58	1.01	98.99
	50,000 – 60,000	21963.81	1898036.19	1.14	98.86
	60,000 – 70,000	27464.95	1892535.05	1.43	98.57
	70,000 -80,000	31174.57	1888825.43	1.62	98.38
	80,000 -90,000	34869.26	1885130.74	1.82	98.18
	90,000 -10,0000	37715.34	1887584.66	1.96	98.04

Table. 7.6. Capacity and Originality Retention comparison between PBIS-3D algorithm and (Cheng and Wang, 2006) method

Image Name	Total number of Pixels	Number of Secret Message Bits embedded	% of Pixel used for embedding		Originality Retention in Stego-Image	
			Cheng and Wang, 2006	PBIS-3D Algorithm	Cheng and Wang, 2006	PBIS-3D Algorithm
Bunny	35947	17320	48.18	15.75	51.82	84.25
Horse	3000	1480	49.33	18.75	50.67	81.25

Table. 7.7. Capacity and Originality Retention comparison between PBIS-3D algorithm and (Agarwal and Prabhakaran, 2009) method

Image Name	Total number of Pixels	Number of Secret Message Bits embedded	% of Pixel used for embedding		Originality Retention in Stego-Image	
			Agarwal and Prabhakaran, 2009	PBIS-3D Algorithm	Agarwal and Prabhakaran, 2009	PBIS-3D Algorithm
Bunny	35947	14841	41.2	13.53	58.80	86.47
Horse	48485	20060	41.5	36.83	58.5	63.17

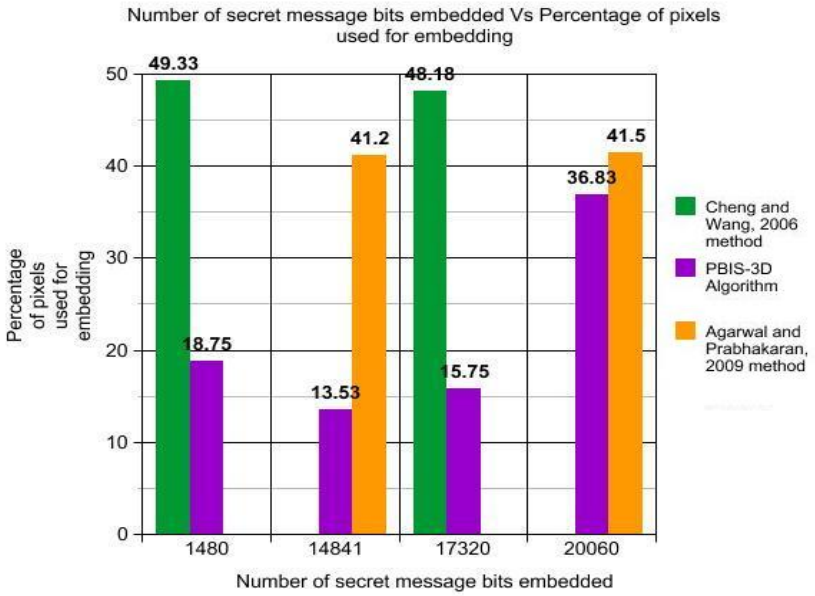


Figure.7.5. Graph – Capacity Comparison of PBIS-3D algorithm with (Cheng and Wang, 2006) and (Agarwal and Prabhakaran, 2009) method

Interpretation of results

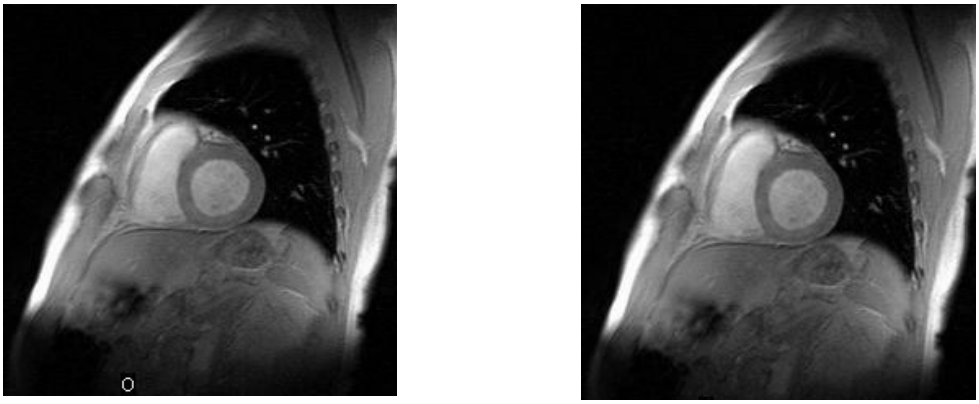
From the experimental results presented above it is obvious the proposed DPIS and PBIS-3D algorithm uses very less number of pixels when compared to other existing algorithms. The originality retention of the DPIS and PBIS-3D algorithms also high compared to other existing algorithms. RDS algorithm generally retains good originality retention as the space available for embedding itself is very less. The invisibility metric is evaluated through histogram analysis and it is discussed in the next section.

7.4. INVISIBILITY

Invisibility is the essence and most crucial evaluation metric in image steganography. Stego-image obtained from any image steganography algorithm should not be differentiated from the cover- image by Human Visual System (HVS). As concealing message in the digital image is the goal of steganography, embedding algorithm devised should not introduce any noticeable change in the cover-image. Human eyes are not sensitive to the small changes in the image and it is shown through stego-image generated by DPIS, RDS and PBIS-3D algorithms in Figure 7.6, Figure 7.7 and Figure 7.8 respectively.

(a) **(b)**

Figure.7.6. Lena (a) Cover-image (b) DPIS algorithm generated stego-image containing 20,000 bits embedded in it



(a) **(b)**

Figure.7.7. Medical (a) Cover-image (b) RDS algorithm generated stego-image containing 1500 bits embedded in it

(a) **(b)**

Figure.7.8. Car (a) Cover-image (b) PBIS-3D algorithm generated stego-image containing 20,000 bits embedded in it

Hence to find the small changes in the image, histogram graphs are drawn to detect the presence of message in the stego-image generated using the three proposed spatial domain image steganography algorithms. In histogram, (Chandramouli et al., 2004) the graph is drawn with pixel values as x axis and frequency of pixel values as y axis.

Histogram graphs are drawn for the cover-image and the stego-image and the graphs are analyzed visually for any changes. The stego-image obtained from the DPIS, RDS and PBIS-3D algorithms are tested using histogram graph to prove invisibility. The following section explains the same in detail.

7.4.1. Histogram Analysis for DPIS Algorithm

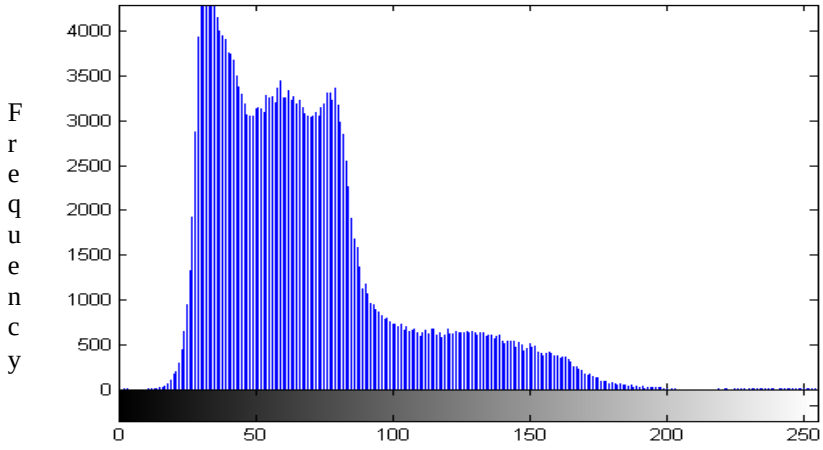


Figure.7.9. DPIS - Blue color histogram for Lena cover-image

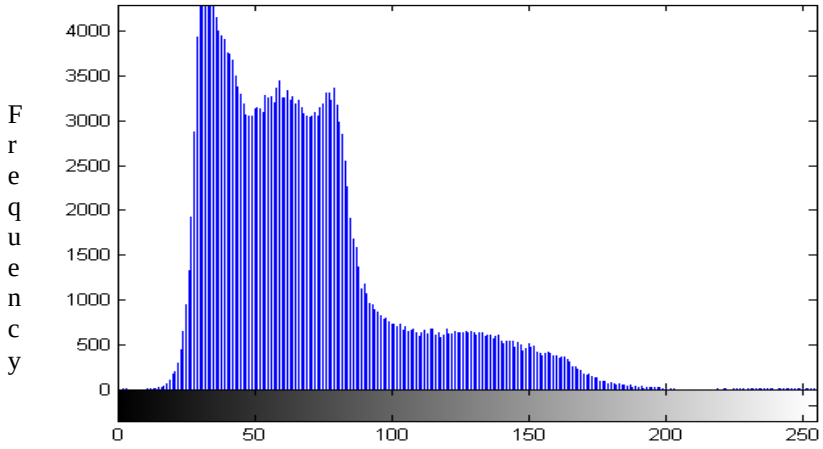


Figure.7.10. DPIS -Blue color histogram for Lena stego-image with 20,000 bits

Three histograms for red, green and blue color are drawn for both cover-image and the DPIS generated stego-images. These histograms are analyzed visually for any noticeable changes. The blue color histogram for the cover-image Figure.7.6 (a) and the stego-image shown in Figure.7.6 (b) are depicted in Figure 7.9 and Figure 7.10.

From the blue histograms shown below, no visual difference can be identified between the cover-image histogram and the DPIS generated stego-image histogram which concludes that the DPIS embedding algorithm does not introduce any noticeable changes in the cover-image.

7.4.2. Histogram Analysis for RDS Algorithm

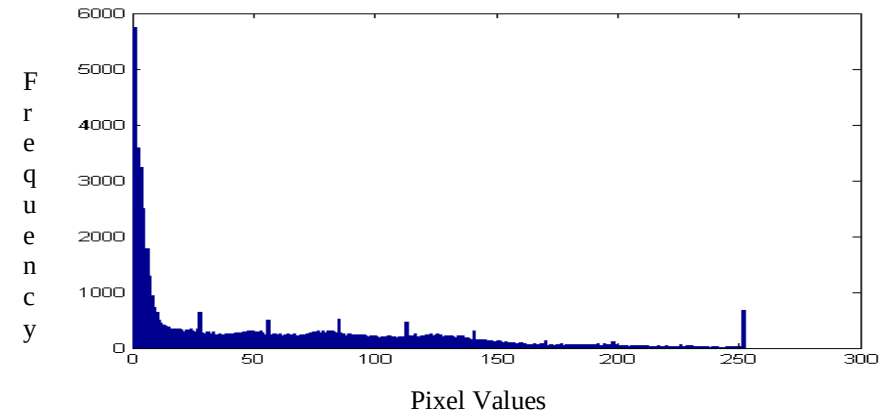


Figure.7.11. RDS – Histogram for medical cover-image

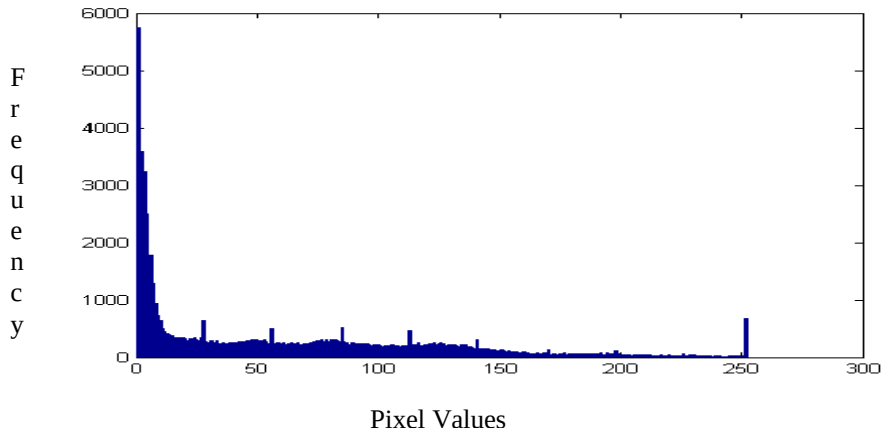


Figure.7.12. RDS – Histogram for medical stego-image with 1,500 bits

Histograms are drawn for the grey scale images shown in the Figure 7.7. As RDS algorithm will embed only short messages, the stego-image shown in Figure 7.7 (b) is obtained by embedding 1,500 bits of secret message bits in it. From the histograms shown in the Figure 7.11 and Figure 7.12 it is clear that the histogram for the cover-image is same as the stego-image histogram.

7.4.3. Histogram Analysis for PBIS-3D Algorithm

Red, green and blue color histograms were drawn for the 3D images which are shown in Figure 7.8. Cover-image and stego-image blue color histogram is shown in Figure 7.13 and Figure 7.14. Careful visual comparison of these histograms reveals that there is no visually notable difference between them.

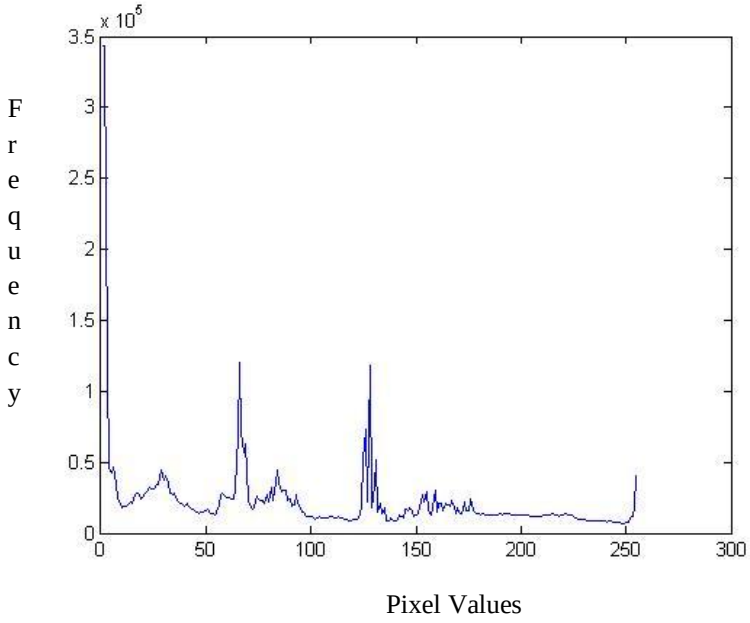


Figure.7.13. PBIS-Histogram for 3D Car cover-image

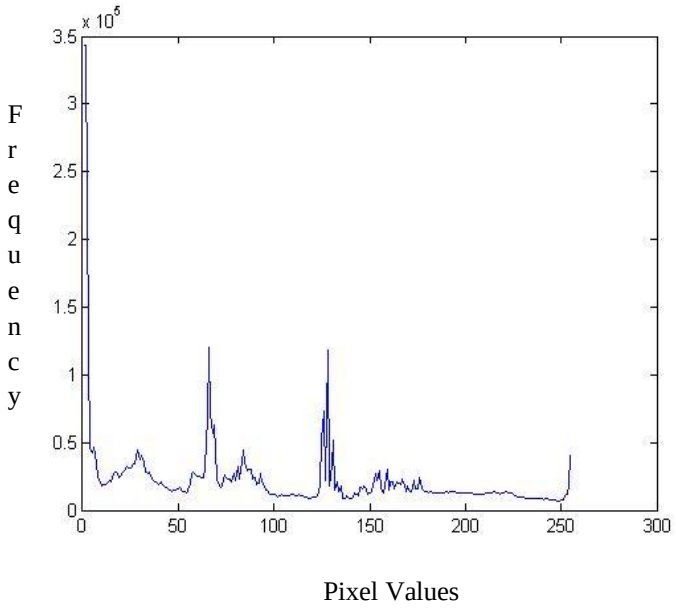


Figure.7.14. PBIS-Histogram for 3D Car stego-image with 20,000 bits

Interpretation of results

The evaluation metric invisibility is evaluated through histogram analysis. DPIS, RDS and PBIS-3D algorithm generated stego-images histograms and their cover-images histograms are compared visually and no changes are detected which shows that the proposed DPIS, RDS and PBIS-3D embedding algorithms do not introduce any major changes to the cover-image by embedding secret message in it. The stego-images generated by DPIS, RDS and PBIS-3D algorithms are tested statistically and it is discussed in the next section.

7.5. STATISTICAL TESTS

DPIS, RDS and PBIS-3D algorithms are evaluated for the statistical metrics such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Bit Error Rate (BER) (Juneja and Sandhu, 2013) . In order to measure the change in visual perceptibility (quality) the statistical parameter PSNR and MSE are calculated. BER is calculated to find the transmission error..

Apart from these above statistical parameters, the chi-square test is also performed on the cover-image and the stego-image generated by the three proposed algorithms to show the dependence between them. Chi-square test is opted in this experiment as it is normally used to detect the presence of message in the stego-image generated by Least Significant Bit (LSB) algorithm (Nissar and Mir, 2010). The details of the statistical parameters which are used to evaluate the proposed algorithms are explained below:

Mean Square Error (MSE)

MSE is the statistical measure to find the cumulative squared error between the cover-image and the stego-image. MSE is represented by Eq. 7.3

$$\mathrm{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [CI(i, j) - SI(i, j)]^2 \tag{7.3}$$

Where

CI is the cover-image,

SI is the stego-image,

m is the number of rows in the cover-image and

n is the number of columns in the stego-image

Peak Signal to Noise Ratio (PSNR)

PSNR is the statistical measure to find the quality of the stego-image. From the literature it has been observed that if the PSNR values are above 30 db then the stego-image generated will be considered as good quality image (Liang et al., 2013, Kondoz, 2009). PSNR is represented by Eq. 7.4

$$PSNR = 10\log_{10}\left(\frac{Max^2}{MSE}\right) \quad (7.4)$$

Where

Max refers to the maximum value of the pixel which is 255 and

MSE is Mean Square Error

Bit Error Rate (BER)

BER is the ratio of the total number of bit errors that occurred during transmission to the total number of bits transmitted. BER is represented by Eq. 7.5

$$BER = \frac{\text{Number of bit error occoured during transmission}}{\text{Total number of bits transmitted}} \quad (7.5)$$

Chi-Square test

There are two types of chi-square test, one is chi-square goodness of fit test and the other is chi-square independence test. Chi-square test for independence is used to find the dependency between two variables and in this research chi-square is used to check whether the image which contains secret message (stego-image) is related to the cover-image.

Chi-square test is performed on various categories of image embedded with different lengths of secret messages. This experiment is performed in Matlab using the command 'crosstab' which return 'p' value. If the 'p' value is less than 0.05 then the null hypothesis is rejected at 5% level of significance. If 'p' value is greater than 0.05 then the alternate hypothesis is rejected at 5% level of significance. Null hypothesis and the alternate hypothesis are stated below to find the relation between cover-image and the stego-image.

Null Hypothesis (H_0): Cover-image and stego-image are not related

Alternate Hypothesis (H_1): Cover-image and stego-image are related

7.5.1. Evaluation of DPIS Algorithm Using Statistical Metric

In order to test the statistical behavior of the stego-images generated by the proposed algorithms on different color combinations, images from various categories are used

for our experiments. Secret messages are taken in the range of 21,000 – 84,000 bits. Experiments were repeated for each range of message bits many times and the average values of PSNR, MSE and BER were calculated and it is shown in Table 7.8.

Good quality stego-image should have low MSE and BER values. From the experimental results shown in Table 7.8 it is observed that the average MSE values vary in the range 0.08 to 1.14 and the average BER varies from 0.04 to 0.07. The average PSNR values shown in Table 7.8 are above 45db which portrays the quality of the stego-image generated by the DPIS algorithm.

Table.7.8. PSNR, MSE and BER for DPIS algorithm for various image categories and various sizes of secret messages

Images	Message Bits embedded in range	Average PSNR	Average MSE	Average BER
Apple	21,000 – 24,000	55.70	0.22	0.04
Bird	24,000 – 28,000	53.11	0.40	0.07
Dosa	28,000 – 32,000	57.99	0.13	0.05
Flower	32,000 – 36,000	47.84	1.07	0.05
Lena	40,000 – 44,000	50.57	0.57	0.05
Person	52,000 – 56,000	61.10	0.08	0.06
Sea	62,000 – 66,000	51.05	0.81	0.05
Tiger	65,000 – 68,000	50.32	0.76	0.04
Zebra	68,000 – 72,000	49.27	0.77	0.05
Nature	80,000 – 84,000	47.55	1.14	0.05

The chi-square test is performed on the stego-images apple, lena, sea and nature each embedded with 20,000, 40,000, 60,000 and 80,000 of secret message bits respectively. Table 7.9 shows that the value of ‘p’ for the different images. The value of ‘p’ is less than 0.05 hence the null hypothesis is rejected. Hence the alternate hypothesis which claims that the cover-image and the stego-image are related is accepted.

Table.7.9. Chi-square test performed on cover-images and stego-images obtained from DPIS algorithm

Image	Size of secret message embedded (Bits)	Value of ‘p’	Null Hypothesis Status
Apple	20,000	0	Reject
Lena	40,000	0	Reject
Sea	60,000	0	Reject
Nature	80,000	0	Reject

7.5.2. Evaluation of RDS Algorithm Using Statistical Metric

Table.7.10. PSNR, MSE and BER for RDS algorithm for various image categories and various sizes of secret messages

Image	Number of Secret message bits embedded(M)	Average PSNR (dB)	Average MSE	Average Bit Error Rate (BER)
Brain	650 to 950	74.36	0.01	0.004
	950 to 1250	73.22	0.01	0.001
	1250 to 1550	72.14	0.01	0.002
	1550 to 1850	71.58	0.02	0.001
Eye	650 to 950	68.65	0.01	0.002
	950 to 1250	67.21	0.01	0.001
	1250 to 1550	66.17	0.02	0.004
	1550 to 1850	65.53	0.02	0.002
Kidney	650 to 950	68.32	0.01	0.003
	950 to 1250	67.08	0.01	0.002
	1250 to 1550	66.07	0.02	0.003
	1550 to 1850	65.57	0.02	0.004
Lungs	650 to 950	72.84	0.01	0.001
	950 to 1250	71.24	0.01	0.002
	1250 to 1550	69.84	0.02	0.001
	1550 to 1850	68.14	0.02	0.001

The proposed RDS algorithm is tested with the medical images. For experimental purpose the medical images from four different categories are chosen and the experiments were repeated and the average results are projected in the Table 7.10. As RDS algorithm embeds secret message of short length, secret message of length in the range 650 to 1850 bits were considered for experiments. From the values shown in Table 7.10 it is observed that the average MSE varies from 0.01 to 0.02 and the average BER varies from 0.001 to 0.004. The average PSNR value of the stego-image generated by the RDS algorithm varies from 65 db to 74 db which ensures that the RDS algorithm generates good quality stego-images.

Chi-square test is performed on the medical images such as brain, kidney, lungs and eye with various lengths of secret message in the range of 650 bits to 1850 bits embedded in it. For all chi-square experiments the value of p is always less than 0.05 therefore the null hypothesis is rejected and the alternate hypothesis which states that there is relation between cover-image and RDS stego-image is accepted. Table 7.11 shows the chi-square test for independence results obtained for the cover-images and the RDS algorithm generated stego-images.

Table.7.11. Chi-square test performed on cover-images and stego-images obtained from RDS algorithm

Image	Size of secret message embedded (Bits)	Value of 'p'	Null Hypothesis Status
Brain	650	0	Reject
Kidney	1050	0	Reject
Lung	1450	0	Reject
Eye	1850	0	Reject

7.5.3. Evaluation of PBIS-3D Algorithm Using Statistical Metric

For testing the statistical parameter of stego-images generated by PBIS-3D algorithm, nine different 3D images were considered for the experiments. Secret message of length varying in the range from 28,000 bits to 78,000 bits were used for the experiments. The experiments were repeated and the average value obtained is tabulated in the Table 7.12. Average MSE values calculated between the cover-image and the PBIS-3D stego-image are low and it varies from 0.01 to 1.66. The average BER values are calculated and the value varies from 0.04 to 0.08. PSNR value shown in Table 7.12 varies between 45 db and 70 db which confirm the PBIS-3D generated stego-images are of good quality.

Chi-square test is performed on the 3D images such as car, bunny, horse and elephant with different lengths of secret messages in the range from 20,000 bits to 80,000 bits embedded in it. The tabulated value shows that the 'p' value in chi-square experiments is less than 0.05. Therefore the null hypothesis is rejected. The alternate hypothesis which states that there is relation between cover-image and the PBIS-3D stego-image is accepted. Table 7.13 shows the chi-square test for independence results for cover-images and the PBIS-3D generated stego-images.

Table.7.12. PSNR, MSE and BER for PBIS-3D algorithm for various image categories and various sizes of secret messages

Images	Message Bits embedded in range	Average PSNR	Average MSE	Average BER
Car	28,000 – 32,000	70.38	0.01	0.05
Dragon	33,000 – 37,000	62.15	0.04	0.06
Horse	38,000 – 42,000	56.40	0.15	0.07
Flower	42,000 – 46,000	68.16	0.01	0.04
Elephant	52,000 – 56,000	55.38	0.20	0.06
Teeth	62,000 – 66,000	53.40	0.30	0.04
Bone	66,000 – 70,000	56.02	0.15	0.07
Dinosaurs	70,000 – 74,000	46.77	1.38	0.05
Bunny	74,000 – 78,000	45.96	1.66	0.08

Table.7.13. Chi-square test performed on cover-images and stego-images obtained from PBIS-3D algorithm

3D Image	Size of secret message embedded (Bits)	Value of 'p'	Null Hypothesis Status
Car	20,000	0	Reject
Bunny	40,000	0	Reject
Horse	60,000	0	Reject
Elephant	80,000	0	Reject

Interpretation of results

The average values of PSNR for all the three proposed algorithms are above 45 db and the average MSE and BER values for the three proposed algorithms are as low as possible which clearly portrays that the stego-image generated by the three proposed algorithms is of high quality. The result of the Chi-square test also reveals that there is a strong relation between the stego-images generated by the three proposed algorithms and the cover-image. The next section discusses the behavior of the proposed algorithms against various attacks.

7.6. ROBUSTNESS

The resistance of the stego-images generated by the proposed algorithms against steganalysis attacks is discussed in this section. The counterpart of steganography is steganalysis which is used to detect the presence of secret message and then to extract the secret message embedded in the stego-image. Some of the steganalysis attacks

such as brute force attacks on key, fixed bits extraction attack, sequential pixel extraction attack (Fridrich and Goljan, 2003) are performed on the stego-images generated by the three proposed algorithms.

Other types of attacks such as geometrical attacks, noise and filtering attacks are performed on the stego-images to scramble the secret message embedded in it. The above mentioned attacks on the stego-image generated by the proposed DPIS, RDS and PBIS-3D algorithms are experimented and the results are analyzed in this section.

7.6.1. Brute Force Attack on the Key

The dynamic key generated in DPIS, RDS and PBIS-3D algorithms are tested for its robustness by the brute force attack. In the brute force attack all the possible keys are tried until a meaningful secret message is extracted from the stego-image. Brute force attack on the three proposed algorithms is discussed below.

7.6.1.1. Behavior of Brute Force Attack on the Key in DPIS Algorithm

As mentioned in section 4.2.1 the DPIS key should contain at least one R (red), one G (green) and one B (blue) color. The number of distinct ways in which the key can be formed with the above condition is mentioned in Eq. 7.6

$$\text{Number of distinct key formed by DPIS algorithm} = 3^{(n-2)} * 2 \quad (7.6)$$

where

'n' is the length of the key

The key can be of any length, the length of the key is directly proportional to the strength of DPIS algorithm. In DPIS algorithm the minimum key size of length 20 is taken for experiments. For the key size 20, the number of distinct keys generated using Eq. 7.6 is 774,840,978 (Seven Hundred Seventy-Four Million Eight Hundred Forty Thousand Nine Hundred Seventy-Eight). As the number of distinct key patterns formed for the key size 20 is large it will take many years to crack the key using brute force attack (Schneier, 1996) .

7.6.1.2. Behavior of Brute Force Attack on the key in RDS Algorithm

The robustness of the key in RDS algorithm directly depends on the computational complexity in deriving the key. The detailed discussion of the computational complexity in obtaining the RDS key is provided in this section.

7.6.1.2.1. Computational Complexity in Hacking the Key

RDS algorithm uses key which is derived from graph 3-coloring problem. In graph 3-coloring problem the vertices of the graph are colored such that no two vertices connected by the edges should have the same color. The color of all the vertices arranged in clock wise direction is used as key for both embedding and extraction. In RDS algorithm tree graphs are taken for experiments as the number of ways to color the tree graph will be cumbersome (Read, 1968).

The number of ways to color the tree graph is called as chromatic polynomial and it is represented by P (G, k) where G is the graph and k is the number of color given to color the graph. Graph 3-coloring is a NP-complete (Papadimitriou, 2003) problem and it cannot be solved in polynomial time. Hence it will be difficult for the hackers to crack it. Tree graphs shown in Figure 7.15, Figure 7.16 and Figure 7.17 with their combinations were used in conducting our experiments. The derivation of chromatic polynomial for the tree graphs is explained in this section.

Case (i)

The number of possible ways to color the root vertex (A) = k ways

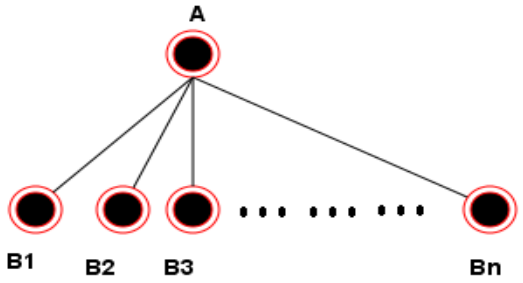


Figure.7.15. Tree with single root vertex

The number of possible ways to color the remaining 'n' vertices ($B_1, B_2, \ldots, B_n$) = (k-1) ways

Chromatic polynomial for case (i) = $[k*(k-1)^n]$ ways (7.7)

Case (ii)

In this case there are two different ways to color the root vertices.

a) Assigning the same color to the root vertices
b) Assigning different color to the root vertices

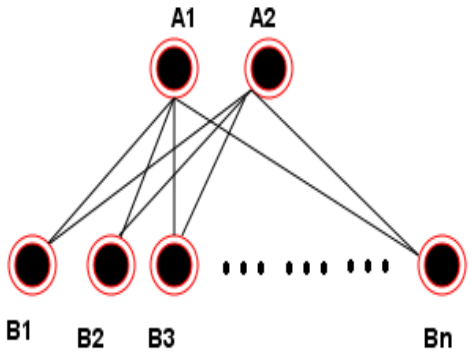


Figure.7.16. Tree with two root vertices

a) Assigning the same color to the root vertices

This coloring schema is same as case (i) and it is explained below

The number of possible ways to color the root vertices (A_1 and A_2) = k ways

The number of possible ways to color the remaining vertices ($B_1, B_2, \ldots, B_n$) = (k-1) ways

Chromatic polynomial of the graph in case (ii) where same color is assigned to root vertices = $[k*(k-1)^n]$ ways

b) Assigning different colors to the root vertices

The number of possible ways to color the root vertex A_1 = k ways

The number of possible ways to color the root vertex A_2 = (k-1) ways

The number of possible ways to color the remaining vertices ($B_1, B_2, \ldots, B_n$) = (k-2) ways

Chromatic Polynomial of the graph in case (ii) where different colors are assigned to root vertices = $[k*(k-1)*(k-2)^n]$ ways

Chromatic polynomial for case (ii) = $[k*(k-1)^n] + [k*(k-1)*(k-2)^n]$ (7.8)

Case (iii)

In this case there are three different ways to color the root vertices.

a) Assigning the same color to all root vertices
b) Assigning the same color to two root vertices
c) Assigning different colors to each root vertices

Assigning the same color to all root vertices is same as case 2 (a) and assigning the same color to two root vertices out of three root vertices in Figure 7.17 can be done in 3 different ways. In section 5.2.3 it is mentioned that the graph assigned for the cover-image is solved for 3-coloring problem. If three different colors are assigned to root vertices (A_1,A_2 and A_3) the remaining vertices ($B_1, B_2, \ldots, B_n$) cannot be colored as no color is left out to color leave nodes which are directly connected to the root vertices. Hence assigning three different colors to the three root vertices is ruled out.

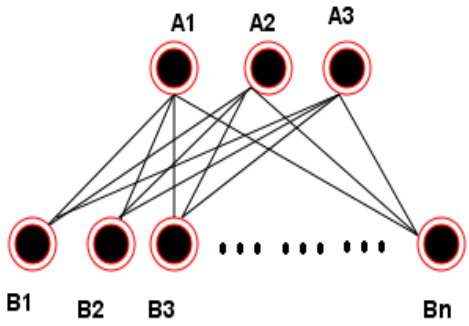


Figure.7.17. Tree with three root vertices

Chromatic polynomial for case (iii)= $[k*(k-1)^n] + 3[k*(k-1)*(k-2)^n]$ (7.9)

The graph taken for RDS algorithm contains minimum 20 vertices. For 20 vertices the chromatic polynomial is calculated from Eq.7.7, Eq. 7.8, and Eq.7.9 are around 3 million which shows the toughness and complexities of the graph 3 coloring problem.

As the number of key combinations obtained for the graph is very large, brute force attack on the key in RDS algorithm will take many years to crack (Schneier, 1996). Following Table 7.14 shows the chromatic polynomial of the various graphs with minimum 20 vertices.

Table.7.14. Chromatic Polynomial of the sample tree graph with 20 vertices

S.No	Graph	Chromatic Polynomial
1	$K_{1,20}$	31,45,728
2	$K_{2,20}$	31,45,734
3	$K_{3,20}$	31,45,746

7.6.1.3. Behavior of Brute Force Attack on the Key in PBIS-3D Algorithm

In PBIS-3D algorithm the key is generated from the secret message which is to be embedded in the cover-image. For every different message to be embedded, the key generated will be different. Using the key, the triangle mesh is formed and from the triangle mesh, vertices of the triangle are chosen for embedding.

The changes in the secret message will lead to different triangle mesh formation and it is shown through an example in Table 6.1. As the secret message is embedded in the vertices of the triangle and it is distributed randomly throughout the image it is difficult for the attackers to extract the message using brute force attack. Even a small variation in the secret message leads to drastic change in the key which results in different triangle mesh formation.

7.6.2. Behavior of Sequential Pixel and Fixed Bits Extraction Attack in the Proposed Algorithms

Mostly LSB steganography algorithms will embed data sequentially in all the pixels and the fixed number of bits are embedded in the pixels of the cover-image. In contrast, the proposed DPIS, RDS and PBIS-3D algorithm does not follow sequential embedding as it skips some of the pixels from embedding data and variable number of bits is embedded in the chosen pixels. Hence, attacker who tries to extract the data sequentially or extract same number of bits from all the pixels in stego-image will fail to extract the embedded secret message.

The sequential pixel extraction and fixed bits extraction attacks are performed on DPIS, RDS and PBIS-3D stego-images and the results are tabulated in Table 7.15. The baboon, eye and flower are the cover-image taken as inputs for DPIS, RDS and PBIS-3D algorithms respectively and secret messages of short length ranging from 350 to 500 bits are embedded in the above cover-images.

Table.7.15. Results of Sequential pixel extraction and fixed bit extraction attacks on DPIS, RDS and PBIS-3D generated stego-images

Algorithm	Image	Experiment	Embedded Secret Message in cover medium	Result
DPIS Algorithm	Baboon	Sequential pixel extraction attack	Prof.G.Aghila, Department of Computer Science, Pondicherry University	QibP(97u2q<<]4]n D |:8*~v&N-FKKeW;'
		Fixed bits extraction attack		T+*m*-&#tKK`w0 -xy
RDS Algorithm	Eye	Sequential pixel extraction attack	P.Thiyagarajan, Research Scholar, School of Engineering and Technology	> þO > 6_ t i t l e 5 • CJ$ OJPJ QJ^J PK ! ,Š¼ú
		Fixed bits extraction attack		ËjÃ0E÷…þƒÐ¶Ørº(¥ØÎ¢Iw},Òä±- j□ „4Éßwì¸Pº t#bÎ™{U® • ã *Y
PBIS-3D Algorithm	Flower	Sequential pixel extraction attack	SSE Project, Sponsored by National Technical Research Organization (NTRO)	eªÔ-Ðµ¸ùÖý ÿÿPK ! ky–*f* Š 7c»(Eb²Ë®»ö ß •
		Fixed bits extraction attack		`j-×ëõº½zAÏ °ïƒ¦V– 2ÍF • -ÞÉi– @öqžv·Ö¬5|‰þÊœ Ì-N§Ól ïƒ¦

The sequential pixel extraction and fixed bits extraction attacks are performed on the stego-images generated by all the three proposed algorithms. Since all three proposed algorithms do not follow sequential pixel embedding and fixed bits embedding, the results obtained from this attack is junk data and it is shown in the last column of Table 7.15.

7.6.3. Geometrical Attacks

Apart from the attacks discussed in the section 7.6.2, geometrical attacks also scrambles the secret message embedded in the stego-image. Geometrical attacks such as scaling, rotation and cropping are experimented in the stego-images generated by the three proposed algorithms. The details of the geometrical attacks are described below:

Scaling

Scaling is the geometrical attack which resizes the digital image. This scaling attack is performed on the stego-images to destroy or modify the content of the secret message embedded in the stego-image. Scaling attack is performed on the stego-image generated by DPIS, RDS and PBIS-3D algorithms on different scaling values 0.5, 1.5 and 2.0.

Rotation

In the rotation geometrical attack, the pixel position (x_1, y_1) in the cover-image is shifted to (x_2, y_2) in the stego-image by rotating through specified angle. This rotation attack is performed on the stego-image generated by all the three proposed algorithms. The stego-image generated by DPIS, RDS and PBIS-3D algorithms is rotated in 45^o, 60^o, 90^o, 120^o angles and impact of the rotation attack in the stego-image is discussed.

Cropping

Cropping refers to removing the outer part of the image. This attack is performed on the stego-image to destroy or remove the secret message embedded in it. 10%, 20% and 30% cropping attack is done on the stego-image generated by DPIS, RDS and PBIS-3D algorithms and the impact of the cropping attack in the stego-image is discussed.

The robustness of the DPIS, RDS and PBIS-3D algorithms against geometrical attacks is tested by calculating Normalized Correlation (NC) value. This NC value is calculated between the stego-image and the attacked stego-image. If the NC values are equal to or close to 1 then it means that the stego-image resists the geometrical attacks. The NC value is calculated as shown in Eq. 7.10

$$NC = \rho(SI, ASI) = \frac{\sum_{i=0}^{n} SI(i)\, ASI(i)}{\sqrt{\sum_{i=0}^{n} SI^2(i)}\sqrt{\sum_{i=0}^{n} ASI^2(i)}} \tag{7.10}$$

where

SI is the stego-image ,

ASI is the attacked stego-image and

n is the size of the cover-image and the stego-image

The section below explains the experimental results of the geometrical attacks on different stego-images with static payload generated by the DPIS, RDS and PBIS-3D algorithms. The behavior of geometrical attacks in the stego-image generated by DPIS, RDS and PBIS-3D algorithms with different payloads are discussed in Appendix-A.

7.6.3.1. Behavior of Geometrical Attacks in DPIS Algorithm

Scaling, rotation and cropping attacks were tested with four different images such as apple, dosa, lena and tiger and the results are presented in Table 7.16. The scaling, rotation and cropping attack are experimented with different values as shown in Table 7.16.

Table.7.16. Resistance of DPIS algorithm against geometrical attacks

Attacks		**NC value for Apple image**	**NC value for Dosa image**	**NC value for Lena image**	**NC value for Tiger image**
Scaling	**0.5**	0.7071	0.7081	0.7071	0.7072
	1.5	0.8165	0.8170	0.8165	0.8166
	2.0	0.7071	0.7082	0.7071	0.7075
Rotation	**45^o**	0.7163	0.6090	0.6962	0.6963
	60^o	0.7504	0.7541	0.7213	0.7214
	90^o	1.000	0.8664	1.000	1.000
	120^o	0.7504	0.7041	0.7213	0.7214
Cropping	**10%**	0.9709	0.9468	0.9591	0.9612
	20%	0.9016	0.9075	0.9323	0.9376
	30%	0.8874	0.8911	0.9056	0.9142

From the experimental results shown in Table 7.16 it is observed that the NC values for scaling attacks vary between 0.7 and 0.8. The NC values for rotation attacks vary between 0.6 and 1.0 and the NC values of cropping attacks vary between 0.8 and 0.9. From the results shown in Table 7.16 it is observed that the NC values are above 0.6 which shows that the DPIS generated stego-image reasonably resists against geometrical attacks.

7.6.3.2. Behavior of Geometrical Attacks in RDS Algorithm

The RDS algorithm is tested for geometrical attacks with various medical images. Normalized Correlation (NC) values are calculated between the RDS stego-image and

the attacked stego-image and the results are shown in Table 7.17. The NC values for scaling attacks for RDS stego-image vary between 0.7 and 1.0.

The NC values for RDS algorithm rotation attack vary between 0.8 and 1.0 and NC values for cropping attack are above 0.8. From the results tabulated in Table 7.17 it is observed that NC value for RDS stego-image and the attacked RDS stego-image are above 0.75 which shows that the RDS algorithm sensibly resists geometrical attacks.

Table.7.17. Resistance of RDS algorithm against geometrical attacks

Attacks		**NC value for Brain image**	**NC value for Eye image**	**NC value for Kidney image**	**NC value for Lungs image**
Scaling	**0.5**	0.8512	1.000	1.000	1.000
	1.5	0.8295	0.8671	0.8647	0.08769
	2.0	0.7614	0.7826	0.8013	0.7738
Rotation	**45^o**	0.9121	0.9321	0.8910	0.9321
	60^o	0.9481	0.8547	0.9243	0.9242
	90^o	0.8589	0.9205	0.8508	0.9562
	120^o	0.8928	1.000	1.000	1.000
Cropping	**10%**	0.9981	0.9999	0.9959	0.9893
	20%	0.9647	0.9725	0.9628	0.9751
	30%	0.9354	0.9204	0.88	0.87

7.6.3.3. Behavior of Geometrical Attacks in PBIS-3D Algorithm

Four different images are taken for testing PBIS-3D algorithm for geometrical attacks. Scaling, rotation and cropping attacks were tested for different values and Normalized Correlation (NC) values are computed to find the resistance of the PBIS-3D algorithm against these attacks and it is depicted in Table 7.18.

NC values for scaling attacks vary between 0.8 and 0.9. The PBIS-3D algorithm generated stego-images are completely resistant to rotation attack as the NC values for stego-image and the rotated stego-image is one. The NC values for cropping attack vary between 0.8 and 0.9. All the NC values computed for PBIS-3D algorithm generated stego-image and attacked stego-image are above 0.85 which shows PBIS-3D algorithm strongly resists geometrical attacks.

From the experimental results shown in Table 7.16, Table 7.17 and Table 7.18 it is evident that most of the NC values for the stego-image and the attacked stego-image varies between 0.7 and 1.0 which portrays that the strength of the stego-images generated by the DPIS, RDS and PBIS-3D algorithms. The next section explains the behavior of the three proposed algorithms on noise and filtering attacks.

Table.7.18. Resistance of PBIS-3D algorithm against geometrical attacks

Attacks		**NC value for Bunny image**	**NC value for Horse image**	**NC value for Dragon image**	**NC value for Car image**
Scaling	**0.5 X**	0.9765	0.9456	0.9890	0.9678
	1.5 Y	0.985	0.952	0.973	0.968
	2.0 Z	0.987	0.896	0.942	0.87
Rotation (45^o, 60^o, 90^o,120^o)		1	1	1	1
Cropping	**10%**	0.9988	0.9999	0.9995	0.9983
	20%	0.933	0.985	0.96	0.97
	30%	0.913	0.902	0.88	0.87

7.6.4. Noise and Filtering Attacks

The DPIS, RDS and PBIS-3D stego-images are tested for noise and filtering attacks. The filtering techniques are generally applied to images for improving their quality. On applying these filtering techniques the embedded messages in the stego-image will alter. There are many filtering techniques out of which Median filtering and Gaussian filtering are applied to the stego-images generated by the three proposed algorithms. In order to measure the number of bits changed due to filtering attack, Bit Error Rate (BER) was calculated.

Adding noise is another attack which alters the secret message embedded in the stego-image. Two different noises, Gaussian noise and Salt and pepper noise, were added in the DPIS, RDS and PBIS-3D generated stego-images with the variance of 0.02 and 0.05. BER value is calculated to find the number of bits changed due to noise attack in the stego-image. The experimental results of filtering and noise attacks on the stego-images generated by the three proposed algorithms are discussed in the next section.

7.6.4.1. Behavior of Noise and Filtering Attacks in DPIS Algorithm

Filtering and noise attacks were performed on DPIS algorithm generated stego-images. The impact of noise and filtering attacks are measured by BER. As discussed in section 7.4, BER is the ratio of the number of bit errors that occurred during transmission to the total number of bits transmitted. Four different images are taken for these experiments and the messages with lengths in the range 20,000 to 90,000 bits are embedded in the image. Several experiments were conducted and the average of the results is shown in Table 7.19.

Table.7.19. DPIS Algorithm - BER experimental results for filtering and noise attacks

Images	**Size of secret message embedded**	**Median Filtering**	**Gaussian Filtering**	**Noise adding**			
				Gaussian with variance		**Salt & pepper with variance**	
				0.02	**0.05**	**0.02**	**0.05**
Apple	20,000 - 30,000	2.19	2.87	3.78	4.16	4.74	5.24
Lena	40,000 - 50,000	3.24	3.39	4.67	4.98	5.17	5.53
Dosa	60,000 - 70,000	3.89	4.21	5.64	6.25	5.98	6.47
Tiger	80,000 - 90,000	4.96	4.84	4.71	5.61	6.84	7.48

The experimental results shown in Table 7.19 show that around 96% of the bits were extracted successfully from DPIS stego-image which is prone to filtering attack and around 93% of the bits were extracted successfully from DPIS stego-image which is prone to noise attack.

7.6.4.2. Behavior of Noise and Filtering Attacks in RDS Algorithm

RDS algorithm is experimented with the medical images such as brain, eye, kidney and lungs. BER is used to measure the bit error occurred in the RDS stego-image due to noise and filtering attack. The stego-images used in this experiment were obtained by embedding different lengths of secret messages in the range 20,000 to 90,000 bits.

Table.7.20. RDS Algorithm - BER experimental results for filtering and noise attacks

Images	Size of secret message embedded	Median Filtering	Gaussian Filtering	Noise adding			
				Gaussian with variance		Salt & pepper with variance	
				0.02	0.05	0.02	0.05
Brain	20,000 - 30,000	1.12	1.85	1.54	1.92	2.08	2.57
Eye	40,000 - 50,000	1.07	2.27	2.42	2.64	2.61	2.98
Kidney	60,000 - 70,000	1.41	1.78	2.65	2.54	2.84	3.41
Lungs	80,000 - 90,000	1.76	1.54	2.06	2.16	3.23	3.67

The experiments were conducted repeatedly and the average of the result is projected in Table 7.20. Around 98% of the bits embedded were successfully extracted from the RDS stego-image which is prone to filtering attack. Also around 97% of the secret message bits embedded in the RDS generated stego-images are extracted successfully which are prone to noise attack.

7.6.4.3. Behavior of Noise and Filtering Attacks in PBIS-3D Algorithm

The 3D images, horse, dragon, car and bunny were taken for experiments to analyze the behavior of noise and filtering attacks. BER is used as parameter to analyze the impact of noise and filtering attacks in PBIS-3D stego-image.

Table.7.21. PBIS-3D Algorithm - BER experimental results for filtering and noise attacks

Images	Size of secret message embedded	Median Filtering	Gaussian Filtering	Noise adding			
				Gaussian with variance		Salt & pepper with variance	
				0.02	0.05	0.02	0.05
Horse	20,000 - 30,000	1.98	3.14	2.93	3.21	4.14	4.71
Dragon	40,000 - 50,000	2.23	2.65	4.66	4.86	3.35	5.23
Car	60,000 - 70,000	2.05	1.23	4.15	5.21	2.61	5.07
Bunny	80,000 - 90,000	1.06	2.37	3.12	3.53	3.72	4.67

Four different message groups in the range 20,000 to 90,000 bits were embedded in the 3D cover-image and these experiments were conducted repeatedly and the average value of the result are projected in Table 7.21. Around 98% of the embedded bits were extracted from PBIS-3D stego-image which is prone to filtering attack and around 95% of the embedded bits were extracted from the PBIS-3D stego-images under noise attack.

Interpretation of results

The robustness of the proposed algorithms is tested by exposing the stego-image generated by the three proposed algorithms to various attacks such as cropping, scaling, rotation, filtering and noise. The results discussed above by testing the three proposed algorithms for robustness are encouraging. The next section compares the three proposed algorithms with other spatial domain image steganography algorithms.

7.7. COMPARISON OF PROPOSED ALGORITHM WITH SIMILAR OTHER EXISTING ALGORITHMS

The proposed DPIS, RDS and PBIS-3D algorithm were compared with the similar other existing algorithms against various parameters and it is presented in this section.

7.7.1. Comparison of DPIS Algorithm with Similar Other Existing Algorithms

Dynamic Pattern based Image Steganography (DPIS) algorithm is compared with (Parvez and Gutub, 2008) and (Gutub et al., 2008) algorithms with the parameters such as key, brute force attack, number of bits embedded in the data channel, sequential data embedding in all the pixels and integrity of the message. The comparison is shown in Table 7.22.

The nature of the key in DPIS algorithm is dynamic while the key for other steganography algorithms taken for comparison are either static or vary among red, green and blue color. Since the key size is large and dynamic in DPIS algorithm it is not possible to find the key using brute force attack.

(Parvez and Gutub, 2008) and (Gutub et al., 2008) algorithm follow sequential embedding whereas the DPIS algorithm does not follow sequential pixel embedding and pixels are chosen for embedding with the help of dynamic key. In DPIS algorithm the secret message are embedded in the color channel which contribute less to the

pixel color, this procedure is followed in order to make sure that embedding does not affect pixel color drastically.

Table.7.22. Comparison of DPIS algorithm with similar other steganography algorithms

Algorithms / Parameters	**Parvez and Gutub, 2008 method**	**Gutub et al., 2008 method**	**DPIS algorithm**
Key	Vary among Red, Green or Blue	Static	Varying with different length
Brute force attack	Breakable	Breakable	Not Breakable
Number of bits embedded in data channel	Static and depends on partition schema	Static	Dynamic and its decided at run time
Sequential data embedding in all pixels	Yes	No	No
Integrity of the stego-image	NA	NA	Possible

*(Yes – Availability of the quality in the method; No – Non availability of the quality in the method NA- Not Available)

In DPIS algorithm, the number of bits to be embedded in each pixel is decided by the value of the data channel of that pixel. The integrity of the DPIS algorithm generated stego-image can be checked at the DPIS extraction part by using hash function whereas the same is not been made sure in other two algorithms considered for comparison.

7.7.2. Comparison of RDS Algorithm with Similar Other Existing Algorithms

RDS algorithm is compared with the five recent similar steganography algorithms. They are (Bouslimi et al., 2012, Dhavale, 2010, Mohamed Ali Hajjaji, Abdellatif Mtibaa, El-bey Bourennane., 2011, Dogan et al., 2012, Das and Kundu, 2012). These algorithms were compared with the parameters such as domain, extraction, resistance against geometric transformations, dynamic key, number of bits embedded in a pixel, reversible property and integrity. The detailed comparison is shown in Table 7.23.

(Dhavale, 2010) and (Das and Kundu, 2012) algorithms belongs to frequency domain while all the other algorithms taken for comparison belong to spatial domain

algorithms. All the algorithms taken for comparison do not need the cover-image during extraction hence blind extraction is followed in these algorithms. (Dogan et al., 2012) and RDS algorithm resists geometric transformations attack while the rest of the algorithms did not report that information in their experiments.

Table.7.23. Comparison of RDS algorithm with similar other steganography algorithms

Algorithms / Parameters	**Bouslimi et al., 2012**	**Dhavale, 2010**	**Mohamed Ali Hajjaji, Abdellatif Mtibaa, El-bey Bourennane., 2011**	**Dogan et al., 2012**	**Das and Kundu, 2012**	**RDS algorithm**
Domain	Spatial	frequency	Spatial	frequency	frequency	Spatial
Extraction	Blind	Blind	Blind	Blind	Blind	Blind
Robust – Geometric Transformation	NA	NA	NA	Yes	NA	Yes
Key	Static	Static	Static	Static	Static	Dynamic
Number of bits embedded in a pixel	Static	Static	Static	Static	Static	Dynamic
Reversible Algorithm	No	No	No	No	No	Yes
Detection of transmission error	Yes	Yes	Yes	No	No	Yes

*(Yes – Availability of the quality in the method; No – Non availability of the quality in the method NA- Not Available)

Pixel selection and the number of bits embedded in the selected pixels are dynamic in RDS algorithm while other algorithms taken for comparison are static in nature. RDS algorithm along with (Bouslimi et al., 2012, Dhavale, 2010, Mohamed Ali Hajjaji, Abdellatif Mtibaa, El-bey Bourennane., 2011) could find the error that is introduced during transmission. RDS algorithm restores the cover-image from the stego-image after extracting the secret message, while the other algorithms do not reverse the cover-image from stego-image.

7.7.3. Comparison of PBIS-3D Algorithm with Similar Other Existing Algorithms

PBIS-3D algorithm is compared with five algorithms (Aspert et al., 2002**,** Cayre and Macq, 2003**,** Maret and Ebrahimi, 2004**,** Wang and Cheng, 2005 and Cheng and Wang, 2006). These algorithms are compared in line with the parameters such as domain, extraction, robust geometric transformation, mesh formation, number of bits embedded in a pixel and robust against noise attacks and it is shown in Table 7.24. PBIS-3D algorithm is in spatial domain and the cover-image is not required for extracting secret message. Hence it follows the blind procedure during extraction.

Table.7.24. Comparison of PBIS-3D algorithm with similar other steganography algorithms

Algorithms / Parameters	Aspert et al., 2002	Cayre and Macq, 2003	Maret and Ebrahimi, 2004	Wang and Cheng, 2005	Cheng and Wang, 2006	PBIS-3D Algorithm
Domain	Transform	Spatial	Transform	Spatial	Spatial	Spatial
Extraction	Blind	Blind	Blind	Blind	Blind	Blind
Robust – Geometric Transformation	Yes	Yes	Yes	Yes	Yes	Yes
Mesh formation	Static	Static	Static	Static	Static	Dynamic
Number of bits embedded in a pixel	Static	Static	Static	Static	Static	Dynamic
Robust -Noise attacks	Yes	No	No	No	No	Yes

(Yes – Availability of the quality in the method; No – Non availability of the quality in the method)

All the algorithms taken for comparison are resistant to geometric attacks. The mesh formation in PBIS-3D algorithm is dynamic as it varies with the message to be embedded. All the other algorithms taken for comparison follow static procedure for mesh formation. The number of bits to be embedded in the vertices of the triangle in PBIS-3D algorithm varies with respect to the key bit assigned to it where as other algorithms considered for comparison embed static number of bits. (Aspert et al., 2002**)** and PBIS-3D algorithms are resistant to noise attack where as other algorithms taken for comparison are not resistant to noise attack.

7.8. SUMMARY

This chapter discussed the various experiments carried out to check the efficiency of the proposed algorithms. The proposed algorithms are evaluated with the various metrics like capacity, invisibility and are subjected to statistical tests also. From the experimental results it is proved that the three proposed algorithms uses less number of pixels compared to other existing algorithms. The invisibility nature of secret message in stego-image is proved through histogram analysis of the cover-images and the stego-images. The proposed algorithms generated stego-images are of good quality which has been proved through PSNR, MSE and BER statistical metrics. The association of the cover-image and the stego-image generated by the proposed algorithms has been tested with chi-square test. The robustness of the stego-images generated by DPIS, RDS and PBIS-3D algorithm are tested with different attacks such as scaling, rotation, cropping, noise and filtering attacks. The experiments are repeated and the average of the results have been projected and found to be encouraging. The DPIS, RDS and PBIS-3D algorithms are compared with existing algorithms against various parameters. The next chapter discusses the applications of the DPIS, RDS and PBIS-3D algorithms in various domains.

CHAPTER 8

APPLICATIONS OF THE PROPOSED ALGORITHMS

Any research finding should be applied to the real world for the use of common man. In this line this chapter discusses the different domains where the proposed Dynamic Pattern based Image Steganography (DPIS), Reversible Dynamic NROI based Steganography using Graph Coloring (RDS) and Pattern based 3D Image Steganography (PBIS-3D) algorithms are applied. In section 8.1 the applications of DPIS algorithm in the Internet banking domain are discussed. In section 8.2 and section 8.3 the applications of RDS and PBIS-3D algorithms in medical domain are discussed. Apart from the domains discussed below the proposed algorithms can also be applied to other domains and this is considered as future enhancements.

8.1. APPLICATIONS OF DPIS ALGORITHM IN BANKING DOMAIN

Image steganography can be applied to a number of fields where exchange of secret information is mandatory. For example, in the medical field image steganography may be used for storing patient information in the digital medium. On the other hand in military field it can be used for transmission of secret information. The developed Dynamic Pattern based Image Steganography (DPIS) algorithm, is applied in Internet banking domain to enhance the transaction security and to prevent the phishing attack. The following section discusses the application of DPIS algorithm in Internet banking.

8.1.1. Enhancing Transaction Security in Internet Banking using DPIS Algorithm

It is mandatory that any banking industry which provides Internet banking facility should always provide secure and reliable connection. Advanced Encryption Standard (AES) is the most common cryptographic algorithm used in Internet[7] for providing security. In this work, an attempt has been made to enhance the security in banking domain, by introducing 'stego-layer' which uses DPIS algorithm in both client and the server side for secure transaction. Any data that passes through the client-server

[7] "First Flaws in the Advanced Encryption Standard Used for Internet Banking Identified" http://www.sciencedaily.com/releases/2011/08/110817075424.htm Retrieved on: 15th April 2013

architecture will have to pass through the stego-layer. The architecture of the proposed stego-layer method is shown in Figure.8.1.

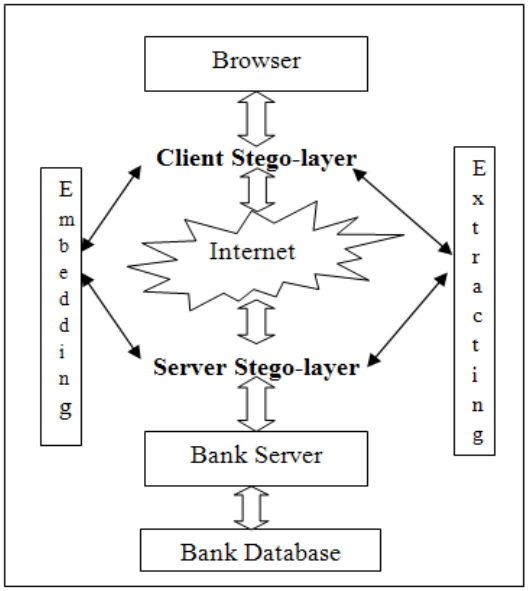


Figure.8.1. Architecture of DPIS Stego-layer Method

In Internet banking any data that is transmitted between client and server will always employ some cryptography algorithms like AES for secure transactions. As already discussed in this method a 'stego-layer', an additional layer is introduced on both the client and server sides which uses DPIS algorithm for both the embedding and extracting process. Since steganography is coupled with cryptography this method enhances the Internet banking transaction security. The step wise process of how the stego-layer method works while the user uses the above architecture to execute his/her transaction is explained in the following steps.

- When a user login into banking website with the customer-id, the customer-id is validated and then the stego-key is issued by the bank server for the particular session to the client.
- Each user will be assigned an image. Once the user authenticates the image, the system prompts for entering the username and password.
- Once the user enters the username and password, it is encrypted by the cryptography algorithm as deployed by bank and the encrypted user credentials will be embedded with the help of stego-key in the user specific image. The resultant image (stego-image) is transmitted to the server.

- At the server side, the content is extracted from the stego-image using stego-key assigned for the particular session. The extracted message is the encrypted text of the user credentials and it is decrypted by the corresponding decryption algorithm deployed by the bank.

The implementation of the proposed stego-layer method is done in ASP.Net and the DPIS embedding and extracting procedure is developed in MATLAB and its executable is invoked in ASP.Net. There are many methods proposed in the literature to enhance the security of Internet banking transaction. This DPIS stego-layer method is compared with the standard Advanced Encryption Standard (AES) against functional and non-functional parameters and it is shown in Table 8.1. The non-functional parameters used for comparison are performance, efficiency and time to decipher the message. The functional parameters used for comparison are key length, integrity and covertness in communication.

Table.8.1. Comparison of DPIS Stego-Layer method with Advanced Encryption Standard algorithm

Type	**Parameters**	**AES Algorithm**	**Stego-layer method**
Non functional parameters	Performance	+++	**++++**
	Efficiency	+++	**++++**
	Time need to decipher a message	++++	**+++**
Functional Parameters	Key	Static and vary with 3 different key length	**Dynamic**
	Identification of tampered message at receiver's side	No	**Yes**
	Covertness in message transmission	No	**Yes**

(+++ - Good ++++ - Very Good)

The performance and efficiency is appraised with respect to security. Since stego-layer is built above cryptographic layer it provides enhanced security when compared to AES algorithm. Hence ++++ is given for stego-layer method and +++ for AES algorithm. Since the time taken to decipher a message for stego-layer is longer than the time taken for AES algorithm, ++++ is awarded to AES and +++ to stego-layer method. In AES cryptographic algorithm, three different key lengths of size, 128 bits, 192 bits and 256 bits are used, whereas in stego-layer method keys of any length are

used and it is dynamic. By using Hash algorithm the stego-layer method reports any tampering during transmission of the stego-image. Thus integrity is addressed whereas this mechanism is not available in AES. Since the stego-layer method involves image steganography it hides the content inside the image where as AES only modifies the original text to encrypted text.

This section explained the application of DPIS algorithm to enhance the transaction security in Internet banking domain. The next section explains how the DPIS algorithm is applied in banking domain to prevent the phishing attack.

8.1.2. Pixastic – DPIS Algorithm Based Anti-phishing Browser Plug-in

Internet has provided a lot of comfort to human life, on the other hand it has its own security concerns too. One such threat from which Internet banking suffers is phishing. In phishing, the attacker creates a website which looks similar to the original bank website and the link is send to the user. Once the user clicks the link it will navigate to a fake website. Since the fake website resembles the legitimate website, the user will tend to give their user name and password which will make the attacker to get hold of the user account. Literature proves that though there are many anti-phishing mechanisms still the user still falls prey for phishing attacks[8].

In this work an attempt has been made to prevent phishing attack, by providing a browser plug-in which uses DPIS algorithm. The browser plug-in is named as Pixastic. Following are the two prerequisite that is essential for the working of pixastic browser plug-in:

a) Any bank website which wishes to uses Pixastic should keep the stego-image generated by DPIS algorithm in their website login page.
b) The user who is possessing Internet banking transaction facility should install Pixastic browser plug-in in their browser from legitimate bank website.

The architecture of the Pixastic plug-in consists of three components, browser, server and user. The browser component consists of subcomponents such as scanner, DPIS extraction and message handler. The architecture of the Pixastic is shown in the Figure 8.2.

[8] "Phishing Activity Trends Report 4th Quarter 2012"
http://docs.apwg.org/reports/apwg_trends_report_Q4_2012.pdf Retrieved on: 20th April 2013

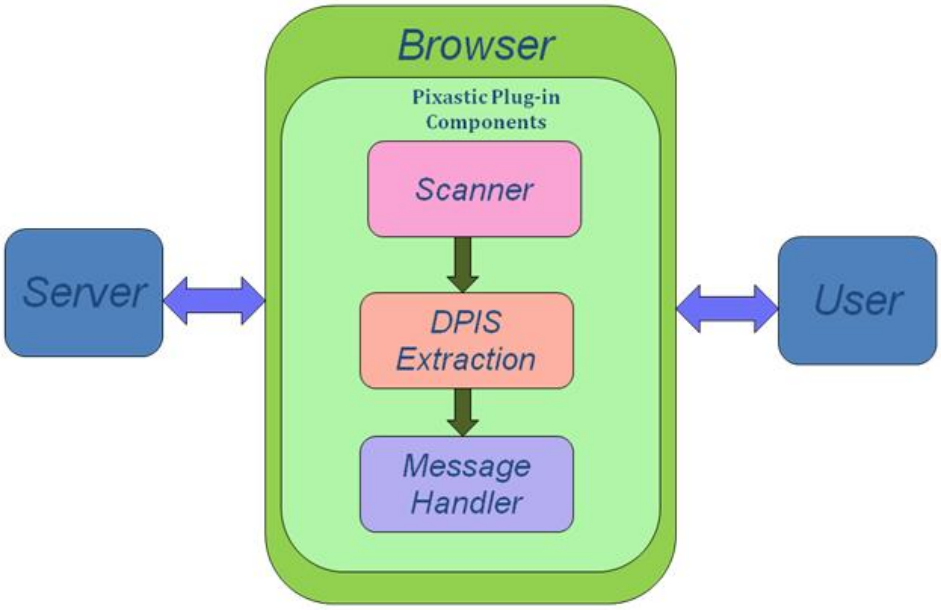


Figure.8.2. Architecture of Pixastic browser plug-in

Scanner scans the browser address bar to find whether the banking site for which the Pixastic was developed is being accessed. If the site for which the browser plug-in was developed is being accessed then Pixastic plug-in will get triggered automatically. Pixastic which is triggered will locate the stego-image generated by the DPIS algorithm in the banking website and the stego-image is passed to the DPIS extraction part. The extraction part extracts the secret message from the stego-image. The extracted message is compared with the message in the plug-in. If it matches then the user is allowed to enter the user credentials else all the controls in the website will be blocked and a warning is displayed to the user about the validity of the website. The workflow of the Pixastic browser plug-in is depicted in Figure 8.3.

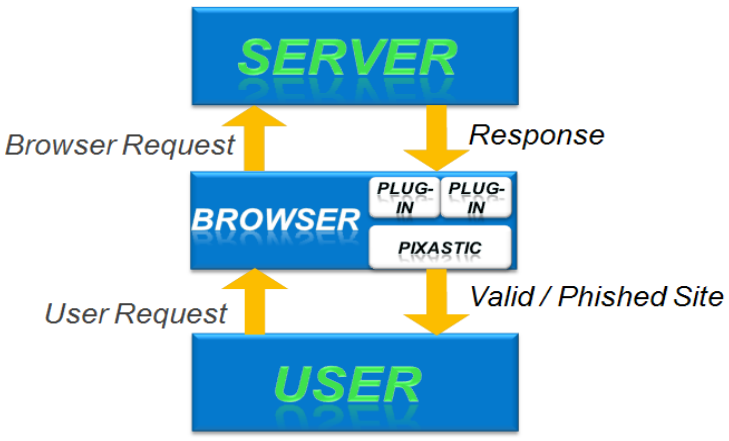


Figure.8.3. Workflow of DPIS Pixastic browser plug-in

This Pixastic browser plug-in was developed in safari browser and is tested for its functionalities. The prototype developed for Pixastic browser plug-in is shown in Figure 8.4.

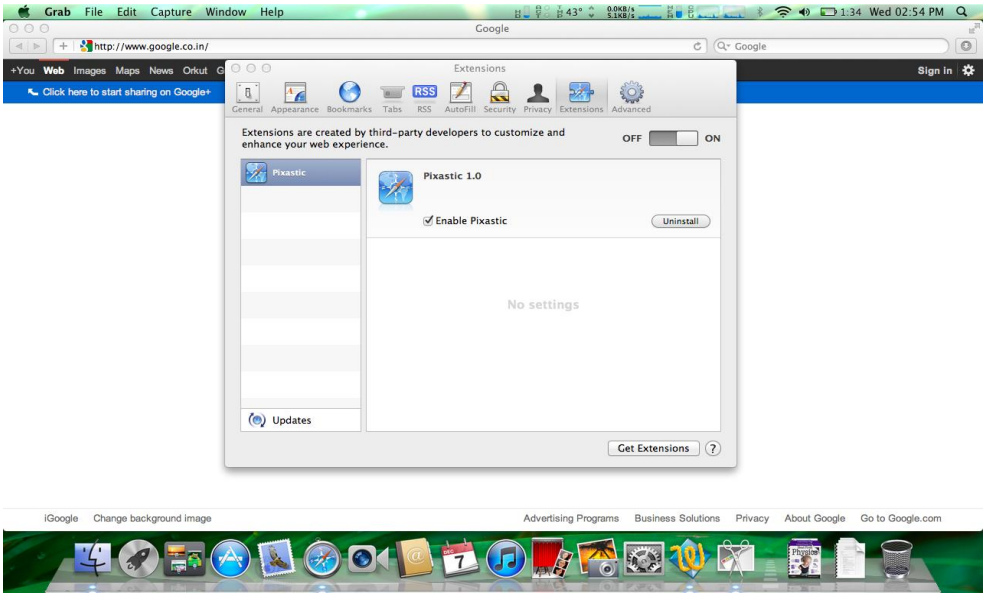


Figure.8.4. DPIS algorithm – Pixastic browser plug-in screen shot

The pixastic browser plug-in is compared with other existing browser plug-in such as Net Craft, Trust Watch, Phish Net, Spoof Stick and Spam Blocker which are discussed in section 2.3.2.2 as a part of literature review. The robustness, visibility of the result, preventing user from accessing phished website, aesthetic and privacy and training costs are the six parameters which are used to compare the Pixastic with other plug-in and it is shown in Table 8.2. The grading has been given to different plug-ins where +++ stands for very good, ++ for good, + for average, -- for substandard. The evaluation criteria that are followed to rate these plug-in are explained below.

All the browser plug-ins taken for comparisons are generic in nature where as Pixastic plug-in is specific for bank websites. DNS (Domain Name System) spoofing is one of the attacks in Internet banking domain, where the user request for a particular website is re-directed to hackers system by fooling the DNS Session. Net Craft and Pixastic plug-in are resistant to DNS spoofing attack but Net Craft is given '+' where as Pixastic is given '++' as the people using Net Craft needs prior knowledge about the location of the website. If the website which the user is accessing is found to be phished site, then the Pixastic plug-in displays warning message about the validity of

the website. But the other browser plug-in displays the website validity in the browser which user may go unnoticed. Hence '+++' is given to Pixastic for visibility of result.

The Pixastic, apart from giving warning message also blocks all the controls in the phished website. Thus even if the user ignores the message, he or she will not be able to enter the user credentials. In other plug-ins there is a possibility that the user may ignore the message given by the plug-in and they may enter their details. In such cases user will fall prey to the phished site. Hence other plug-ins were given '- -'and Pixastic is given '++'.

Table.8.2. Comparison of Pixastic browser plug-in with other existing Anti-Phishing Plug-ins

Plug-ins	**Type of Plug-in**	**Robustness**	**Visibility of the Result**	**Prevent user from accessing Phished website**	**Aesthetic and Privacy**	**Training Costs**
Net craft	**Generic**	+	--	--	+	--
Trust Watch	**Generic**	--	--	--	+	--
Phish Net	**Generic**	--	--	--	+	--
Spoof Stick	**Generic**	--	--	--	+	--
Scam Blocker	**Generic**	--	--	--	+	--
Pixastic Plug-in	**Specific**	++	+++	++	++	+++

+++ stands for very good, ++ for good, + for average, -- for substandard

Pixastic does not add any extra components in the browser. Therefore '++' is given to Pixastic for Aesthetic and privacy parameter and '+' is given for other plug-ins as they introduced a separate component in the browser. For Net craft and Spoof stick plug-ins user should be trained to know the host place and the domain name of the website for their safe browsing. In Trust watch, Spoof stick and Phish net the users need to be trained on the functionalities of the toolbar to prevent them from phishing attack. Pixastic does not require the user to be trained on domain name, hosting place of the website, hence '+++' is given to Pixastic plug-in and '-'to other plug-ins. The following section discusses about the application of the RDS algorithm to medical and GIS domain.

8.2. APPLICATION OF THE RDS ALGORITHM

The Reversible Dynamic NROI based Steganography algorithm using Graph Coloring (RDS) is applied to medical domain and Geographical Information System (GIS) domain. In RDS algorithm, the given input image is split into ROI and NROI region. The NROI region is used to embed the secret message. In medical image, the information about the patient is embedded in the NROI region of image where as in GIS domain the information about the metadata of the map image is embedded. The experimental results of RDS algorithm on medical images were discussed in the previous chapter. The application of RDS algorithm on the GIS image and medical image is illustrated through Figure 8.5 and Figure 8.6 respectively.

Figure.8.5. GIS Cover image (left) and GIS Stego-image (right) with 1500 bits embedded by RDS algorithm Image Size: 266 x 190

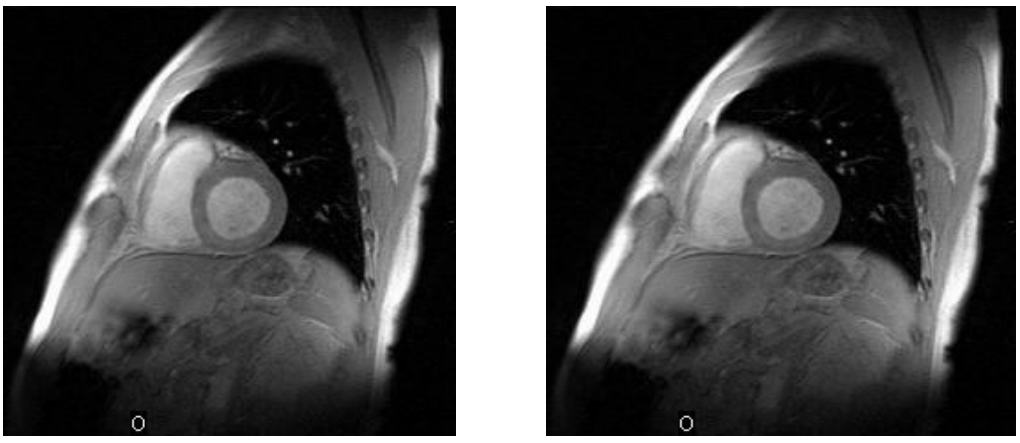


Figure.8.6. Medical Cover image (left) and Medical Stego-image (right) with 1500 bits embedded by RDS algorithm Image Size: 256 x 256

8.3. APPLICATION OF PBIS-3D ALGORITHM

Pattern Based 3D Image Steganography (PBIS-3D) algorithm is applied to medical domain. Recently there is a transit from 2D medical images to 3D medical images (Sakas, 2002) which gives more information to the doctor for diagnosis. PBIS-3D algorithm is applied to 3D medical image for hiding the patient medical data inside the medical image thus preventing the unauthorized person from viewing the patient's medical data. Generally in medical image steganography only the essential patient information will be embedded in the image such that it does not affect the content of the medical image. Figure 8.7 shows the heart cover medical image and heart stego medical image generated using PBIS-3D algorithm.

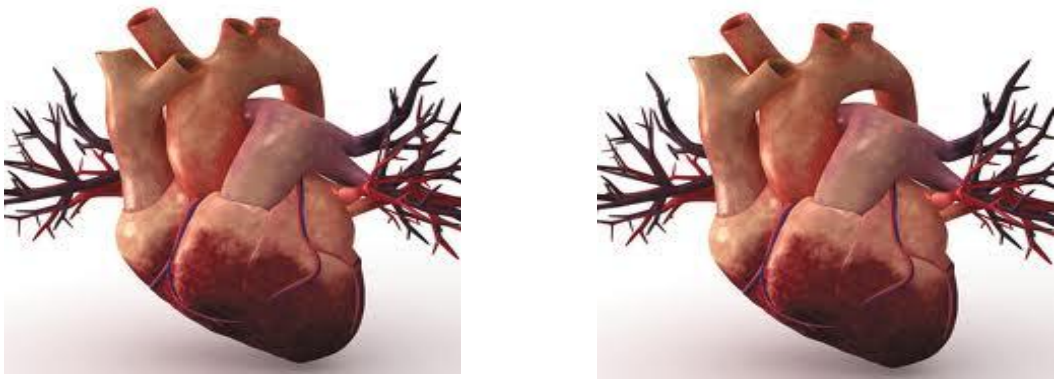


Figure.8.7. Medical Cover image (left) and Medical Stego-image (right) with 1500 bits embedded by PBIS-3D algorithm Image Size: 225 x 224

8.4. SUMMARY

This chapter presented the various domains where the DPIS, RDS and PBIS-3D algorithms were applied. DPIS is applied to Internet banking domain to enhance the transaction level security and to prevent phishing attack. DPIS stego-layer method is proposed to enhance the transaction level security and DPIS Pixastic browser plug-in is proposed to prevent phishing attack. RDS and PBIS-3D algorithms are applied to medical domain where the patient information is hidden inside the medical images. RDS algorithm is also applied to GIS domain to hide the metadata about the location in GIS images.

CHAPTER 9

CONCLUSION AND FUTURE DIRECTIONS

This chapter summarizes the dynamic approaches in spatial domain image steganography which are achieved through dynamic keys. The conclusions derived from this thesis and the future directions of this research work are discussed in this chapter.

9.1. CONCLUSION

The detailed literature survey on 2D and 3D spatial domain image steganography algorithms was carried out to understand the characteristics of existing algorithms. The existing algorithms were analyzed critically and their limitations were discussed. The research issues in spatial domain image steganography algorithms are explored through three research questions. This thesis addressed all the three research questions by proposing DPIS, RDS and PBIS-3D algorithms.

The "Research Question-1" is concerned with encompassing dynamicity in spatial domain image steganography. This thesis addressed this question by proposing three algorithms namely Dynamic Pattern based Image Steganography (DPIS) algorithm, Reversible Dynamic NROI based Steganography algorithm using graph coloring (RDS) and Pattern Based 3D Image Steganography (PBIS-3D) algorithm. In DPIS algorithm, the dynamicity is ensured by the random key generation for each embedding process. In RDS algorithm the dynamicity is addressed by the graph which is assigned to every cover-image. The graph is assigned to the cover-image with the help of the pixels in the Region of Interest (ROI). The assigned graph is solved for graph 3-coloring and the resultant colors of the graph vertices are used as the key for embedding and extracting. The dynamicity in PBIS-3D is ensured through the secret message which is to be embedded in the cover-image. In the given cover-image, the initial triangle is formed by taking the maximum values from all the three axes and this initial triangle is used as the base for triangle mesh formation. The initial triangle is bifurcated somewhere around the middle of the edge with the help of the decomposition ratio which is obtained from the secret message. The number of

triangle meshes formed from the initial triangle depends on the size of the secret message to be embedded in the cover-image.

The “Research Question-2” is about strengthening security in the spatial domain image steganography algorithms using dynamic key. The dynamic keys generated by the DPIS, RDS and PBIS-3D algorithms are used to select the pixels for embedding the secret message bits and also to embed variable number of bits in the selected pixels.

The proposed three algorithms were implemented using Matlab and evaluated with series of parameters such as capacity, invisibility and statistical test. The robustness of the stego-image generated by DPIS, RDS and PBIS-3D algorithms are also tested with various attacks. Capacity metric quantifies the number of pixels used for embedding various lengths of secret messages whereas originality retention quantifies the originality of the cover-image which is retained after embedding the secret message. Various experiments were conducted for embedding different lengths of secret messages in different images with different color compositions and the average of results was analyzed and projected. The average originality retentions of the DPIS and PBIS-3D algorithms, for embedding 90,000 to 1, 00,000 bits of secret message in the cover-image, are 87.18 % and 78.75% respectively. The invisibility parameter is evaluated by drawing the histograms of the cover-image and the stego-image. Histograms are drawn for the cover-images and the stego-images generated from DPIS, RDS and PBIS-3D algorithms. The quality of the stego-images generated by the proposed algorithms is proved by visual analysis of the histograms.

PSNR, MSE and BER are the parameters used for statistical test. The messages with lengths between 80,000 and 84,000 bits are embedded in the nature cover-image using DPIS algorithm and the average of PSNR, MSE and BER values obtained for the nature cover-image and the stego-image are 47.55, 1.14 and 0.05 respectively. Generally in RDS algorithm, only secret messages of short length are embedded. Medical images are chosen for experimenting RDS algorithm. The messages with lengths between 1550 and 1850 bits are embedded in the lung cover-image using RDS algorithm and the average of PSNR, MSE and BER values obtained for the lung cover-image and the stego-image are 68.14, 0.02 and 0.001 respectively. The average of PSNR, MSE and BER obtained for the bunny cover-image and bunny stego-image

which is generated by the PBIS-3D algorithm by embedding secret message bits of 74,000 to 78,000 are 45.96, 1.66 and 0.08 respectively. The PSNR value of the three proposed algorithms are above 40 db and the MSE and BER of these proposed algorithms were as low as possible which portrays that the stego-image generated by the DPIS, RDS and PBIS-3D are statistically not distinguishable from the cover-image. The chi-square test for independence is also tested for cover-image and the DPIS, RDS and PBIS-3D algorithms generated stego-images at 5% level of significance. The chi-square test shows that the cover-image and the stego-image generated by the three proposed algorithms are strongly correlated.

The robustness of the DPIS, RDS and PBIS-3D algorithms were tested with different attacks such as brute force attacks on key, fixed bits extraction attack, sequential pixel extraction attack, geometrical attacks, noise and filtering attacks. Normalized Correlation (NC) value is calculated to find the impact of geometrical attacks on the stego-images generated by the three proposed algorithms. The NC is above 0.7 which depicts the robustness of the stego-image generated by the DPIS, RDS and PBIS-3D algorithms. Bit Error Rate (BER) value is calculated to find the error rate introduced by the filtering and noise attacks in the stego-image generated by the DPIS, RDS and PBIS-3D algorithms and it varies between 1.06 and 7.48.

The "Research Question-3" is about the application of the proposed spatial domain image steganography algorithms. This thesis explored the application of the three proposed algorithms in Internet banking domain and medical domain. DPIS algorithm is applied to Internet banking domain to enhance the transaction level security by introducing 'stego-layer' method. DPIS algorithm was also used to prevent the phishing attack by developing a browser plug-in named as pixastic. RDS and PBIS-3D algorithms are applied to medical domain to hide the patient information in the medical image.

The conclusions derived from this research "Dynamic Key based Approaches for Security Amelioration in Spatial Domain Image Steganography" in a nutshell are listed below:

- Dynamicity is encompassed in the spatial domain image steganography algorithms by generating the key randomly (DPIS), generating the key from the image (RDS) and generating the key from the secret message (PBIS-3D)

- The stego-images generated from the three dynamic spatial domain image steganography algorithms are resistant towards scaling, rotating, cropping, noise and filtering attacks and this is proved through experimental results.

- The DPIS algorithm is applied to Internet banking domain. The RDS algorithm and PBIS-3D algorithm are applied to medical domain. RDS algorithm is also applied to GIS domain.

The following section explains the future directions of this research work.

9.2. FUTURE DIRECTIONS

In this research, an attempt is made to introduce dynamicity in spatial domain image steganography algorithm. The algorithms developed in this research can be extended further with the following aspects:

- In the same line of the proposed spatial domain image steganography algorithm, dynamicity could be experimented for the frequency domain image steganography.

- Statistical property of the cover-image can be explored to introduce the dynamicity in spatial and frequency domain image steganography.

- Another dimension is to carry out this research work towards reverting the cover-image completely from the extraction part.

- Another endeavor for encompassing dynamicity can be devised by considering the dominant and submissive color in the given image.

REFERENCES

Abd-Eldayem, M.M., 2013. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. Egyptian Informatics Journal. 14, pp.1–13.

Abraham, A., Paprzycki, M., 2004. Significance of steganography on data security, in: International Conference on Information Technology: Coding and Computing (ITCC 2004). pp. 347–351.

Acharya, U.R., Subbanna Bhat, P., Kumar, S., Min, L.C., 2003. Transmission and storage of medical images with patient information. Computers in Biology and Medicine. 33, pp.303–310.

Agarwal, P., Prabhakaran, B., 2009. Robust Blind Watermarking of Point-Sampled Geometry. IEEE Transactions on Information Forensics and Security. 4, pp. 36 –48.

Al-Husainy, M.A.F., 2011. A New Image Steganography Based on Decimal-Digits Representation. Computer and Information Science. 4, pp.38–47.

Alface, P.R., Macq, B., 2005. Blind watermarking of 3D meshes using robust feature points detection, in: IEEE International Conference on Image Processing (ICIP 2005). pp. 693–696.

Amat, P., Puech, W., Druon, S., Pedeboy, J.P., 2010. Lossless 3D steganography based on MST and connectivity modification. Signal Processing: Image Communication. 25, pp.400–412.

Amin, P.K., Liu, N., Subbalakshmi, K.P., 2007. Statistical attack resilient data hiding. International Journal of Network Security. 5, pp. 112–120.

Aspert, N., Drelie, E., Maret, Y., Ebrahimi, T., 2002. Steganography for three-dimensional polygonal meshes, in: SPIE 47th Annual Meeting. pp. 705–708.

Bahi, J.M., Couchot, J.F., Friot, N., Guyeux, C., 2012. Application of Steganography for Anonymity through the Internet, in: The First Workshop on Information Hiding Techniques for Internet Anonymity and Privacy. pp. 96 –101.

Behbahani, Y.M., Ghayour, P., Farzaneh, A.H., 2011. Eigenvalue Steganography based on eigen characteristics of quantized DCT matrices, in: International Conference on Information Technology and Multimedia (ICIM 2011). pp. 1 –4.

Beineke, L.W., Wilson, R.J., Cameron, P.J., 2004. Topics in Algebraic Graph Theory. Book by Cambridge University Press.

Bergholz, A., Chang, J.H., Paaß, G., Reichartz, F., Strobel, S., 2008. Improved phishing detection using model-based features, in: Conference on Email and Anti-Spam (CEAS 2008). pp. 1–10.

Bhattacharyya, D., Dutta, J., Das, P., Bandyopadhyay, R., Bandyopadhyay, S.K., Kim, T., 2009a. Discrete Fourier Transformation based Image Authentication technique, in: 8th IEEE International Conference on Cognitive Informatics (ICCI 2009). pp. 196 –200.

Bhattacharyya, D., Roy, A., Roy, P., Kim, T., 2009b. Receiver compatible data hiding in color image. International Journal of Advanced Science and Technology. 6, pp.15–24.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A., 2010. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. Advances in Cryptology–EUROCRYPT 2010. pp. 299–319.

Bouslimi, D., Coatrieux, G., Cozic, M., Roux, C., 2012. A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. IEEE Transaction on Information Technology in Biomedicine. 16, pp. 891–899.

Cayre, F., Macq, B., 2003. Data hiding on 3-D triangle meshes. IEEE Transaction on Signal Processing. 51, pp. 939–949.

Chan, C.K., Cheng, L.M., 2004. Hiding data in images by simple LSB substitution. Pattern Recognition. 37, pp. 469–474.

Chandramouli, R., Kharrazi, M., Memon, N., 2004. Image steganography and steganalysis: Concepts and practice, in: International Workshop on Digital Watermarking (IWDW 2004). Springer (LNCS). pp. 35–49.

Chang, C.C., Tai, W.L., Chen, K.N., 2008. Lossless data hiding based on histogram modification for image authentication, in: IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC 2008). pp. 506–511.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P., 2010. Digital image steganography: Survey and analysis of current methods. Signal Processing. 90, pp. 727–752.

Chen, W.J., Chang, C.C., Le, T., 2010. High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications. 37, pp. 3292–3301.

Cheng, Y.M., Wang, C.M., 2006. A high-capacity steganographic approach for 3D polygonal meshes. The Visual Computer. 22, pp. 845–855.

Cho, J.W., Prost, R., Jung, H.Y., 2007. An Oblivious Watermarking for 3-D Polygonal Meshes Using Distribution of Vertex Norms. IEEE Transaction on Signal Processing. 55, pp. 142 –155.

Chou, C.M., Tseng, D.C., 2006. A public fragile watermarking scheme for 3D model authentication. Computer-Aided Design. 38, pp. 1154–1165.

Cotting, D., Weyrich, T., Pauly, M., Gross, M., 2004. Robust watermarking of point-sampled geometry, in: International Conference on Shape Modeling Applications. pp. 233 – 242.

Das, S., Kundu, M.K., 2012. Effective Management of Medical Information Through A Novel Blind Watermarking Technique. Journal of Medical Systems. 36, pp. 3339–3351.

Dey, S., Abraham, A., Sanyal, S., 2007. An LSB Data Hiding Technique Using Prime Numbers, in: Third International Symposium on Information Assurance and Security (IAS 2007). pp. 101–108.

Dhamija, Rachna, Tygar, J.D., 2005a. Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks, in: Second International Workshop on Human Interactive Proofs (HIP 2005). pp. 127–141.

Dhamija, R., Tygar, J.D., 2005b. The battle against phishing: Dynamic security skins, in: ACM Symposium on Usable Privacy and Security (UPS 2005). pp. 77–88.

Dharwadkar, N.V., Amberker, B.B., Supriya, Panchannavar, P.B., 2010. Reversible fragile medical image watermarking with zero distortion, in: International Conference on Computer and Communication Technology (ICCCT 2010). pp. 248 –254.

Dhavale, S.V., 2010. Blind Robust Image Adaptive Watermarking for Medical Images with Multilevel Security. International Journal of Computer Science and Application.1, pp.87–90.

Dogan, S., Tuncer, T., Avci, E., Gulten, A., 2012. A New Watermarking System Based on Discrete Cosine Transform (DCT) in Color Biometric Images. Journal of Medical Systems. 36, pp. 1–7.

Fette, I., Sadeh, N., Tomasic, A., 2007. Learning to detect phishing emails, in: 16th International Conference on World Wide Web (WWW 2007). pp. 649–656.

Fridrich, J., Goljan, M., 2003. Digital image steganography using stochastic modulation, in: International Conference on Security and Watermarking of Multimedia Contents (SWMC 2003). pp. 191–202.

Gang, W., Ni-ni, R., 2005. A Fragile Watermarking Scheme for Medical Image, in: 27th IEEE Annual International Conference of Engineering in Medicine and Biology Society (EMBS 2005). pp. 3406 –3409.

Garera, S., Provos, N., Chew, M., Rubin, A.D., 2007. A framework for detection and measurement of phishing attacks, in: ACM Workshop on Recurring Malcode (WORM 2007). pp. 1–8.

Garg, H., Agrawal, S., Varshney, G., 2012. Double Security Watermarking Algorithm for 3D Model using IEEE-754 Floating Point Arithmetic. International Journal of Computer Applications. 46, pp. 18–22.

Gribunin, V.G., Okov, I.N., Turintsev, I.V., 2002. Digital steganography. Book by SOLON-Press Mosc.

Gutub, A., Ankeer, M., Abu-Ghalioun, M., Shaheen, A., Alvi, A., 2008. Pixel indicator high capacity technique for RGB image based Steganography, in: 5th IEEE International Workshop on Signal Processing and Its Applications (WoSPA 2008).

Hiltgen, A., Kramp, T., Weigold, T., 2006. Secure Internet banking authentication. IEEE Security Privacy. 4, pp.21 –29.

Hussain, M., 2010. Pixel intensity based high capacity data embedding method, in: International Conference on Information and Emerging Technologies (ICIET 2010). pp. 1–5.

Hussain, M., Hussain, M., 2011. Embedding data in edge boundaries with high PSNR, in: 7th International Conference on Emerging Technologies (ICET 2011). pp. 1 –6.

Johnson, N.F., Jajodia, S., 1998. Exploring steganography: Seeing the unseen. IEEE Explore Computer. 31, pp. 26–34.

Juneja, M., Sandhu, P.S., 2013. Two Components based LSB and Adaptive LSB Steganography based on Hybrid Feature Detection for Color Images with improved PSNR and Capacity. International Journal of Computer Science and Electronics Engineering. 1, pp. 345-351.

Kahn, D., 1996. The history of steganography, in: First International Workshop on Information Hiding. 2578, pp. 1–5.

Kanzariya Nitin, K., Nimavat Ashish, V., 2013. Comparison of Various Images Steganography Techniques. International Journal of Computer Science and Management Research. 2, pp. 1213–1217.

Karni, Z., Gotsman, C., 2000. Spectral compression of mesh geometry, in: 27th Annual Conference on Computer Graphics and Interactive Techniques. pp. 279–286.

Keshari, S., Modani, S.G., 2011. Weighted fractional Fourier Transform based image Steganography, in: International Conference on Recent Trends in Information Systems (ReTIS 2011). pp. 214 –217.

Kondoz, A., 2009. Visual Media Coding and Transmission. Book by John Wiley & Sons.

Lavoué, G., 2009. A local roughness measure for 3D meshes and its application to visual masking. ACM Transactions on Applied perception. 5, pp.1-23.

Lavoué, G., Denis, F., Dupont, F., 2007. Subdivision surface watermarking. Computer Graphics 31, pp. 480–492.

Lavoué, G., Denis, F., Dupont, F., Baskurt, A., 2006. A watermarking framework for subdivision surfaces. Multimedia Content Representation, Classification and Security. 4105, pp.223–231.

Lee, Y.K., Bell, G., Huang, S.Y., Wang, R.Z., Shyu, S.J., 2009. An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding, in: 3rd Pacific Rim Symposium on Advances in Image and Video Technology (PSIVT 2009). pp. 349–360.

Li, C.T., Li, Y., 2009. Medical Images Authentication through Repetitive Index Modulation Based Watermarking. International Journal of Digital Crime Forensics IJDCF. 1, pp. 32–39.

Liang, H.Y., Cheng, C.H., Yang, C.Y., Zhang, K.F., 2013. A Blind Data Hiding Technique with Error Correction Abilities and a High Embedding Payload. Journal Applied Research and Technology. 11, pp. 259–271.

Lim, Y., Xu, C., Feng, D.D., 2001. Web based image authentication using invisible Fragile watermark, in: Workshop on Visual Information processing (VIP 2001), 11. pp. 31–34.

Liu, Y., Prabhakaran, B., Guo, X., 2008. A robust spectral approach for blind watermarking of manifold surfaces, in: 10th ACM Workshop on Multimedia and Security (MM&SEC 2008). pp. 43–52.

Luo, W., Huang, F., Huang, J., 2010. Edge Adaptive Image Steganography Based on LSB Matching Revisited. IEEE Transaction on Information Forensics Security. 5, pp. 201 –214.

Luo, X., Liu, F., Lu, P., 2007. A LSB steganography approach against pixels sample pairs steganalysis. International Journal of Innovative Computing, Information and Control (IJICIC). 3, pp. 575–588.

Ma, J., Saul, L.K., Savage, S., Voelker, G.M., 2009a. Beyond blacklists: learning to detect malicious web sites from suspicious URLs, in: 15th ACM International Conference on Knowledge Discovery and Data Mining (KDD 2009). pp. 1245–1254.

Ma, J., Saul, L.K., Savage, S., Voelker, G.M., 2009b. Identifying suspicious URLs: an application of large-scale online learning, in: 26th Annual International Conference on Machine Learning (ICML 2009). pp. 681–688.

Majeed, A., Kiah, M.L.M., Madhloom, H.T., Zaidan, B.B., Zaidan, A.A., 2009. Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and Technology. 1, pp.63–69.

Malakooti, M.V., Khederzdeh, M., 2012. A Lossless Secure data embedding in image using DCT and Randomize key generator, in: Second International Conference on Digital Information and Communication Technology and It's Applications (DICTAP 2012). pp. 236 –239.

Mandal, J.K., Das, D., 2012. Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. International Journal of Information Science and Technology. 2, pp.83–93.

Mao, X., Shiba, M., Imamiya, A., 2001. Watermarking 3D geometric models through triangle subdivision, in: Security and Watermarking of Multimedia Contents (SWMC 2001). pp. 253–260.

Maret, Y., Ebrahimi, T., 2004. Data hiding on 3D polygonal meshes, in: ACM Workshop on Multimedia and Security (WMS 2004). pp. 68–74.

Marvel, L.M., Boncelet Jr, C.G., Retter, C.T., 1998. Reliable blind information hiding for images, in: Second International Workshop on Information Hiding (IH 1998). pp. 48–61.

McKeon, R.T., 2006. Steganography using the Fourier Transform and Zero-Padding Aliasing Properties, in: IEEE International Conference on Electro/information Technology. pp. 492 –497.

Mohamed Ali Hajjaji., Abdellatif Mtibaa., El-bey Bourennane., 2011. A Watermarking of Medical Image:Method based LSB. Journal of Emerging Trends in Computing and Information Sciences. 2, pp.714–721.

Mohan, M., Anurenjan, P.R., 2011. A new algorithm for data hiding in images using contourlet transform, in: IEEE Recent Advances in Intelligent Computational Systems (RAICS 2011). pp. 411 –415.

Motameni, H., Norouzi, M., Jahandar, M., Hatami, A., 2007. Labeling method in Steganography, in: World Academy of Science, Engineering and Technology (SCT 2007). pp. 349–354.

Moulin, P., Koetter, R., 2005. Data-Hiding Codes, in: Conference Proceedings of IEEE, 93. pp.2083 –2126.

Nadernejad, E., Sharifzadeh, S., Hassanpour, H., 2008. Edge detection techniques: evaluations and comparisons. Applied Mathematical Sciences. 2, pp. 1507–1520.

Nagaraja, S., Houmansadr, A., Piyawongwisal, P., Singh, V., Agarwal, P., Borisov, N., 2011. Stegobot: a covert social network botnet, in: 13th International Conference on Information Hiding (IH 2011). pp. 299–313.

Nergui, M., Acharya, U.S., Acharya U, R., Yu, W., 2009. Reliable and Robust Transmission and Storage Techniques for Medical Images with Patient Information. Journal of Medical Systems. 34, pp. 1129–1139.

Ni, Z., Shi, Y.Q., Ansari, N., Su, W., 2006. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology. 16, pp. 354–362.

Nikoukar, A.A., 2010. An Image Steganography Method with High Hiding Capacity Based on RGB Image. International Journal of Signal and Image Processing. 1, pp.238–241.

Nissar, A., Mir, A.H., 2010. Classification of steganalysis techniques: A study. Digitial Signal Processing. 20, pp. 1758–1770.

Ohbuchi, R., Masuda, H., Aono, M., 1997. Watermarking three-dimensional polygonal models, in: Fifth ACM International Conference on Multimedia (ICM 1997). pp. 261–272.

Ohbuchi, R., Mukaiyama, A., Takahashi, S., 2002. A frequency-domain approach to watermarking 3D shapes, in: Computer Graphics Forum. pp. 373–382.

Ohbuchi, R., Mukaiyama, A., Takahashi, S., 2004. Watermarking a 3D shape model defined as a point set, in: International Conference on Cyberworlds (ICC 2004). pp. 392–399.

Ohbuchi, R., Takahashi, S., Miyazawa, T., Mukaiyama, A., 2001. Watermarking 3D polygonal meshes in the mesh spectral domain, in: Graphics Interface (GRIN 2001). pp. 9–18.

Othman, F., Maktom, L., Taqa, A.Y., Zaidan, B.B., Zaidan, A.A., 2009. An extensive empirical study for the impact of increasing data hidden on the images texture, in: International Conference on Future Computer and Communication (ICFCC 2009). pp. 477–481.

Panneerselvam, R., 2004. Research Methodology. Book by PHI Learning Pvt. Ltd.

Papadimitriou, C.H., 2003. Computational complexity. Book by John Wiley and Sons Ltd.

Parvez, M.T., Gutub, A.A.A., 2008. RGB intensity based variable-bits image steganography, in: IEEE Asia-Pacific Services Computing Conference (APSCC 2008). pp. 1322–1327.

Picione, D.D.L., Battisti, F., Carli, M., Astola, J., Egiazarian, K., 2006. A Fibonacci LSB data hiding tecnique, in: 14th European Signal Processing Conference (EUSIPCO 2006).

Pieprzyk, J., Hardjono, T., Seberry, J., 2003. Fundamentals of Computer Security. Book by Springer.

Prabakaran, G., Bhavani, R., 2012. A modified secure digital image steganography based on Discrete Wavelet Transform, in: International Conference on Computing, Electronics and Electrical Technologies (ICCEET 2012). pp. 1096 –1100.

Provos, N., Honeyman, P., 2003. Hide and seek: an introduction to steganography. IEEE Security and Privacy. 1, pp. 32–44.

Qi, K., Zhang, D.F., Xie, D., 2010. A high-capacity steganographic scheme for 3D point cloud models. Information Technology Journal. 9, pp. 412–421.

Read, R.C., 1968. An introduction to chromatic polynomials. Journal of Combinatorial Theory. 4, pp. 52–71.

Reserve Bank of India, 2003. Report on Internet Banking by RBI.

Sajedi, H., Jamzad, M., 2008. Adaptive steganography method based on contourlet transform, in: 9th International Conference on Signal Processing (ICSP 2008). pp. 745 –748.

Sakas, G., 2002. Trends in medical imaging: from 2D to 3D. Computer Graphics. 26, pp. 577–587.

Sarreshtedari, S., Ghaemmaghami, S., 2010. High Capacity Image Steganography in Wavelet Domain, in: 7th IEEE Consumer Communications and Networking Conference (CCNC 2010). pp. 1 –5.

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition Book by Wiley.

Seyedi, S.H., Aghaeinia, H., Sayadian, A., 2011. A new robust image adaptive steganography method in wavelet domain, in: 19th Iranian Conference on Electrical Engineering (ICEE 2011). pp. 1 –5.

Shih, F.Y., 2007. Digital Watermarking and Steganography: Fundamentals and Techniques, 1st ed. Book by CRC Press, Inc., Boca Raton, FL, USA.

Soman, C., Pathak, H., Shah, V., Padhye, A., Inamdar, A., 2008. An Intelligent System for Phish Detection, using Dynamic Analysis and Template Matching. World Academy of Science, Engineering and Technology. 42, pp. 321–327.

Song, X., Wang, S., Niu, X., 2012. An Integer DCT and Affine Transformation Based Image Steganography Method, in: Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2012). pp. 102 –105.

Tan, C.I., Lin, C.K., Tai, W.K., Chang, C.C., 2009. Hiding data: a high-capacity distortionless approach. Multimedia Systems 15, pp. 325–336.

Taubin, G., 1995. A signal processing approach to fair surface design, in: 22nd Annual Conference on Computer Graphics and Interactive Techniques (CGIT 1995). pp. 351–358.

Tirandaz, H., Davarzani, R., Monemizadeh, M., Haddadnia, J., 2009. Invisible and High Capacity Data Hiding in Binary Text Images Based on Use of Edge Pixels, in: International Conference on Signal Processing Systems (ICSPS 2009). pp. 130–134.

Todorov, D., 2010. Mechanics of User Identification and Authentication: Fundamentals of Identity Management. Book by Taylor & Francis.

Tu, S., hsu, H.W., Tai, W., 2010. Permutation steganography for polygonal meshes based on coding tree. International Journal of Virtual Reality. 9, pp. 55-60.

Tu, S.C., Tai, W.K., 2012. A high-capacity data-hiding approach for polygonal meshes using maximum expected level tree. Computer Graphics. 36, pp. 767–775.

Uccheddu, F., Corsini, M., Barni, M., 2004. Wavelet-based blind watermarking of 3D models, in: Workshop on Multimedia and Security (WMS 2004). pp. 143–154.

Ulutas, G., Ulutas, M., Nabiyev, V.V., 2010. Reversible secret image sharing scheme with enhanced stego image visual quality, in: International Conference on Information Society (i-Society 2010). pp. 157–161.

Ulutas, M., Ulutas, G., Nabiyev, V.V., 2011. Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of System Software. 84, pp. 341–353.

Upreti, K., Verma, K., Sahoo, A., 2010. Variable Bits Secure System for Color Images, in: Second International Conference on Advances in Computing, Control and Telecommunication Technologies (ACT 2010). pp. 105 –107.

Vallet, B., Lévy, B., 2008. Spectral geometry processing with manifold harmonics, in: Computer Graphics Forum. pp. 251–260.

Viswanatham, V.M., Manikonda, J., 2010. A Novel Technique for Embedding Data in Spatial Domain. International Journal of Computer Science Engineering. 2, pp. 233–236.

Wagner, D., Schneier, B., 1996. Analysis of the SSL 3.0 protocol, in: The Second USENIX Workshop on Electronic Commerce Proceedings. pp. 29–40.

Wang, C.M., Cheng, Y.M., 2005. An Efficient Information Hiding Algorithm for Polygon Models, in: Computer Graphics Forum.24, pp.591–600.

Wang, C.-M., Wang, P.-C., 2006. Steganography on point-sampled geometry, in: Computer Graphics. 30, pp. 244–254.

Wang, K., Lavoué, G., Denis, F., Baskurt, A., 2007. Hierarchical blind watermarking of 3D triangular meshes, in: IEEE International Conference on Multimedia and Expo (ICME 2007). pp. 1235–1238.

Wang, K., Lavoué, G., Denis, F., Baskurt, A., 2008. Hierarchical watermarking of semiregular meshes based on wavelet transform. IEEE Transaction on Information Forensics Security. 3, pp. 620–634.

Wang, K., Luo, M., Bors, A.G., Denis, F., 2009. Blind and robust mesh watermarking using manifold harmonics, in: 16th IEEE International Conference on Image Processing (ICIP 2009). pp. 3657–3660.

Wei-Chih, H., Yu, T.Y., 2009. E-mail spam filtering using support vector machines with selection of kernel function parameters, in: Fourth International Conference on Innovative Computing, Information and Control (ICICIC 2009). pp. 764–767.

William, S., Stallings, W., 2006. Cryptography And Network Security, 4/E. Book by Pearson Education.

Wu, C.C., Kao, S.J., Hwang, M.S., 2011. A high quality image sharing with steganography and adaptive authentication scheme. Journal of System Software. 84, pp. 2196–2207.

Yang, C.Y., 2007. Color image steganography based on module substitutions, in: Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2007). pp. 118–121.

Yang, G., Zhou, Y., 2009. LSB Algorithm Research Based on Chaos, in: Ninth International Conference on Hybrid Intelligent Systems (ICHIS 2009). pp. 427 –430.

Younes, M.A.B., Jantan, A., 2008. A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion. International Journal of Computer Science and Network Security. 8, pp. 247–257.

Yu, Z., Ip, H.H.S., Kwok, L.F., 2003. A robust watermarking scheme for 3D triangular mesh models. Pattern Recognition. 36, pp.2603–2614.

Zaz, Y., 2010. Protecting EPR Data Using Cryptography and Digital Watermarking, in: International Conference Models Information Communication Systems (ICMIC 2010). 1, pp. 1-4.

Zeng, X., Ping, L., Li, Z., 2009. Lossless data hiding scheme using adjacent pixel difference based on scan path. Journal of Multimedia. 4, pp. 145–152.

Zhang, H., 2004. Discrete combinatorial Laplacian operators for digital geometry processing, in: SIAM Conference on Geometric Design and Computing (GDC 2004). pp. 575-592.

APPENDIX – A

RESULTS OF GEOMETRICAL ATTACKS WITH DIFFERENT PAYLOAD

In chapter 7, section 7.6.3 the robustness of the Dynamic Pattern based Image Steganography algorithm (DPIS), Reversible Dynamic NROI based Steganography algorithm using Graph Coloring (RDS) and Pattern based 3D Image Steganography algorithm (PBIS-3D) are tested for geometrical attacks with fixed payload. Here the behavior of DPIS, RDS and PBIS-3D algorithms against geometrical attacks are tested with different payloads.

a) Behavior of the DPIS algorithm against geometrical attacks with variable payload

Scaling, rotation and cropping attacks were tested with Lena image with different payloads in the range 20,000 to 30,000, 40,000 to 50,000, 60,000 to 70,000 and 80,000 to 90,000 bits. Scaling attack is performed on the stego-image with three different parameters such as 0.5, 1.5 and 2.0. The stego-image generated by DPIS algorithm is rotated with four different angles 45^o, 60^o, 90^o and 120^o. Cropping attack is performed on the DPIS stego-image with 10%, 20% and 30%. Normalized Correlation value is calculated between the DPIS stego-image and DPIS attacked stego-image. From the experimental results, shown in the Table A.1 below it is observed that as the size of the message increases the Normalized Correlation (NC) value calculated for the stego-image and the attacked stego-image decreases.

b) Behavior of the RDS algorithm against geometrical attacks with variable payload

The RDS algorithm is tested for geometrical attacks with brain medical image. The brain cover-image is embedded with payload in the range 20,000 to 90,000 bits. Normalized Correlation (NC) value is calculated between the brain stego-image and the attacked brain stego-image. From the experimental results shown in Table A.2 it is observed that when the size of the payload increases the NC values decreases.

c) Behavior of the PBIS-3D algorithm against geometrical attacks with variable payload

The payload in the range 20,000 to 90,000 bits are embedded in the car 3D image and the obtained stego-image are subjected to geometrical attacks such as scaling, rotation and cropping. Normalized Correlation (NC) value for the car 3D stego-image and the attacked car 3D stego-image is calculated and the result in shown in Table A.3. From the result it is obvious that NC value and payload are inversely proportional.

Table.A.1. Resistance of DPIS algorithm generated Lena stego-image with different payload against geometrical attacks

Image	**Payload**	**Attacks**									
		Scaling			**Rotation**				**Cropping**		
		0.5	**1.5**	**2.0**	**45^o**	**60^o**	**90^o**	**120^o**	**10%**	**20%**	**30%**
Lena Image (512*512)	**20,000 to 30,000**	0.71	0.82	0.72	0.69	0.72	1.00	0.72	0.94	0.92	0.89
	40,000 to 50,000	0.68	0.79	0.70	0.71	0.70	1.00	0.68	0.93	0.90	0.88
	60,000 to 70,000	0.66	0.75	0.68	0.67	0.66	1.00	0.64	0.89	0.89	0.86
	80,000 to 90,000	0.63	0.72	0.61	0.64	0.60	1.00	0.60	0.85	0.86	0.80

Table.A.2. Resistance of RDS algorithm generated Brain stego-image with different payload against geometrical attacks

Image	Payload	Attacks									
		Scaling			Rotation				Cropping		
		0.5	1.5	2.0	45^o	60^o	90^o	120^o	10%	20%	30%
Brain Image (512*512)	20,000 to 30,000	0.85	0.82	0.76	0.91	0.94	0.86	0.89	0.99	0.97	0.94
	40,000 to 50,000	0.83	0.79	0.72	0.87	0.91	0.85	0.85	0.95	0.93	0.89
	60,000 to 70,000	0.79	0.74	0.68	0.85	0.87	0.81	0.84	0.93	0.89	0.87
	80,000 to 90,000	0.776	0.72	0.66	0.83	0.84	0.79	0.81	0.89	0.85	0.83

Table.A.3. Resistance of PBIS-3D algorithm generated Car stego-image with different payload against geometrical attacks

Image	Payload	Attacks									
		Scaling			Rotation				Cropping		
		0.5	1.5	2.0	45°	60°	90°	120°	10%	20%	30%
Car Image (1600*1200)	20,000 to 30,000	0.97	0.96	0.88	1.00	1.00	1.00	1.00	0.99	0.97	0.88
	40,000 to 50,000	0.94	0.91	0.85	1.00	1.00	1.00	1.00	0.94	0.91	0.83
	60,000 to 70,000	0.90	0.86	0.78	0.99	0.98	1.00	0.99	0.88	0.87	0.77
	80,000 to 90,000	0.85	0.77	0.75	0.98	0.99	1.00	0.98	0.82	0.81	0.73

LIST OF PUBLICATIONS

I INTERNATIONAL JOURNALS

1. **Thiyagarajan P, Aghila G, "**Reversible Dynamic Secure Steganography for Medical Image using Graph Coloring", *International Journal of Health Policy and Technology, **Elsevier***, Vol.2, no. 3, pp.151-161, ISSN: 2211-8837, 2013.

2. **Thiyagarajan P, Natarajan V, Aghila G, Venkatesan V.P, Anitha R**, Pattern based 3D image Steganography, *International Journal of 3D Research, **Springer*** Vol. 4, pp. 1–8, ISSN: 2092-6731, 2013.

3. **Thiyagarajan P, Aghila G, Prasanna Venkatesan V**, "Pixastic: Steganography based Anti-Phishing Browser Plug-in", *Journal of Internet Banking and Commerce*, Vol. 17, no. 1,ISSN: 1204-5357, 2012. (SNIP : 0.150)

4. **Thiyagarajan P, Aghila G, Prasanna Venkatesan V**, "Dynamic Pattern Based Image Steganography", *Journal of Computing*, Vol. 3, no. 2, pp.117-125, ISSN : 2151-9617, 2011. (Impact Factor : 0.21)

5. **Thiyagarajan P, Aghila G, Prasanna Venkatesan V**, "Stepping up Internet Banking Security using Dynamic Pattern Based Image Steganography", *Springer (LNCS) in Communications in Computer and Information Science Series(CCIS),*Vol. 193, pp.98-112, ISSN: 1865:0929, 2011. (SNIP : 0.020 ; SJR : 0.08)

6. **Thiyagarajan P, Aghila G, Prasanna Venkatesan V**, "Stego-Image Generator (SIG) - Building Steganography Image Database" , *Springer (LNCS) in Communications in Computer and Information Science (CCIS) Series*, Vol.205, pp.257-267, ISSN: 1865:0929, 2011. (SNIP : 0.020 ; SJR : 0.08)

*SNIP – Source Normalized Impact Factor; SJR – SCImago Journal Rank

II DOCTORAL COLLOQUIUM

7. **Thiyagarajan P, Aghila G, Prasanna Venkatesan V,** "Qualitative Analysis of Dynamic Pattern based Image Steganography in providing E-Banking Security", *First IDRBT Doctoral Colloquium by IDRBT*(**A Reserve Bank Institute**), Vol. 15, no. 3, pp.26, ISSN: 0973-2527, 2011.

III CONFERENCES

8. **Thiyagarajan P, Swarnambigai G, Aghila G, Prasanna Venkatesan V**, StegoRivalry: Steganography Vs Steganalysis", *National Conference On Imaging, Computing, Object and Mining (ICOM'10)* ,pp.104-110, ISBN: 978-93-80408-29-3, 2010.

9. **Thiyagarajan P, Prasanna Venkatesan V, Aghila G**, "Anti-Phishing Techniques using Automated Challenge Response Method", *International conference on Communication and Computational Intelligence*, pp.585-590, ISBN: 978-81-8371-369-6 (IEEE Explore), 2010.

VITAE

Mr.P.Thiyagarajan, the author of this thesis, is a full time research scholar in the Department of Computer Science, School of Engineering and Technology, Pondicherry University. He was born on 06th April 1985 at Kumbakonam, India.

He has passed his Integrated M.Sc Computer Science with distinction from College of Engineering Guindy (CEG) Anna University Chennai in the year 2007. At the end of his post graduation he got job offers from Multi-National Companies (MNC) such as TCS, WIPRO and Aricent Technologies. Since he is interested in research, he took up the offer in Research and Development (R&D) division of Aricent Technologies in the year 2008. During his training in Aricent Technologies he won best technical project award.

Owing to pursue doctorate degree, he joined as Research Associate in the Collaborative Directed Basic Research on Smart and Secure Environment Project (CDBR-SSE), Pondicherry University sponsored by National Technical Research Organization (NTRO) New Delhi. He worked there from July 2009 to July 2012. During his tenure in CDBR-SSE project, he has presented ten of his research findings and demonstrated four of his prototypes in the various quarterly SSE workshops conducted by eight SSE nodes.

He has total of six years experience both in industry and academic research. He has published seven papers in International Journals which includes Elsevier and Springer. He has also presented his research findings in four International Conferences and one paper in Doctoral Colloquium conducted by Reserve Bank of India (RBI) research institute, Institute for Development and Research in Banking Technology (IDRBT), Hyderabad. His area of interest includes Information Security, Biometrics and Image Processing.