A Novel Image Steganographic Framework for Efficient Embedding Capacity and Stego Quality

Author

MUHAMMAD ADNAN ASLAM

Regn Number

0000274974

Supervisor

PROF DR. FAROOQUE AZAM

DEPARTMENT OF COMPUTER ENGINEERING
COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING
NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY
ISLAMABAD
July, 2021

A Novel Image Steganographic Framework for Efficient Embedding Capacity and Stego Quality

Author

MUHAMMAD ADNAN ASLAM

Regn Number

0000274974

A thesis submitted in partial fulfillment of the requirements for the degree of

MS Computer Software Engineering

Thesis Supervisor:

PROF. DR. FAROOQUE AZAM

Thesis Supervisor's Signature:____

DEPARTMENT OF COMPUTER ENGINEERING
COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING
NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY,
ISLAMABAD
July, 2021

Declaration

I certify that this research work titled "*A Novel Image Steganographic Framework for Efficient Embedding Capacity and Stego Quality"* is my own work. The work has not been presented elsewhere for assessment. The material that has been used from other sources has been properly acknowledged / referred.

Signature of Student
MUHAMMAD ADNAN ASLAM
2018-NUST-MS-Computer-0000274974

Language Correctness Certificate

This thesis has been read by an English expert and is free of typing, syntax, semantic, grammatical and spelling mistakes. Thesis is also according to the format given by the university.

Signature of Student

Muhammad Adnan Aslam

0000274974

Signature of Supervisor

Copyright Statement

Acknowledgements

I am thankful to my Creator Allah Subhana-Watala to have guided me throughout this work at every step and for every new thought which You setup in my mind to improve it. Indeed, I could have done nothing without Your priceless help and guidance. Whosoever helped me throughout the course of my thesis, whether my parents or any other individual was your will, so indeed none be worthy of praise but You.

I am profusely thankful to my beloved parents who raised me when I was not capable of walking and continued to support me throughout in every department of my life.

I would also like to express special thanks to my supervisor PROF. DR FAROOQUE AZAM for his help throughout my thesis and for SDA course which he has taught me. I can safely say that I haven't learned any other engineering subject in such depth than the ones which he has taught.

I would also like to pay special thanks to SIR WASEEM ANWAR for his tremendous support and cooperation. Each time I got stuck in something, he came up with the solution. Without his help I wouldn't have been able to complete my thesis. I appreciate his patience and guidance throughout the whole thesis.

I would also like to thank DR. WASI HAIDER BUTT (Co-Supervisor), DR. USMAN AKRAM (GEC Member) and DR. ARSLAN SHAUKAT (GEC Member) for being on my thesis guidance and evaluation committee.

Finally, I would like to express my gratitude to all the individuals who have rendered valuable assistance to my study.

Dedicated to my exceptional parents and adored siblings whose tremendous support and cooperation led me to this wonderful accomplishment

Abstract

Internet has emerged a major platform to support many activities in our daily life. However, the countless facilities offered by Internet brings numerous challenges thereof. One of the major challenge is regarding *security and privacy* of data transmitted over internet. *Information security* is an emerging area of research, in which *steganography* is a promising technique to *hide the presence of secret information* into the cover media such as, *image, video, audio files.* Although various steganographic schemes have been designed and proposed by researchers, however, the tradeoff among important steganography parameters, i.e., *embedding capacity* and *Peak Signal to Noise Ratio (PSNR)* remains challenging, because efforts to enhance the *embedding capacity* significantly degrades the *PSNR* and vice versa. Since, both these parameters have an important impact over the steganographic scheme therefore, a compromise on anyone may jeopardize the desired objectives. Hence this research fill-up this gap by proposing a novel steganographic framework that ensures an optimal tradeoff between embedding capacity and PSNR by achieving *higher* embedding capacity with *lower* visual quality distortions (PSNR), while comparing with current state of the art approaches. The proposed scheme uses *Pixel Value Difference (PVD), Least Significant bits (LSB) and Difference Expansion (DE)* techniques simultaneously and hide the secret data in the cover image with due emphasis on achieving *higher embedding capacity*, as well as, *visual quality*. The validity of proposed framework has been demonstrated using benchmark case study by choosing test images from publicly available Signal and Image Processing Institute (SIPI) dataset. The achieved results prove that the proposed scheme, enhances the embedding capacity by *1053858 bits (min) to 1061248 bits (max)* (on average *0.27% to 0.63% more than the reported* so far), while maintaining the visual quality within 32dB (min) - 36dB (max) (*on average 1.69 to 5.21 dB improvement*). Moreover, because of higher PSNR, our proposed scheme is more effective against *histograms* and *statistical attacks* due to improved visual quality of the stego images.

Key Words: *Image Steganography, Least Significant Bit, Systematic Literature Review, LSB, PVD,RDE*

Table of Contents

List of Figures

List of Tables

CHAPTER 1 : INTRODUCTION

The chapter contains four sections. In Section 1.1 provides brief background of Information Security, Section 1.2 discusses about the problem statement, Section 1.3 covers about the Motivation for research work, Section1.4 discusses about the Structure of thesis.

1.1 Background of Information Security

The evolution of speedy internet for long distance communication enabled the information to travel everywhere across the world [49]. This has made the world a global village in true sense. However, at the same time cyber-attacks and leakage of sensitive information have made people and organizations anguish about the secrecy and privacy of data [50]. So, the Information security is the only way that assures that all data or information is secure and not been compromised by Intruders or hackers at any stage. The security of information is further divided into three types [51]: -

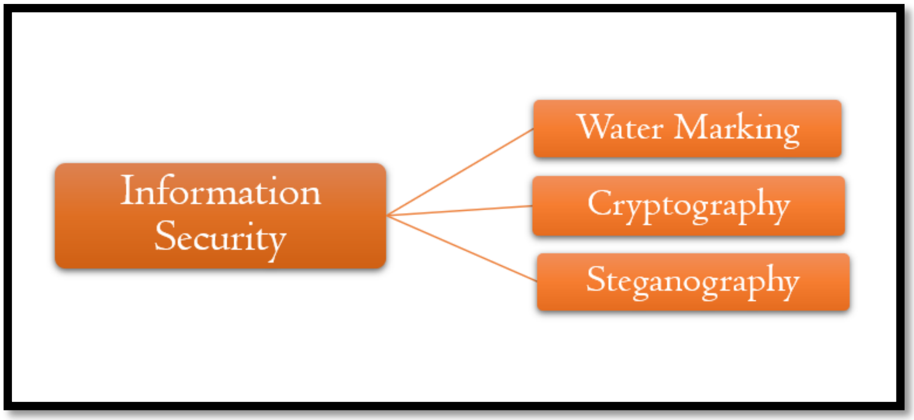


Figure 1- **Types of the Information Security**

Watermarking technique is used to identify the ownership or a copyright of someone and either visible or nonvisible. [52] Watermarking is also called as authentication tool that restricts the unauthorized disclosure and distribution of digital files, either it is a text file / image file or a video / audio file. Watermarking can be done by directly adding visible or non-visible watermark into the data and that watermark become an integral part of that data. Here, it can be considered that the valuable data is secure and not been compromised until the watermark is evident in the digital file. The goal of a watermark is to ensure the safety and the integrity of original data. While Human beings from years onwards would have two fundamental needs (i) one is to communicate and share the information (ii) and secondly is to communicate particularly or specifically. These two objectives explicitly contributed to the art of encoding and decoding of the sensitive information that are achieved by cryptography. [53] cryptography is the art of secret writing in such a way that the data is converted into unreadable format (plaintext to cipher text) by using the key and only the designated recipient can read and revert the unreadable data into readable (cipher text to plaintext). This research is based on third type of information security known as Steganography Technique. [54] Steganography is derived from the Greek words ' Steganos ' mean covered and 'graphei' mean (writing or drawing). It literally means ‘covered writing’. Digital steganography is art and science to hide the data in such a way that the only intended recipient has the knowledge about the existence of message inside the cover media rather than the data is encrypted like Cryptography. While on the other hand steganographic methodologies have been used for a long since ancient times but have been known by this name in the late 15th century. Traces back to around 440 B.C one of the classic historical precedents of Steganography were found. [32] Histiaeus used his most trustworthy slave by shaving the head and make a tattoo on his scalp with a message. Once the hair of slaves had grown, the message was disappeared completely then the salve was sent to receiver with hidden message on their scalp. Salve’s hair was used as a cover media for a message. Even [33] in World War the invisible ink was used to hide the secret data and send to the receiver. Certain liquids like milk, lemon juice is also used to hide the secret data, moreover such as adopting the mechanisms for different types of invisible inks. For secret data hiding purpose, chemical liquids, vapors or heating were applied on the paper mechanisms to maintain the data secrecy before dispatch to intended recipient. In [55] Steganography applied on cover files that are used to hide the secret data. Cover files may be the audio file, video file or an image file. Steganography itself divided to further parts

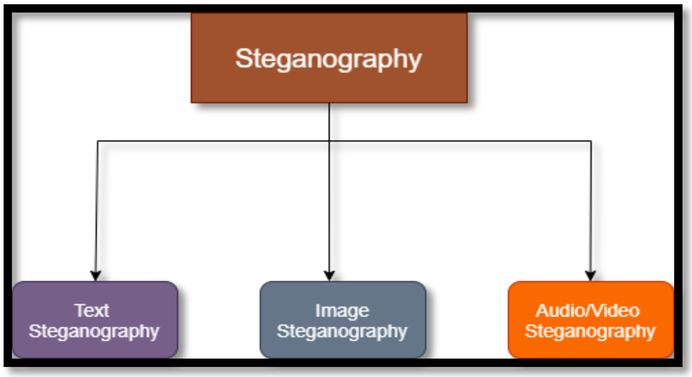


Figure 2-Types of the Steganography

In text steganography text files are used to hide the valuable data. [56] While on the other hand, In Audio/video Steganography secret messages are embedded into digital sound or in a video files, for this purpose mostly messages are incorporated in MP3 sound files and mp4 video files are used and many other formats are also used by many researchers as well. This research is based on Image steganography (IS) technique in which images are used as a cover file to hide the secret data. Various applications of Image Steganography have emerged over the period of time along with the technological evolution [57]. Many organizations are spread across the globe, and they need to communicate frequently by take advantage of the enormous facilities that internet provides, however, mostly, internet users are concerned about their privacy and anonymity. Therefore, Specific methods and algorithms are always more than welcomed by the concerned individuals/ organizations and their respective employees to secure their intellectual properties/ and proprietary assets as well as information sent via internet.

Since image steganography offers variety of approaches/ techniques to hide the information of interest. Thereafter it may serve the purpose of providing sense of security to the internet users by hiding their information of interest. It enables the secret communication of two parties to take place in an undetected manner thus avoiding the malicious attacks [4]. It also offers copyright protection on digital files by utilizing the message as a secret digital watermark. None the less, even top-secret documents can be transmitted, embedded within the images [7]. On the other hand, attackers can also use image steganography to send malware and Trojans to oblivious users. So, we can say that steganography may be misconstrued [34], such as the scenario of the transmission of confidential information by the Internet worms. So, in other word we can say that the Information security itself facing a biggest challenge regarding to several steganalysis type of attacks like statistical attack, visual attack and many other attacks are also involved. Steganalysis is the mechanism to detect the existence of the secret data inside the cover image. Steganalysis can be done by identifying the algorithms that are used to hide the secret data and exploit those algorithms to expose the hidden secret data. Mainly the hackers discriminate or measure the difference between original image that is called cover image and the stego image that is as an output image once the secret data is successfully hide in it by using the steganalysis approach to detect the existence of the secret data because as we know steganography deals with the hiding information by using some cover media and not encrypting the secret data so it can be easily exploit by using steganalysis approaches.

Steganalysis is divided into two main categories mentioned in [44-45] (i) discrete steganalysis method (ii) general steganalysis Method. The first category focuses on a particular image steganography approach and makes an attempt to attack that technique in other word we can say that the discrete method or a specific method only focuses and attack only one steganographic method at a time. But on the other hand, general steganalysis Method that is also called blind steganalysis Method attacks on more than one steganography techniques at a time. [58] Blind method is based upon the features collection from different steganography techniques and after that arrange all the features. Blind method uses the classifier approach to determine the stego image and helps to exploit the existence of the secret data. All steganalysis attacks lies under the umbrella of two attacks one is passive attacks and second one is active attacks. Passive attacks deal to exploit the existence of the secret message in cover file as well as identify which embedding terminologies are adopted to hide the secret data while on the other hand the active attacks determine the properties of the cover file such as the size of the image and the size of the secret message. [46] Visual attacks or statistical attacks are most popular and adopted steganalysis method because they are based on histogram. [47] In LSB (Least Significant Bit) and LSB matching steganography approach the least important bits are replaced with the secret data bits and in result the stego image have similar index to the cover image which means it is extremely hard to determine the difference between the original image and stego image. So, in statistical or visual attack by observing the histogram it become quite easy to detect the existence of the secret message inside the image. There are many steganography based framework was also proposed that prevent the active and passive attacks significantly such as in [48].

There are two diverse types of digital image or a signal processing domain in which digital image steganography is used: (i) Spatial domain steganography (ii) Frequency domain steganography.

- ***Spatial Domain Steganography:*** In this domain the digital image steganography can manipulate directly to the pixels of the cover image by changing or embedding the secret data in it.There are several mechanisms are lie in this domain, but least significant bits (LSB) is most popular spatial domain technique that are mostly adopted by many researchers due to its simplicity and easy to handle mechanism. Contrarily LSB have several vulnerabilities and drawbacks as well and multiple intruders, or hackers have so far discovered multiple loopholes in it. It deals with directly replaces the least important bits (most right-side bits) of the cover image with the secret data bits. By using least significant bit technique the immense amount of sensitive data can be incorporated in cover image but on the other side the visual quality (PSNR) could not be same intact with the original image that also led to greater distortion in the output image and this drawback of visual distortion can be clearly visible by comparing both images histogram. Another spatial domain based digital image steganography technique is LSB based matching that is also a derivative of least significant bit [34-35]. In which adds or subtracts 1 from the least significant bits of the cover image pixel if and only if the value of cover image LSB bits does not match with the secret data bits. In [37] another technique is introduced in which LSB is the integral part along with the new Genetic algorithm terminology. In this study author apply genetic algorithm to improve the visual quality of the image once the secret data is embedded in it that are distorted while applying the LSB technique, but this type of spatial domain research has also a drawback of large computation power. Another Study is conducted in [38] where author improve the significant visual quality of the image by calculating the difference or the error between the cover image and the stego image. In [39] Author uses pair consecutive pixels of the cover image and calculate the difference between them before embedding the secret data in it to determine that the pair pixels are good enough that maintain the visual quality if data embed in it, but this research have drawback of limited amount of data encoding capacity. On the other hand, the computation power is significantly over head in this study. Furthermore, more spatial domain techniques are explained in chapter 2 in detail that are also related to Research.

- ***Frequency Domain Steganography:*** In this type of steganography firstly convert the cover image and the secret data in the form of frequency domain from spatial domain and then secret data is embedded in the frequency domain signal form image. There are multiple ways are available for the conversion or transformation of any image in spatial domain to frequency domain like [40] DCT abbreviation of discrete cosine transformation and called as wavelet transformation. [41] Z transformation is another mechanism was proposed to convert the spatial domain image into the frequency domain.

  In frequency domain steganography many researchers proposed any steganography techniques that can embed secret data in the form of frequency signal by using DCT and other form of frequency domain terminologies like [44] outguess and [43] F5 are most popular techniques. In [43] the main aim of F5 technique is to convert the spatial domain image and secret data into the frequency domain by using the classical discrete Cosine transformation (DCT) method and then incorporate the secret data inside the frequency domain signal form of cover image by using the wavelet transformation coefficient's parameters and if required for the secret data incorporation simply add or subtract the 1 from the available discrete cosine transformation (DCT) coefficient's just like in the spatial domain [34-35] approach to hide the secret data but again the drawback of this approach is less embedding capacity and better visual quality even in frequency domain as well. On the other hand, F5 also prevents and reduces the multiple visual attacks from the hacker or the intruder. Outguess technique is proposed in [44] that is also uses discrete cosine transformation (DCT) coefficients to embed the secret data by using LSB technique. Outguess technique consist of two parts first one is to embed the secret data by using DCT confidents parameter except the 0's and 1's. In second part the histogram of the stego image is going to be adjusted in such a way that it should be similar to the original cover image histogram with some additional information that will helps to retrieve data on extraction process. Both parts working achieved in frequency domain. Outguess also have much better visual quality than [44] due to its histogram adjustment terminology and regarding to the security it is also prevents from visual and statistical attacks as well as chi-square attacks from the hackers.

Several Steganographic strategies are used and adopted by many public and private sector organization for their secrecy and privacy of data. Mostly the ancient technique like least significant bit (LSB) widely adopted and used for hiding the secret data by directly manipulating the pixels values of the cover image and replacing the least important bits with the secret data bits. Moreover, LSB technique is used to achieve high embedding capacity [8]. Difference Expansion (DE) Technique received more attention from few years just like LSB because DE is reversible data hiding approach this will not reverse the data bits but also reverts the original pixel pair values of the cover image.[10]PVD is another type of steganography technique that is based on the consecutive pixels difference to determine the number of bits that can be embedded into the pixel pair instead of embedding a fixed number of confidential data bits directly into the least significant bits of each byte of the cover image. In this research, we are focused towards hiding the maximum amount of secret data into a covered image by integrating the techniques of Pixel Value Difference (PVD), Modified Difference Expansion and Least Significant Bit (LSB). We also intend to improve the PSNR (Quality) of the image after embedding/hiding the secret data in order to make the stego image un-differentiable from the original image. Thus, our proposed approach intends to improve the security of sensitive data transmitted over unsecure medium and makes it much more difficult for the intruders to compromise the security of our sensitive data. Consequently, our proposed approach has two-fold advantages in terms of higher embedding capability and improved PSNR over the existing schemes.

1.2 Problem Statement

Hide the Maximum amount of secret data in cover image in such a way that the similarity index between the Stego image and original image should be significantly same and provide the better security to the secret/sensitive data while transmitting over the unsecure network in such a way that the data should not be compromised by the intruders/hackers.so there is dire need of a framework to hide and secure the secret data. In chapter 3 proposed framework is based on two algorithms vice versa. One is secret data embedding algorithm and second one is data extraction algorithm.

Embedding algorithm is based on hybrid approach including modified pixel value difference, least significant bit and difference expansion techniques that will not only increase the data embedding capacity but also enhance the visual quality of the cover image and stego image. Data embedding algorithm is based on two-bit plane and each plane is used to embed the secret data bits. Starts with converting the secret data into bits and then choose the two consecutive pair pixels from the cover image. After that converting consecutive pair pixels into lower bit plane and upper bit plane. Then each bit plane is used to embed the secret data separately. On Upper bit plane modified PVD is applied and the difference of PVD is further used to incorporate secret data in the form of bits by creating space and encode two more bits by using modified LSB technique Furthermore the difference will be far away from the original one then we need to reduce that one as much as possible to near about the original difference of pair pixels so in order to do this we apply the reduce difference expansion after that we still have space to embed one more secret data bit and again reduce the difference expansion and on the result new stego upper bit plane is received. On the other hand, Lower bit plane pixels are directly replaced with using LSB technique and on the result stego Lower bit plane pixels are generated. After that combining stego upper bit plane and stego lower bit plane to get final stego pair pixels. Contrarily Extraction algorithm is just like the vice versa of embedding algorithm by applying all techniques reversibly on stego pair pixels by converting them into two-bit planes.

1.3 Motivation

The internet now plays a significant role in the development and growth of society, and there are many benefits of using the internet that provide freedom to all. However, the internet is based on the public mean of communication where data is transmitted. Therefore, the secrecy and privacy of the data made worried to many people, organizations and many other government sectors while transmitting over the unsecure network. There are various methodologies for protecting critical amount of data transmitted over the Internet such as cryptography and steganography are used. Many researchers proposed many cryptography and steganography-based techniques to secure the sensitive data but every proposed technique have some benefits and drawbacks. By using least significant bit or a Pixel value difference technique the larger amount of secret data can be embedded in cover image but on the other hand it also causes of the distortion that will reduce the visual quality of the image and this one can be clearly seen by the image histogram. Many of the hybrid approaches also proposed by many researchers as well such as in [19] KH Jung proposed the derivative or a hybrid approach to significantly enhance the embedding capacity instead of using simple one Technique at a time. He proposed combined approach of LSB and PVD, but he compromised on the visual quality parameter and consider only embedding capacity parameter for improvement and secondly by applying the steganalysis active or a passive attack like statistical or visual attack by observing the histogram it become extremely easy to detect the existence of the secret message inside the image. So I inspired to these studies and conducted a latest brief SLR (Systematic Literature Review) Systemic literature review in chapter 2 to get more knowledge regarding to the sensitive data security over the internet and I found that the secrecy and the privacy of the data is still become a big challenge whenever we are going to embed more data inside the image the visual appearance quality get distorted so, there is dire need of solution or a framework that will not only increase the embedding capacity to incorporate the secret data but also enhance the visual quality of the image in such a way that the similarity index between the cover image and the stego image should be near to each other even by analyzing the histogram of the cover image and the stego image should be appear same and discourage the attackers and hackers to easily detect the existence of the secret data. In chapter 3 proposed framework will achieve the highest embedding capacity and the visual quality as well as enhance the secrecy of the data from the intruders and the hackers. This system will definitely help those organizations and the government sector where the sensitive data is concerned.

1.4 Structure of thesis

This structure of the thesis is as follows:

Chapter 2: Cover the Systematic Literature Review (SLR) to address the key questions and the significant work done by researchers in the past few years for Least Significant Bit technique and to conduct critical analysis and finally identifies research gaps.

Chapter 3: Proposes Novel steganography framework and methodology in details. It includes the two main parts: *secret data encoding, secret data decoding*.

Chapter 4: Provides validation of proposed framework by using benchmark case study which contains test images from publicly available Signal and Image Processing Institute (SIPI) dataset and this chapter provides evaluation and comparison with previous studies. All the experimental results are discussed in detail with all desired figures and tables.

Chapter 5: concludes the thesis and reveals the future scope of this research

1.5 Summary

In This Chapter Brief background and introduction of information security have been covered. In addition, discussion about the different types of information Security and their domains along with different classical standalone and hybrid techniques to hide the secret data. Outcomes and the issue were addressed in image steganography while hiding the secret data was discussed in Problem statement. Secrecy and the privacy of data still be the biggest challenge and the biggest area of research upon which multiple researchers are working. So, I got motivation to add my contribution to secure the data to prevent from hackers and intruders. So, in this chapter, described the motivation for conducting research briefly about the preference of steganography over the other methodologies of information security. Brief structure of thesis is depicted in Section 1.4 and complete scope of study is organized and narrated chapter

CHAPTER 2 : LITERATURE REVIEW AND GAP ANALYSIS

In this chapter performs Systematic Literature Review (SLR) and Gap Analysis. The chapter contains seven sections. In Section 2.1 provides Review Protocol about selection of research articles/papers. Section 2.2 discusses about the existing techniques/algorithms. Section 2.3 covers about the dataset used by the researchers. Section 2.4 provides Evaluation Criteria for Improvements. Section 2.5 covers about Tools used in research. Section 2.6 covers the Overview of Studies. In Section 2.7 discuses about Related Techniques.

Several Image Steganography techniques are in vogue [21], amongst which, Least Significant Bit (LSB) [9] is a well know approach. It is used to embed the secret message/ data/ information within a cover image. Two famous sub techniques that can be covered under the umbrella of LSB are (i) Insertion based Method (ii) Substitution based Method [11]. Both are widely adopted and used for hiding data but there are some differences between them. Insertion based method increases the size of the image when secret data is embedded while on other hand the substitution-based method is used to replace the bits of the image with secret data without increasing the size of the image [25]. The past decade has seen rich contribution to the domain of image steganography by the researchers due to its obvious significance. In this regard, various steganography techniques are comparatively analyzed in a survey presented by the authors of [21]. However, the limitations of such surveys are that they do not encompass latest advancement in this domain. Moreover, another important aspect that need to be highlighted is that the LSB based image steganography approaches are particularly hard to find in literature. Therefore, there is a dire need that the latest LSB based Image steganography approaches may be explored and summarized. This would help in the identification of the targeted image steganography regions where contemporary LSB techniques have been used till now. Furthermore, this will also facilitate the researchers to select the right LSB approach for a particular image steganography requirement. Consequently, in this study a Systematic Literature Review (SLR) is carry out [22] to answer the following research questions:

RQ1: What are the latest and important research studies where LSB is utilized for image steganography during 2016-2020?

RQ2: What are the most popular methodologies and approaches for LSB-based image steganography that researchers have proposed or provided?

RQ3: What are the leading and publicly available datasets for LSB based image steganography?

RQ4: What are the crucial evaluation parameters for the quality assessment of image steganography?

RQ5: What are the existing implementation frameworks / tools for LSB based image steganography?

RQ6: What are the fundamental advantages and limitations of utilizing LSB for image steganography?

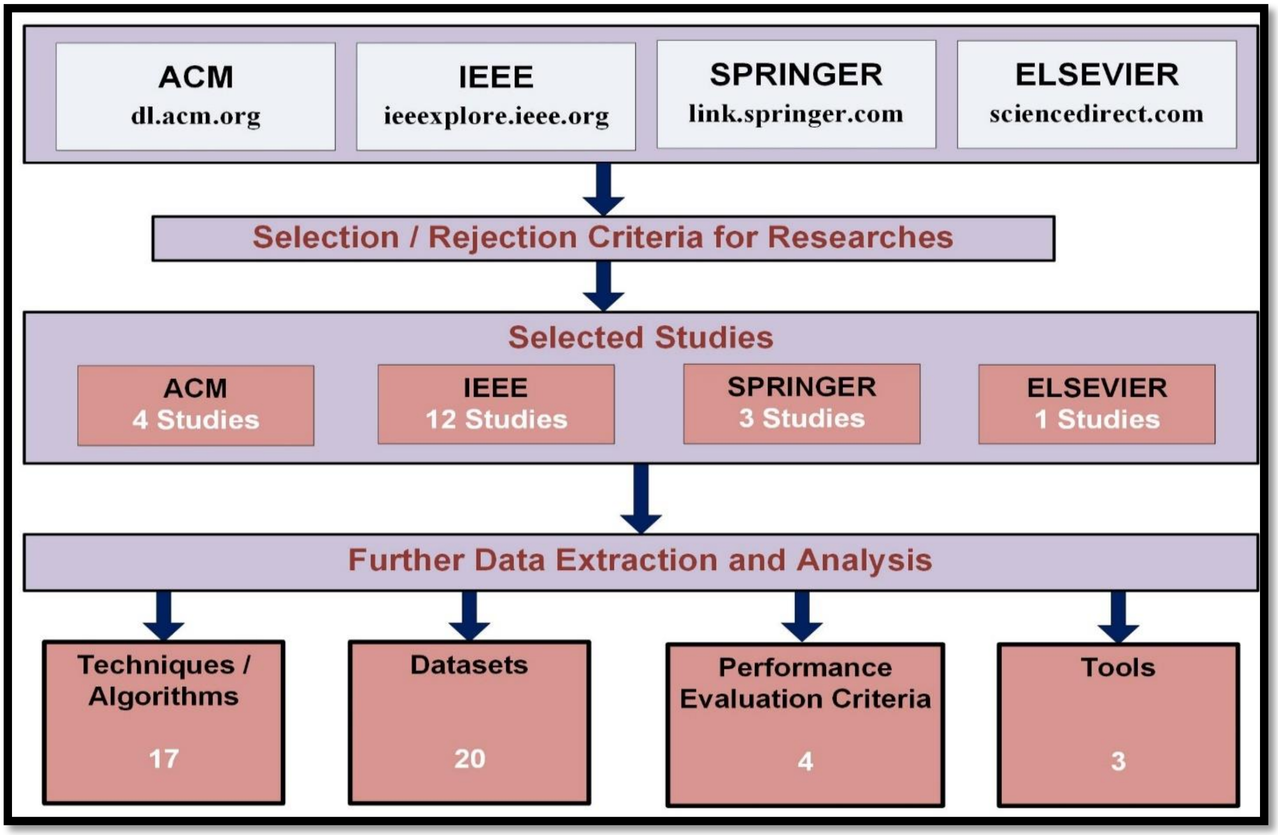


Figure 3: Research Study – An Overview

In order to conduct this study, four of the very renowned archives (i.e. Elsevier, ACM, IEEE, and Springer) have been explored. Developing the review protocol (Section 2) including Selection Rules (Section 2.2), consequently, helped us identify 20 studies in order to achieve the sole purpose of this SLR as shown in Figure 1. The results are presented in Section **3**. Answers to formulated RQs along with the discussion is presented in Section 4. Finally, section 5 presents the concluding remarks.

2.1 Review Protocol

In this section, the Review Protocol details are summarized. The details are summarized in subsequent sections as: -

2.1.1 Selection Rules

Rules have been defined in order to select the research articles. On one hand these rules endeavor to find the answer of the RQ's (Section 1) and on the other hand a high-quality outcome is enforced. The rules are

1. Only those research studies may be selected where LSB Based Image Steganography approach has been explored.
2. Only those researches are selected if the research has been published in any of the well-known scientific archives of ACM, Springer, Elsevier and IEEE.
3. Only those research studies are considered that are published with in the time duration 2016-2020.
4. A research study may be selected only if all of the above-mentioned rules are followed, the violation of a single rule will cause refusal of the study e.g., a study following the first two rules but published before 2016 should be rejected.

2.1.2 Search process

The search process is here in after performed on the basis of clearly outlined selection rules. Only four famous and well known archives as provided in the second selection rule (Section **2.1.1**) have been searched. To impose the third selection rule, a year filter (i.e. 2016-2020) was applied during the search process. We also used a combination of different search terms to get the best search results. The results are summarized in **Table 1**.

Table 1: Search Results - Summary

Sr.#	**Search Queries**	**Search Results**			
		ACM	**IEEE**	**Springer**	**Elsevier**
1	Image steganography	467	250	345	112
2	LSB steganography	256	348	170	212
3	Steganography Data Protection	650	450	256	354

4	Multilevel data hiding	267	265	338	198
5	Adaptive reversible images	179	188	218	218
6	Steganography Enhancement	80	192	103	201

Table 1 also depicts the different search queries that are used to get the corresponding results from each of the repository. The relatively larger search queries (e.g., Steganography Data Protection) enumerate a very large number of search outcomes which could not be fully assessed in case of first selection rules. Consequently, using diverse techniques such as journal selection (Springer) to narrow down the search results, served the purpose. To evaluate the first selection rule, we perform certain steps as shown in **Figure 2**.

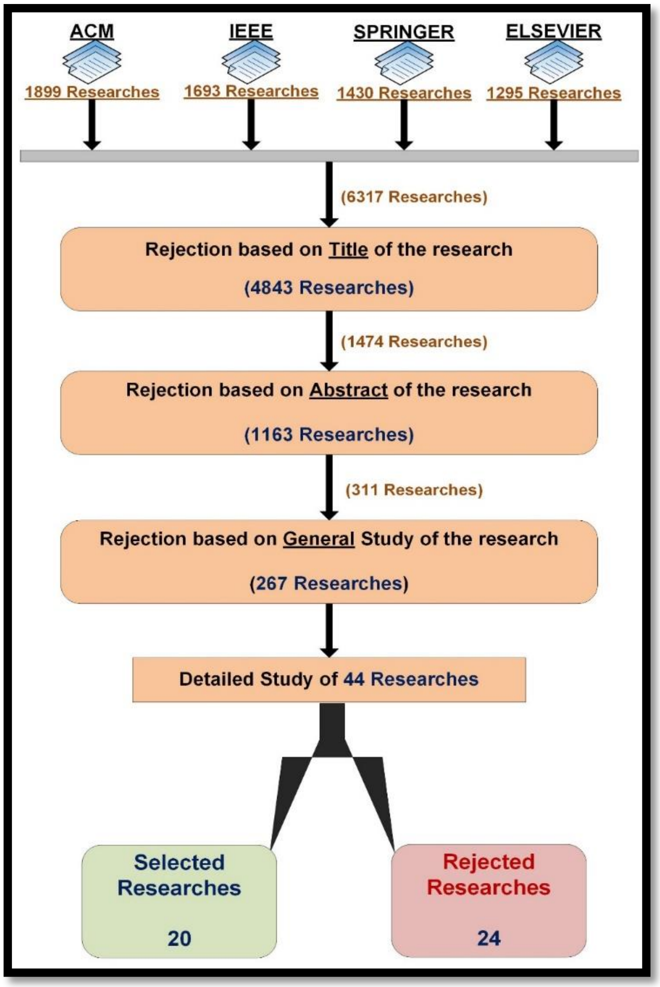


Figure 4: Steps for Selection of Research Studies

We overall considered 6317 search results to evaluate first selection rule. However, 4843 search results were rejected on the basis of irrelevant study title. Furthermore, 1163 abstract based rejections were made due to clear violation of first selection rule. Subsequently, 267 studies are rejected by reading various sections. Finally, we thoroughly investigated 44 studies and selected 20 studies which are completely satisfying all three selection rules (Section **2.1.1**).

2.1.3 Quality Assessment

We have chosen the prestigious scientific frameworks that consistently publish high-quality research studies. As a result, the high quality of this study's outcomes has been ensured, and the obtained results are regarded as reliable. The distribution of selected studies is given in **Table 2.**

Table 2: Selected Researches with Reference to Databases

Sr. #	Databases		References	Total
1	IEEE	Conference	[1][2][3][4][5][6][7][8][9][10][15][17]	12
		Journal	NIL	0
2	Springer	Conference	NIL	0
		Journal	[18][19][20]	3
3	ACM	Conference	[11][12][13][14]	4
		Journal	NIL	0
4	Elsevier	Conference	[16]	1
		Journal	NIL	0
Total				20

An endeavor has been made to include the latest studies. The year-by-year distribution of selected studies is provided in given **Table 3**.

Table 3: Selected researches as per publication Year

Sr.#	Year	References	Total
1	2016	[3][5][8][10][15][16]	6
2	2017	[2][7][12][13][17][19]	6
3	2018	[1][4][14][18]	4
4	2019	[6][11]	2

5	2020	[9][20]	2

2.1.4 Data Extraction

In order to extract and analyze the information of interest from the selected research studies, various data extraction/ synthesis parameters have been defined so that answers to the RQs may be provided. **Table 4** shows the relevant details.

Table 4: Parameters – Data Extractions and Synthesis

SR. #	Parameter	Specifics
1	Common information	Name of Author, study title, publisher details, publication year
Data Extraction		
2	Summary of study	Purpose of Study, Significance and Findings, impact
3	Limitations	Assumptions (if any)
4	Proof-of-concept	Evaluation via experimentation or other proof-of-concept methods
Synthesis of data		
5	Techniques and algorithms	Techniques and algorithms for image steganography in selected studies (**Table 5**)
6	Datasets	Data sets used in selected studies (**Table 6**)
7	Evaluation Parameters	Parameters used to evaluate the quality in selected studies (**Table 7**)
8	Leading Tools	Tools used for the implementation of image steganography techniques in selected studies

2.2 Results

This section summarizes the outcomes of this SLR in order to obtain the answers of RQ’s. The details are provided in subsequent sections.

2.2.1 Techniques / Algorithms

We have selected 20 LSB based image steganography studies which are published during the period 2016-2020. Since, the isolated application of LSB is not feasible to achieve desired results. Therefore, LSB is frequently applied with other techniques / algorithms. The utilization of LSB with another techniques / algorithm is summarized in Table 5. Particularly, first column of Table 5 provides the reference of selected study. The second column (Substitution LSB Replacement) evaluates the number of bits used in each selected study. Finally, additional techniques / algorithms utilized along with LSB are given in third column of Table 5.

Table 5: Image steganography techniques in selected studies

Ref	Substitution LSB Replacement				Additional Techniques / Algorithm
	One Bit	Two Bits	Three Bits	Four Bits	
[1]	✓				RSA* Encryption algorithm
[2]	✓				SHA-1* hash Algorithm
[3]	✓				AES* + Wavelet Transform +Neural Network
[4]	✓				N/A
[5]		✓	✓		Specific Coordinates Cropping
[6]		✓			LZW* Algorithm
[7]			✓		Character Bit Shuffler
[8]			✓		AES* 256 bit Encryption
[9]				✓	Local Entropy Filter
[10]	✓				RSA*Encryption algorithm
[11]	✓				Hashing Encryption algorithm
[12]		✓	✓		N/A
[13]	✓	✓			Contrast Compression
[14]	✓		✓		Skewness and kurtosis
[15]	✓	✓	✓	✓	Improved LSB with directional algorithm

[16]	✓				Random Pixel Key
[17]	✓				OTP* Algorithm + Canny Algorithm
[18]		✓	✓		CRC-32*+ GZIP* + AES* Encryption
[19]		✓			Pixel Value Difference
[20]	✓	✓			SIPHT Compression algorithm +DWT* +SVD*

RSA* = Rivest–Shamir–Adleman

AES* = Advanced Encryption Standard

OTP* = One Time Pads

GZIP* = GNU Zip

SVD* = Singular Vector Decomposition

SHA-1*=Secure Hash Algorithm

LZW*= Lempel–Ziv–Welch

CRC-32*=Cyclic Redundancy Check

DWT*=Discrete Wavelet Transform

It may be noticed in **Table 5** that LSB one bit approach is most commonly utilized (thirteen research studies). Furthermore, researchers simultaneously utilized multiple bits LSB approaches e.g., in [15], all four bits LSB approaches have been simultaneously utilized. It can also be analyzed from Table 5 that AES and RSA are leading techniques / algorithms which are used along with LSB to achieve certain image steganography objectives. In two studies, [4] [12], only LSB is utilized without employing any additional technique / algorithm.

2.2.2 Datasets

Datasets have immense importance while performing particular steganography operations. Therefore, we have identified and analyzed twenty datasets as given in Table 6. Particularly, first column of Table 6 provides reference of selected study. The name of dataset is given in second column (Dataset Name). The evaluation of datasets based on certain characteristics is performed in third column (Characteristics). Particularly, third column is further sub-divided into five columns to evaluate distinctive characteristics: 1) *Cover File Type* defines the type of dataset images like grayscale, RGB etc. 2) *Cover File Size* defines size of images in dataset like 521x512 etc. 3) *Cover File Resolution* defines resolution of dataset in terms of size e.g., 8 bits etc. 4) *Secret Data Type* defines type of secret data (e.g., image, text etc.) that need to be hide through LSB. 5) *Secret Data Size* defines size of secret data e.g., bytes / kilobytes etc. Finally, in last column

(Availability), the accessibility of dataset is evaluated i.e., private, or publicly available. The results are summarized in Table 6.

Table 6: Datasets used in the selected studies

Ref.	**Dataset Name**	**Characteristics**						**Availability**
		Cover File Type	**Cover File Size in pixels**	**Cover File Resolution**	**Secret Data Type**	**Secret Data Size**		
[1]	Medical Images	Grayscale images	512x512 & 320 x 320	8 bit	Image	19k		Public
[2]	Medical Images	Grayscale images	512 x512	8 bit	Image	N/A		Private
[3]	Generic Images	RGB images	108KB	N/A	Image	19KB		Public
[4]	Paralyzed images of a hand gesture	RGB images	800x600 to 4000x3000	N/A	Text	175KB to 4.26 MB		Public
[5]	Child images	RGB images	512 x 512	96 x96 dpi	Text	N/A		Public
[6]	Student Information	RGB images	N/A	24 bit	Text	N/A		Public
[7]	Aerials Dataset	RGB images	100x100	N/A	N/A	1857 Bytes		Private
[8]	Random Dataset	RGB images	N/A	8 bit	N/A	N/A		Public
[9]	Aerial dataset	RGB images	512x512	N/A	Image	512x512 & 256x256 pixels		Public

[10]	Anime Images	RGB images	256x256	N/A	Image	90x90 pixels	Public
[11]	Aerial Dataset	RGB images	402 x 566	N/A	Text	N/A	Public
[12]	Window 10 Wallpapers	RGB images	1920x1200	24 bit	Text	N/A	Public
[13]	10 Generic Images	RGB images	N/A	N/A	Text	N/A	Public
[14]	632 natural images from INRIA Holidays dataset	RGB images	600 x 450	180 pixels/inch	Text	270,000 bits	Public
[15]	Aerial dataset	RGB images	360 x 360	N/A	Text	N/A	Public
[16]	Aerial dataset	Grayscale images	512 x 512	8 bit	Image	128 x 128 pixels	Public
[17]	Opera dataset	Grayscale images	512 x 512	8 bit	Text	8 bytes To 1024bytes	Private
[18]	Baboon and Lena Images	RGB images	512 x 512	24 bit	Text	1KBS To 256KBS	Public
[19]	USC-SIPI Image Database	Grayscale images	512 x 512	8 bit	Text	13116 To 13259 bytes	Public
[20]	USC-SIPI Image Database	RGB images	256 x 256 & 512 x 512	N/A	Image	256 x 256 & 512 x 512 pixels	Public

It may be noticed from **Table 6** that 12 research studies deal with textual or numerical secret data for steganography while 6 studies employed images as a secret data. There are two studies [7-8] that do not provide the details of secret data. It is important to note that there are 17 datasets [1] [3-6] [8-16] [18-20] which are publicly available, so that, researchers and practitioners may utilize them for experimentation. On the other hand, only 3 studies [2][7][17] utilize private datasets for experimentation.

2.2.3 Evaluation Criteria for Improvements

Once image steganography is performed through particular approach, the evaluation for the assessment of improvements is performed. In this regard, several parameters like embedding capacity, quality of original picture after steganography (Stego) etc. are utilized. There are four major parameters to evaluate the steganography quality which are:

1. **PSNR** (Peak Signal-to-Noise Ratio) is an expression to measure the maximum amount of distortion in the stego image after embedding the secret data in the cover image. Particularly, PSNR measures the similarity index between the cover image and the Stego Image. Higher PSNR means lower noise in the Stego image, consequently, the quality of stego image would be almost similar to the cover image.
2. **MSE** (Mean Square Error) represents the cumulative squared error between the stego image and the cover image. The lower the value of MSE, the lower the error.
3. **CPU Consumption** is related to the resources of machines that are utilized during the encoding and / or decoding of secret data. CPU Consumption is directly proportional to the efficiency of the proposed technique / algorithm.
4. **Embedding Capacity** is related to the maximum capacity available to hide the secret data into the cover image. Larger the embedding capacity, greater would be the amount of secret data hidden in the cover image.

In **Table 7**, aforementioned parameters are investigated while performing the evaluation of proposed technique in selected studies. It is analyzed that PSNR is frequently used to evaluate the performance of proposed approach in selected studies because it is a major requirement to keep the stego image same to cover/ original image. MSE is another important criterion as it deals with the encoding / decoding errors of secret data. Embedding capacity is only effective, if PSNR and MSE are also reasonable.

Table 7: Parameters used for the evaluation of improvements / enhancements

Sr. #	Evaluation Parameters	References
1	PSNR alone	[4][9]
2	PSNR and MSE	[1][2][3][6][7][8][10][12][13][14][15][16][17][18][19][20]
3	PSNR, MSE and CPU consumption	[5]
4	Embedding Capacity	[11]

2.2.4 Tools

It is analyzed from the investigation of selected studies that image steganography is mostly performed through Matlab platform [1-4] [4-19] [21-22]. Particularly, 18 of the selected studies have utilized matlab where different components like Image Processing Toolbox, Simulink, and Neural Network Toolbox etc. are exploited to achieve particular image steganography goals. Whereas only two studies [7][18] have been identified for utilizing other platform and languages. For example, authors in [18] have used Dot Net Framework and C# language for implementation. In [7], authors have used FPGA (field programmable gate array) hardware board and Java Language. It can be safely concluded that Matlab platform is highly supportive for image steganography through LSB approach.

It is important to highlight that Matlab platform is frequently utilized for implementation purposes. However, image steganography may involve other operations e.g., improving security of secret data before actual steganography. For such operations, researchers also employed other framework / tools. For example, few studies utilize Python Stepic and ezPyCrypto libraries [11] in order to perform cryptographic techniques on secret data. Similarly, other libraries / toolkits like OpenCV [59], boofCV [60], Deeplearning4j [7], AlgART [61] etc. can be employed through JAVA Language to perform desired operations.

2.2.5 Overview of Studies

This section briefly summarizes the selected studies. Arslan et al. [1] proposed LSB technique for image steganography where the canny algorithm for Edge Detection is applied on cover image. Subsequently, the secret message is compressed by applying the swapped Huffman coding lossless compression technique. Finally, the compressed secret data bits are replaced with edges pixels bits of the cover images using classical LSB bits technique. In another study [2], secret data (medical image) is hidden in general cover image. Particularly, the separation of ROI and NROI for secret data is performed. Subsequently, SHA-1 algorithm is utilized to compute the hash of ROI. Finally, ROI is embedded in NROI using even odd incremental embedding algorithm. In another study, Seethalakshmi et al. [3] utilized AES encryption algorithm to encrypt the secret data and then convert the cover image into blocks of 16x16. Subsequently, IWT is applied on cover image to determine the pixel's location for steganography using neural network. Finally, classic LSB algorithm is used to replace the LSB bits of pixels with the secrete data bits.

Eakbodin Gedkhaw et al. [4] considered the different size of covered images with different dimension like 1200*2000 and 5000*12000 and embedded the secret data using substitution based LSB technique. In another study, Khalid et al. [5] cropped image to specific coordinates and replaced the secret data bits with substitution LSB for hiding the students' information's in student images. Yıldıray et al. [6] utilized LZW (Lempel–Ziv–Welch) algorithm to compress the secret message. Subsequently, LSB bits of RGB image are replaced with compressed data through LSB. In another study [7], authors first encrypted the secret data using character bit shuffler algorithm. Subsequently, FPGA is employed to replace the image bits with data bits of secret data and covered image after converting in MIF format. In [8], authors propose a scheme to encrypt the secret data using AES (Advanced Encryption Standard) algorithm and then convert data into byte array. Finally, this array is embedded into image using classic Substitution LSB Method.

Omar et al. [9] proposed K-LSB based data hiding scheme where last four bits are used to embed the secret image in cover image. To enhance the quality of cover image, quality enhancement algorithm i.e., 'relative global histogram stretching' (RGHS) is also utilized. Finally, local entropy filter is applied in order to extract the secret image from cover image. In another study [10], authors employ RSA (Rivest–Shamir–Adleman) to determine the embedding position of secret image through public and private keys. Finally, LSB technique is applied to perform desired steganography operations. Muyco et al. [11] performed encryption and decryption operations on image through modified hashing and then performed enhanced LSB technique for improved steganography.

G.G Rajput et al. [12] proposed LSB technique where RGB windows wallpaper images are used to hide secret data. The cover images are rotated to 90 degree and then replaced the secret message binary bits to the color red, green, blue bits intensity. Similarly, authors in [13] use contrast compression technique to compress the cover image by calculating new lower maximum colour values of each three channels red, green, blue of RGB coloured image. Subsequently, the secret message is embedded to compressed covered image and after embedding again convert compress image to its original quality. In another study [14], author proposed an interactive scheme to select an appropriate suitable cover image to hide the secret data using secure LSB technique. Initially, the suitability of cover image is checked through skewness and kurtosis of the image. Finally, LSB is applied. Sherin Sugathan et al. [15] hides the secret data in cover image with directional approach. Particularly, LSB approach based on directional bit is proposed for data hiding.

Rupali Bhardwaj et al. [16] proposed an inverted bits substitution LSB technique where random pixel's location is determined using secret key. Subsequently, four-bit LSB approach is applied for effective steganography. In another study [17], author employ canny algorithm to perform edge detection process of cover image. Subsequently, OTP random key for cover image is generated and conversion of data in binary format is performed. Finally, the replacement of 8th bit with the secret data bits is performed using Classical LSB Substitution technique. In [18], authors proposed a new LSB based technique where conversion of secret data into byte array is performed and then compute checksum using crc-32 Finally, LSB is applied to embed the data inside the stego image. In [19], authors propose a data hiding scheme for improving embedding capacity using mixed PVD and LSB by dividing image into two-bit plane. LSB substitution is considered in lower bit planes and PVD in higher bit planes. In [20], authors propose a scheme to hide data efficiently using LSB technique where SIPHT compression technique is used to compress secret data. Subsequently, the compressed data is converted into the bits to embed the secret data in cover image to generate the stego image.

Systematic Literature Review is conducted to explore the latest researchers in the domain of image steganography that are implementing the new effective approach in which the most adaptive LSB based data hiding approach is an integral part of each study. Hence the results of this SLR have been summarized in section 3, whereas this section provides answers to each research question as under: -

RQ1: What are the latest and important research studies where LSB is utilized for image steganography during 2016-2020?

Answer: 20 research studies have been identified where LSB is utilized for image steganography. The classification of studies based on scientific repositories is given in **Table 2**. Furthermore, the year-based categorization of selected studies is presented in **Table 3**.

RQ2: What are the most popular techniques and methods recommended / offered by researchers for LSB-based image steganography?

Answer: In this SLR, we have only selected those studies where LSB based approach for image steganography has been explored. Therefore, LSB is an integral part of each study. However, it has also been revealed during the course of SLR that researchers have also utilized additional techniques and algorithms along with LSB to achieve particular image steganography objective. In this regard, 17 techniques / algorithm, as identified, have been presented in **Table 5**. Furthermore, analysis of the specific type of LSB approach (i.e., 1-bit, 2-bit, 3-bit and 4- bit) has also been given in **Table 5**.

RQ3: What are the leading and publicly available datasets for LSB based image steganography?

Answer: We identified 20 datasets, where 17 datasets are publicly available and remaining 3 are private. The datasets are thoroughly analyzed through important characteristics. The details are given in Section 3.2 (**Table 6**).

RQ4: What are the crucial evaluation parameters for the quality assessment of image steganography?

Answer: We identified four most important and frequently utilized parameters (i.e., PSNR, MSE, CPU (Central Processing Unit) consumption and embedding capacity) for quality assessment of image steganography. The details are given in Section 3.3 (**Table 7**).

RQ5: What are the existing implementation frameworks / tools for LSB based image steganography?

Answer: We identify 3 main frameworks / tools / languages to implement LSB for image steganography. The most frequently utilized framework / tool is Matlab followed by Java language and Python. The details are available in Section **3.4**.

RQ6: What are the key advantages and restrictions of utilizing LSB for image steganography?

Answer: We identify that LSB is mostly adopted by many researchers because of its simplicity and effective results for hiding the secret data but on the other hand we identify some limitations as well in LSB that is fixed number of secret data insertion up to four bits. The details have also been given in **Table 5**.

2.3 Related Techniques

In this SLR, we identified only those research papers in which the LSB-based technique is used in image steganography has been explored. Some of the studies are identified that shows tremendous results regarding to hiding the secret data in the form of bits like in [19] KH Jung uses PVD technique and in [28] Tians Proposed Difference Expansion technique but LSB technique is the integrals part of these studies. Basic working principles of PVD, LSB, Difference expansion is explained in this section**.**

2.3.1 PVD Method

The first classical pixel value difference (PVD) technique was suggested by Wu & Tasi in order to hide the secret message in 256 x 256 pixels grayscale images [23]. Instead of entering a limited number of secret pieces directly on the less important parts of each pixel of the cover image, Strength of the PVD is difference between the pixels which means PVD uses the difference of each and every consecutive pair pixel to determine the number of bits that can be embedded. PVD depends on the fact that the human eye can see a slight change in the gray area of the smooth surface but cannot easily detect the change in the edges/peripheral areas. Therefore, PVD divides the cover image into blocks by scanning the cover image from the top left corner in a zigzag pattern. Each block has two non-overlapping consecutive pixels in a cover image. The difference in the two-pixel blocks is used to separate the smooth and contrasting elements of the cover image. The pixels around the edge will have an enormous difference and the pixels in the smooth area will have a slight difference. If the difference is large, more bits can be added to this block.

Wu and Tasi divided the gray scale range are (0, 255) into smaller pixels range. To simplify binary data embedding, each range of the pixels should have 2 strengths. The narrow width represents the smooth surfaces, and the wide width represents the edges. Wu and Tasi uses two different sets of pixels range table for experimenting and hiding the secret data in their paper, one is {8, 8, 16, 32, 64,128} and second one is {2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64}. Both range tables are separated and divided by two bounds one is upper bound represented as *ui* and second one is the lower bound that is represented as *li*, respectively. Both ranges are used to calculate how many numbers of bits of secret data can be embed in pair of two consecutive pixels that is calculated by using this rule $n_i = log2\ (u_i - l_i + 1)$, for range *i* . Assume the consecutive pair pixels are denoted as $(P_i\ , P_{i+1}\ )$ and the new calculated stego pixels are denoted as $(P'_i\ , P'_{i+1}\ )$ After that n_i in the form of decimal value is added in lower bound to obtain new difference and denoted as $\mathbf{d'_m}$ by applying rule

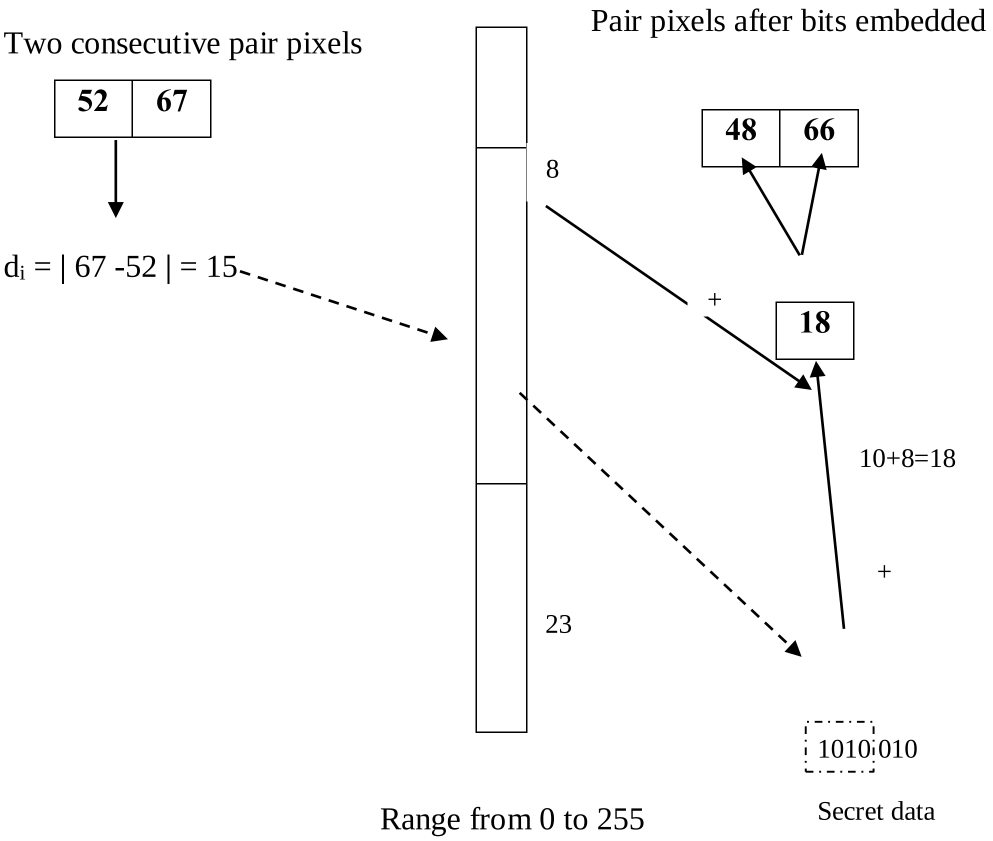
$$\mathbf{d'_m} = \boldsymbol{l_i} + \boldsymbol{b_i^m}$$

$$(P'_i\ , P'_{i+1}\ ) \quad = (P_i - \text{ceil}(m/2)),\ P_{i+1} + \text{floor}(m/2))\ \text{for}\ (d'_m \bmod 2 =1)$$

$$(P'_i\ , P'_{i+1}\ ) \quad = (P_i - \text{floor}(m/2)),\ P_{i+1} + \text{ceil}(m/2))\ \text{for}\ (d'_m \bmod 2 =0)$$

Where $m=|\ d'_m - d_m\,|$.

New pixel $(P'_i\ , P'_{i+1}\ )$ values may fall out of range (0, 255), which is invalid gray level value. That is why secret information will not be embedded in these pixels. Wu & Tasi was suggested a process to cross the line to get these pixels and skip.



Moreover, the pixel value method is not overly sensitive to it precise histogram analysis as compared to LSB. However, by drawing a file for histogram of difference in pixel pairs, variations before and after embedding can be clearly seen. The histogram of the pixel contrast difference has a smooth state of Normal distribution and there are amazing steps for stego image. This is because of quantities of quantization of the PVD method. When the contrast varies accordingly broadly, the calculation of the new difference will start from the same lower boundary of that distance. In general, the number of pixel variation events decreases by an increase in the total number of differences.

2.3.2 PVD and LSB Method

Since the PVD method does not use a smooth surface to hide a enormous number of confidential data, its data embedding capacity is relatively also very low.so in [23] Wu and Tsai achieve the better results by the combination of PVD along with the integration of LSB instead of using single technique to hide the secret data inside the cover image. Mainly the algorithm is based on classic PVD method to hide the secret data on edges of the image where the difference between the pair pixels of the images is used if and only if the difference between pair pixels is larger and on smaller difference between the pixels are utilized by using LSB to embed the secret data on maximum three more secret data bits by applying some adjustments in the equation. They use a fixed threshold value in order to be determining the areas for data embed by comparing the calculated difference between the pair pixels of the image with the threshold that has fixed value. This is also called as a secret key.

While performing the embedding procedure the difference of pixels is denoted as di and the threshold is denoted a t1. If the threshold t1 is greater than the di then LSB technique is used to hide the secret data by embedding maximum up to 3 secret data bits. And if the t1 is less than the di then its mean PVD is used to embed the secret data that is based on the difference between the pair pixels to embed the maximum up to 3 secret data bits. On Both cases new pair pixels need to be calculated that is based on new difference.

2.3.3 Difference Expansion Method

Reversible data hiding is called as lossless data hiding approach because secret data is surely retrieved back by this approach. From a data perspective, data is flexible embedding hides certain details in the digital image in how the authorized group can determine confidential information and restore the image to its original, pure form. The flexibility of the flexible data embedding algorithm can be measured by the data embedding capacity, second one is the algorithm or technique complexity and third one is the visual perceptive of the image that is measured by PSNR that is also referred as visual quality. Reversible data hiding as a single aspect of digital watermarking, embed authentication code to digital imagery in an unobtrusive way, which can be widely used to protect the protection of special digital images, such as digital medical illustrations, original works of art and military geo strategies, and so on. These types of data excluded even if the change is ridiculously small. Increasing power, retaining power feature and decreases simultaneously the destruction of the original image is technological Challenges of embedded data embedding problem. In [28] tians calculate the difference in neighboring pixel values, to select numbers for extended variations for differences (DE). Real details of content recovery, message authentication code, and additional data (any data, such as date / time details, future data, etc.) It’s all embedded in the difference numbers. In their studies they only used dataset of grayscale images. With color illustrations, there are several options. One can decorate the leaning in between distinct color components [30] with variable color change transform and then re-embed data in decorative parts. Or one can re-attach it individually part of the color individually. Tians has introduced the DE process, so you get extra storage space by checking for unwanted image content. They are using the DE process to reversibly get back the embedded secret data information to digital images. Both secret data embedding capacity as well as the spatial resolution of operated DE images is much better, and the complexity level of the algorithm is also moderate and not easily detectable. Tians uses the average of the two neighbor consecutive pair pixels denoted as (P_i , P_{i+1}) by apply l= floor $((P_i , P_{i+1})/2$. And then find the difference between the pair pixels $h=| P_i - P_{i+1} |$. Tians uses h that is difference to hide the secret data bit and denoted new difference is h' by h'= 2 * h + bit. Finally, they calculated the new pair pixels that is based on the new difference h' by using the average l by $(P_i^{'}, P'_{i+1}) = l+$ floor(h'+1)/2 , l – floor(h')/2.

Moreover, the destruction of the image is due to the larger difference made while embedding the secret data bit which cause the triple expansion of the pixels once the secret data is embedded. So, tire need of mechanism to reduce the difference expansion value. Reduced difference expansion (RDE) is the improved scheme of difference expansion (DE) technique.

As in SLR results and in section 2.7 shows that some existing research studies that are conducted have significantly better hiding capacity but lower the visual quality of the stego images and some of studies have less amount of secret data hiding just like difference expansion technique this is because the data hiding, and the visual quality of the images are diametrically relatively metrics. Each technique and terminologies have advantages as well as some disadvantages and drawbacks such as classic LSB technique embed maximum to 3 bits in one pixel of the image and secondly the visual quality of the image is also compromised on the other hand PVD is based upon the difference value. While by using PVD+LSB technique as Wu et al in [23] and KH Jung in [19] are implemented and we know that two consecutive pair pixels of an image are embedded by simple 3-bit LSB substitution method if and only if the difference value between the pair pixels are at lower level and let suppose our threshold is 15 then almost 90% of the pair pixels difference are at lower level which means LSB is used for hiding data as compare to PVD so that will automatically leads toward the poor visual quality of the stego image and anyone can easily detect that something is going on in the image.

Most of the researchers Focused on PSNR and Embedding capacity Parameters in their researches but they are not focusing both of them at the same time because PSNR is inversely proportional to the Embedding capacity which means if we embed as much as data inside the cover image then the quality of the image goes down .so if transmit that low PSNR image over the unsecure network any intruder/hacker can detect it and try to decode it and there is a chance of data compromise if not consider both parameters at same time.so there is a dire need of such solution in the form of framework is required that overcome the loopholes or short comes the existing approaches in term of specially the two parameters that are embedding capacity and that can sustain the appearance and visual quality of the stego image that's why in this research work, the adaptive framework is proposed that are mainly focused on both parameters PSNR and Embedding capacity in such a way that to achieve the maximum embedding capacity to hide the secret data into the cover image as well as with least amount of image distortion that can sustain the visual quality of the stego image. The main research objectives and contribution of the proposed scheme that need to achieve in this research is summarized by using the following bullet points:

- Develop a Framework that preserves the security/ secrecy of the sensitive data.
- To achieve higher data embedding capacity.
- To achieve higher PSNR in order to keep the quality of the image intact.
- Develop a deployable application for hiding the information into an image

2.4 Summary

In this chapter Systematic Literature Review (SLR) and Gap Analysis was performed. The chapter cover and describe the Review Protocol about selection of research articles/papers and the four of the very renowned repositories was discovered as well. After that all research papers were selected for further process of SLR. Whereas in this chapter the techniques and algorithms which are discussed briefly along with the dataset that was used by the researchers mentioned in Section 2.3 of this chapter. In Section 2.4 all the steganography parameters are analyzed and mentioned that was used for Evaluation purpose by the researchers. The tools and terminologies were also discovered for research purposes and same is described briefly in Section 2.5. After that brief Overview of Studies was done in Section 2.6 to get better understanding. In Section 2.7 Some standalone and hybrid techniques was discussed that shows tremendous results in previous studies.

CHAPTER 3 : PROPOSED FRAMEWORK

In this Chapter, a new hybrid LSB, PVD and DE based reversible data concealing Framework is proposed. The Chapter contains two important sections. In Section 3.1 discusses about the data embedding scheme, While in Section 3.2 covers about data extraction Scheme.

3.1 Data Embedding Scheme

A lot of researchers have done work in different techniques of Steganography and proposed the valuable schemes but most of them is based on single bit plane. Our Data embedding Framework is based on two-bit plane and each plane is used to embed the secret data bits. Framework starts with converting the secret data into bits and then choose the two consecutive pair pixels. After those converting pixels into lower bit plane and upper bit plane to embed the data.

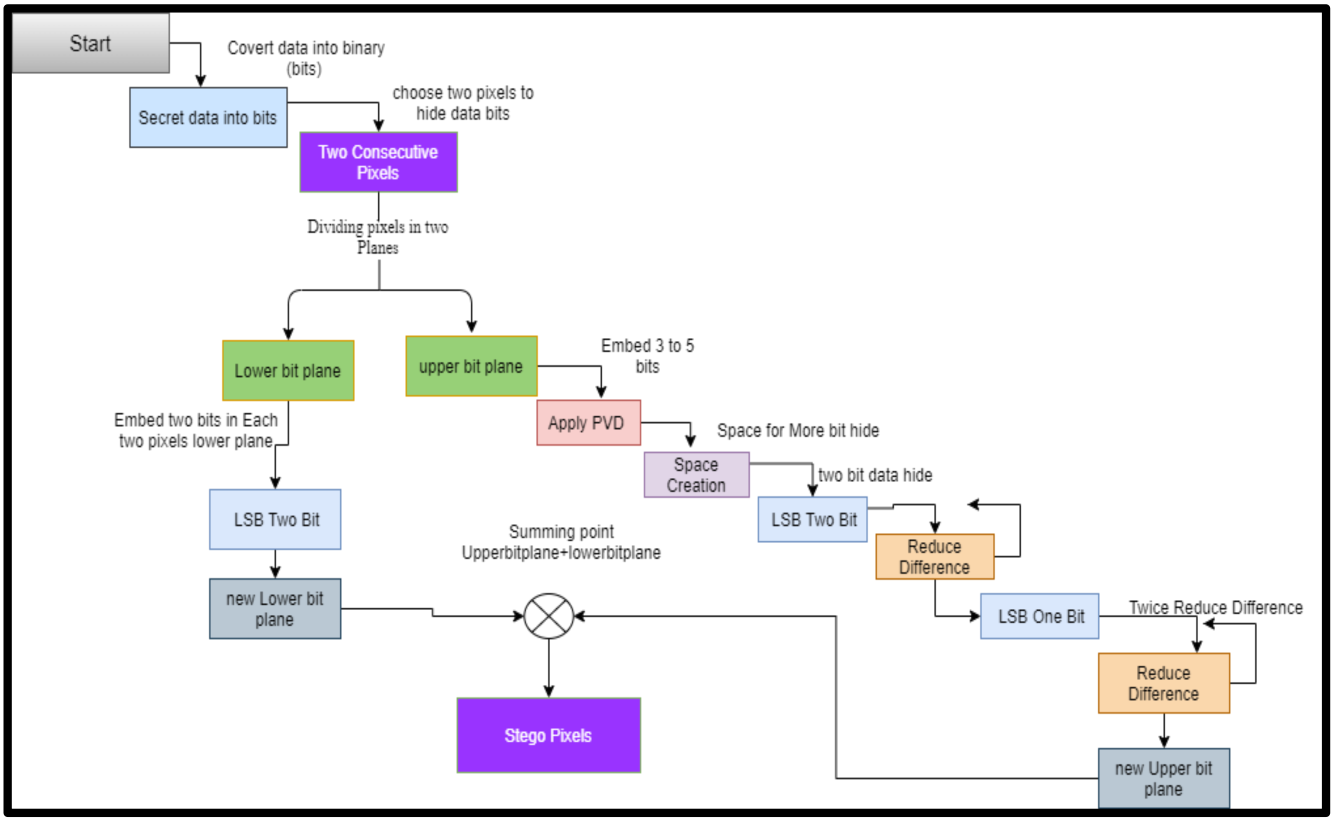


Figure 5: Data Embedding Scheme

Input: Grayscale 8-bit Image I of 512 x 512 and Secret data bit streams S

Output: Stegoimage I' size of 512 x 512

Step 1: Choosing two consecutive pixels ($P_{i,}$ P_{i+1}) from 8-bit image then separate them into two plane lower and upper planes. Upper plane contains 6 MSB bits of the image denoted as I_1 and lower plane contains remaining 2 LSB bits of the image denoted as I_2.

Step 2: Applying PVD on I_1 by taking the difference of two-pixel $d_m = |P_{i+1\,-}\ P_i|$.

Step 3: Determining the number of embedding bits n using range table by looking upper bound U_i and lower bound l_i of the difference $d_{m.}$

```
If   $d_m >= 0$ && $d_m <= 7$
    then  $U_i=7;\ li=0;$
elseif   $d_m >= 8$ && $d_m <= 15$
    then  $U_i=15;\ l_i=8;$
elseif   $d_m >= 16$ && $d_m <= 31$
    then  $U_i=31;\ l_i=16;$
elseif   $d_m >= 32$ && $d_m <= 63$
    then  $U_i=63;\ l_i=32;$
```

$n=log_2(\mathbf{U_i} - \mathbf{l_i} +1)$; *// calculating the number of bits to embed*

Then calculating binary to decimal value b_i^m from n bits streams of secret data.

Step 4: Calculate the new difference value based on n data bits streams.

$$\mathbf{d'_m = l_i + b_i^m}$$

Step 5: Calculate new Pair pixels based on new difference d'_m by following rules.

$$m=|\ d'_m - d_m\,|$$

$$(P'_i\ ,\ P'_{i+1}\ ) = (P_i - ceil(m/2)\ )\ ,\ P_{i+1} + floor(m/2)\ )\ \ \text{for } (d'_m \bmod 2 =1)$$

$$(P'_i\ ,\ P'_{i+1}\ ) = (P_i - floor(m/2)\ )\ ,\ P_{i+1} + ceil(m/2)\ )\ \ \text{for } (d'_m \bmod 2 =0)$$

Step 6: Make a space in order to embed two more data bits in new difference d'_m and embed two bits by converting decimal to binary and placing in last two bits.

$$h= d'_m\ * 4$$

$$newd'_m= bin(h) + n \quad \text{where n is next to bits}$$

Step 7: Twice Reduce the newd$'_m$ near to d$'_m$ by calculating the Location Map first and then Applying the Reduce Difference Expansion to get reduced newd$'_m$.

$$LM = \begin{cases} 0 & if\ 2\times 2^{n-1} \leq newd'_i \leq 3\times 2^{n-1} - 1 \\ 1 & if\ 3\times 2^{n-1} \leq newd'_i \leq 4\times 2^{n-1} - 1 \end{cases}$$

$$\downarrow$$

$$newd'_i = \begin{cases} newd'_i - 2^{\lfloor \log_2 h \rfloor - 1} & if\ 2\times 2^{n-1} \leq newd'_i \leq 3\times 2^{n-1} - 1 \\ newd'_i - 2^{\lfloor \log_2 h \rfloor} & if\ 3\times 2^{n-1} \leq newd'_i \leq 4\times 2^{n-1} - 1 \end{cases}$$

$$\downarrow$$

newd$'_m$ (Reduced new difference)

Step 8: Embed One More secret data bit from bit stream in new reduced difference by making one bit space and adding bit.

$$newd'_m = (newd'_m * 2) + nextbit \qquad (nextbit \in 0,1)$$

Step 9: Again twice Reduce the newd$'_m$ near to d$'_m$ by calculating the Location Map first and then Applying the Reduce Difference Expansion to get reduced newd$'_m$.

$$LM = \begin{cases} 0 & if\ 2\times 2^{n-1} \leq newd'_i \leq 3\times 2^{n-1} - 1 \\ 1 & if\ 3\times 2^{n-1} \leq newd'_i \leq 4\times 2^{n-1} - 1 \end{cases}$$

$$\downarrow$$

$$newd'_i = \begin{cases} newd'_i - 2^{\lfloor \log_2 h \rfloor - 1} & if\ 2\times 2^{n-1} \leq newd'_i \leq 3\times 2^{n-1} - 1 \\ newd'_i - 2^{\lfloor \log_2 h \rfloor} & if\ 3\times 2^{n-1} \leq newd'_i \leq 4\times 2^{n-1} - 1 \end{cases}$$

$$\downarrow$$

newd$'_i$ (Reduced new difference)

Step 10: Calculate updated pair pixel with new difference newd$'_m$ using previous calculated pair pixel.

$$L = \lfloor (P'_i , P'_{i+1}) /2 \rfloor$$

$$X = L + \left\lfloor \frac{newd'_i + 1}{2} \right\rfloor \quad , \quad Y = L - \left\lfloor \frac{newd'_i}{2} \right\rfloor$$

Step 11: Now Calculate the I_1 new upper plane pixels by calculating the new pair pixel (x, y) difference with two consecutive pixels ($P_{i,} P_{i+1}$) of image.

$$\text{If } X > P_i$$

$$\text{Then } R= | P'_i - P_i | ;$$

$$X'_i = P_i - 2 \quad ; \quad Y'_i = P_i - 2 + R$$

$$P'_i = X'_i+[2^{k+1} + 1]; \;\; P'_{i+1} = Y'_i + +[2^{k-1}]; \qquad \text{final } \boldsymbol{I'_1} \textit{ (Upper plane pixels)}$$

Step 12: Now replace $\boldsymbol{I_2}$ Lower Plane bits with next two Secret data bits from data stream Using LSB to get $\boldsymbol{I'_2}$.

Step 13: Now combine both upper bit plane and Lower bit plane to get Stego Pixel.

$$\text{Stego Image } \boldsymbol{I' = I'_1 + I'_2}$$

3.2 Data Extraction Scheme

Secret Data Extraction scheme is based on extraction of secret data bits streams that are embedded using Data embedding algorithm and extraction is exactly reversible process of data embedding scheme from stego image of same dimension. In this section input is stego image and output is secret data bit stream and extraction starts by choosing two consecutive pair pixels from stego image and separating them into upper bit plane and lower bit plane.

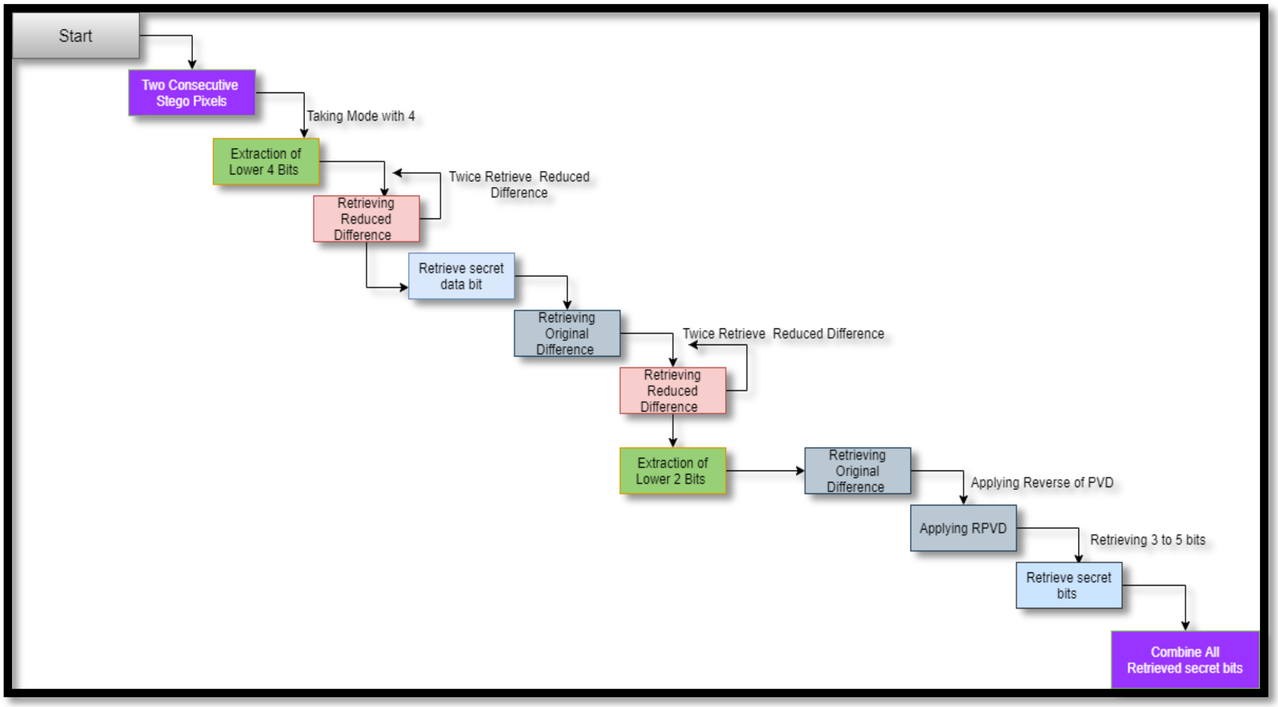

Start
Two Consecutive Stego Pixels
Taking Mode with 4
Extraction of Lower 4 Bits
Twice Retrieve Reduced Difference
Retrieving Reduced Difference
Retrieve secret data bit
Retrieving Original Difference
Twice Retrieve Reduced Difference
Retrieving Reduced Difference
Extraction of Lower 2 Bits
Retrieving Original Difference
Applying Reverse of PVD
Applying RPVD
Retrieving 3 to 5 bits
Retrieve secret bits
Combine All Retrieved secret bits

Figure 6 : Data Extraction Framework

Input: Stego Image I' of (512 x 512) 8 bit pixels.

Output: Secret Data bit Stream represented as (S)

Step 1: Choosing two consecutive pixels ($P'_{i,} P'_{i+1}$) from 8-bit stegoimage and retrieving the pair of stego pixels by reversely apply the normalized formula

$$P'_i = P'_i + [2^{k+1} - 1\ ]; \quad P'_{i+1} = P'_{i+1} - [2^{k-1}\ ];$$

Then separate calculated ($P'_{i,} P'_{i+1}$) into two plane lower and upper plane. upper plane contains 6 MSB bits of the image denoted as I'_1 and lower plane contains 2 LSB bits of datastream $\mathbf{S_1}$ of the image denoted as I'_2.

Step 2: Now taking difference of two stego pair pixels $\mathbf{h' = | P'_{i+1} - P'_i |}$.

Step 3: Applying reverse of reduced difference on I'_1 (Upper bit plane) to retrieve the difference to extract the remaining data stream bits by calculating the Location Map of **h'** and applying the formula twice.

$$\begin{tikzcd}
\text{LM} = \begin{cases} 0 & if\, 2 \times 2^{n-1} \le h' \le 3 \times 2^{n-1} - 1 \\ 1 & if\, 3 \times 2^{n-1} \le h' \le 4 \times 2^{n-1} - 1 \end{cases} \arrow[d] \\
h = \begin{cases} h' + 2^{\lfloor \log_2 h' \rfloor + 1} & \text{if} \quad \text{LM} = 1, \\ h' + 2^{\lfloor \log_2 h' \rfloor} & \text{if} \quad \text{LM} = 0. \end{cases} \arrow[u, bend right] \arrow[d] \\
\textbf{h} \quad \textbf{(retrieved difference)}
\end{tikzcd}$$

Step 4: Convert the **h** decimal to binary bin (h) and extract last bit of data $\mathbf{S_2}$.

Step 5: To retrieve remaining secret data bits then still need to retrieve the further difference by simply dividing h by 2 and taking floor on it and got h' and then again apply the retrieve reduced difference reversely by again calculating Location Map of h.

$$h' = \left\lfloor \frac{\mathbf{h}}{\mathbf{2}} \right\rfloor$$

$$\begin{tikzcd}
\mathrm{LM} = \begin{cases} 0 & if\, 2 \times 2^{n-1} \leq h' \leq 3 \times 2^{n-1} - 1 \\ 1 & if\, 3 \times 2^{n-1} \leq h' \leq 4 \times 2^{n-1} - 1 \end{cases} \arrow[d] \\
d_m = \begin{cases} h' + 2^{\lfloor \log_2 h' \rfloor + 1} & \text{if} \quad \mathrm{LM} = 1, \\ h' + 2^{\lfloor \log_2 h' \rfloor} & \text{if} \quad \mathrm{LM} = 0. \end{cases} \arrow[u, bend right]
\end{tikzcd}$$

Step 6: After that converting d_m into binary first and the split that binary into two planes first 6 MSB Upper plane denoted as ***M*** and last 2 LSB are retrieved data bit streams and denoted as $\boldsymbol{S_3}$**.**

Step 7: Convert the ***M*** binary to Decimal denoted as **d'_m (retrieved PVD difference).**

Step 8: Apply Reverse PVD in order to Determining/Extracting the Secret data bits $\boldsymbol{S_4}$ using range table by looking upper bound U_i and lower bound l_i of the difference **d'_m**.

```
If   d'm > = 0 && d'm < = 7
    then  Ui=7;  li=0;
elseif   d'm > = 8 && d'm < = 15
    then  Ui=15;  li=8;
elseif   d'm > = 16 && d'm < = 31
    then  Ui=31;  li=16;
elseif   d'm > = 32 && d'm < = 63
    then  Ui=63;  li=32;
S4= d'm - li  // Retrieving the secret data bit streams from PVD
S4= bin (S4) // Convert S4 decimal to binary
```

Step 9: Combining all retrieved bits in Reverse order.

$S = \boldsymbol{S_4} + \boldsymbol{S_3} + \boldsymbol{S_2} + \boldsymbol{S_1}$ *// S is retrieved Secret bit Stream*

3.3 Summary

In this Chapter, a novel image steganography based reversible data hiding framework was proposed that incorporated the secret data in the form of bits in cover image as described in Section 3.1 called as data embedding scheme. Whereas the vice versa scheme was introduced called as data extraction scheme in Section 3.2 to decode/ extract the secret data from output image called as stego image.

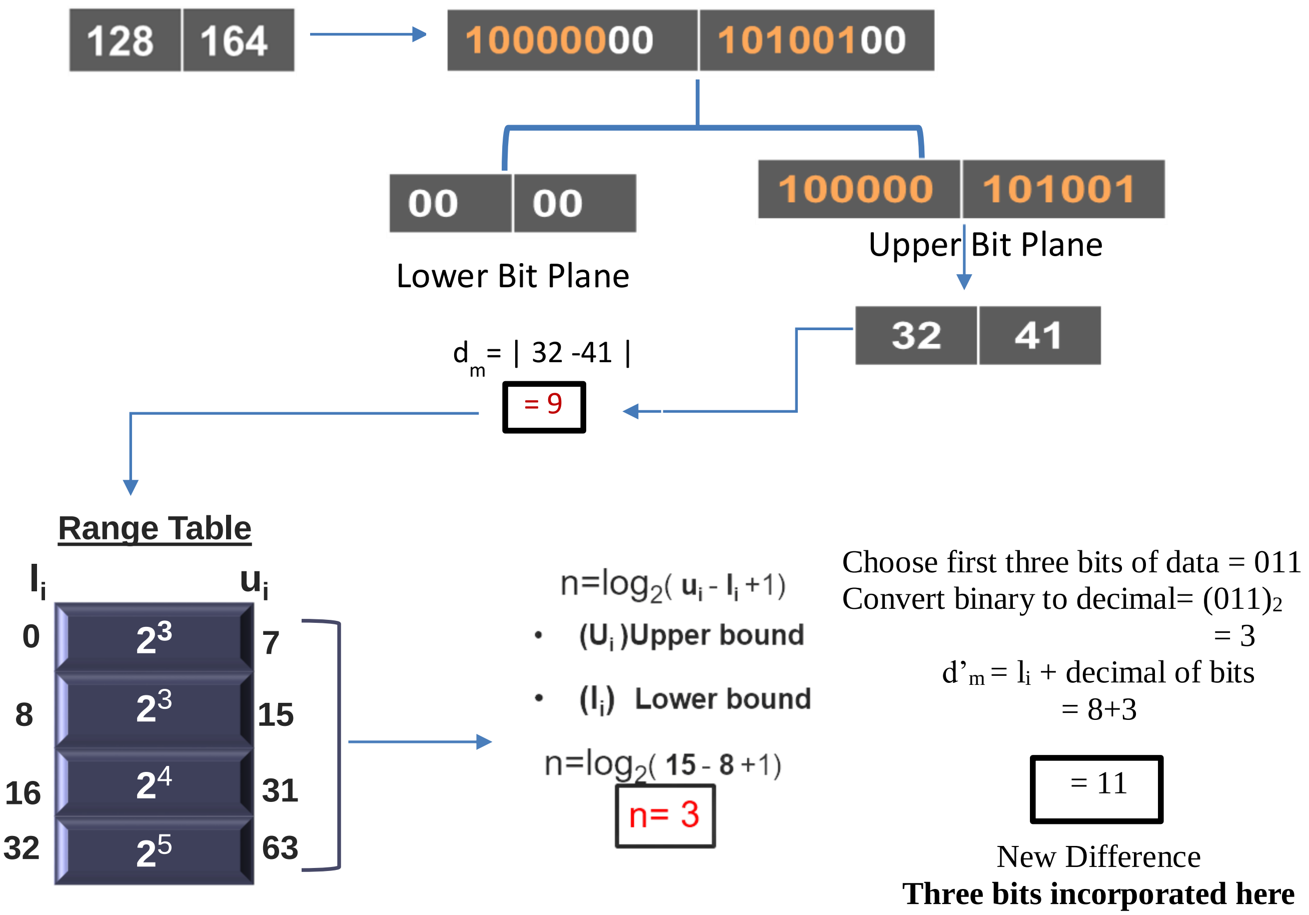
CHAPTER 4 : VALIDATION & EVALUATION OF PROPOSED FRAMEWORK

In this Chapter, the validity of proposed framework has been demonstrated via real world case study. The Chapter consist of two sections. In Section 4.1 covers the Data embedding Scheme validation to hide the maximum amount of data in such way that the visual quality of the image should be maintained significantly. In Section 4.2 provides Data extraction scheme validation to extract the data bit streams on destination side. In section 4.3 provides Evaluation and comparison of proposed framework results with previous studies.

4.1 Data Embedding Validation

Starts with example of two consecutive pixels from cover image then converting that pixel values into bits and separate the bits into 6:2 first 6 MSB bits are upper bit plane and Lower bit plane is last 2 LSB bits.

Secret data Bit's stream: 0111101011……



$$m = |\, d'_m - d_m \,| = |\, 11 - 9 \,| = 2$$

- $(p'_i, p'_{i+1}) = (32 - \text{ceil}(m/2)), 41 + \text{floor}(m/2))$
  $= (32 - \text{ceil}(2/2)), (41 + \text{floor}(2/2))$
  $= (32 - 1), (41 + 1)$

$$\mathbf{(p'_i, p'_{i+1}) = (31, 42)}$$

(New Pixel values)

- $h = (d'_m) * 4$ (Making space for more bits embed)

  $h = 11 * 4$ $\boxed{= 44}$

- Converting h in binary = bin (h) = bin (44) = $1\,0\,1\,1\,\underbrace{0\,0}_{\text{Space Created}}$

Embedding Next two bits of data in space by applying LSB

1 0 1 1 0 0

1 0 1 1 1 1

Two bits embedded here

- Converting $(1\ 0\ 1\ 1\ 1\ 1)_2$ into decimal

$$newd'_m \ \boxed{= 47}$$

As we can see $newd'_m > d'_m$ (47 > 11)

(Huge Difference we need to reduce **newd'$_m$ near to d'$_m$ for** better quality)

$$LM = \begin{cases} 0 & if\ 2 \times 2^{n-1} \le newd'_i \le 3 \times 2^{n-1} - 1 \\ 1 & if\ 3 \times 2^{n-1} \le newd'_i \le 4 \times 2^{n-1} - 1 \end{cases}$$

LM (47) =0 **LM (31) =0**

$$newd'_i = \begin{cases} newd'_i - 2^{\lfloor \log_2 h \rfloor - 1} & if\ 2 \times 2^{n-1} \le newd'_i \le 3 \times 2^{n-1} - 1 \quad \textbf{(If LM=0)} \\ newd'_i - 2^{\lfloor \log_2 h \rfloor} & if\ 3 \times 2^{n-1} \le newd'_i \le 4 \times 2^{n-1} - 1 \quad \textbf{(If LM=1)} \end{cases}$$

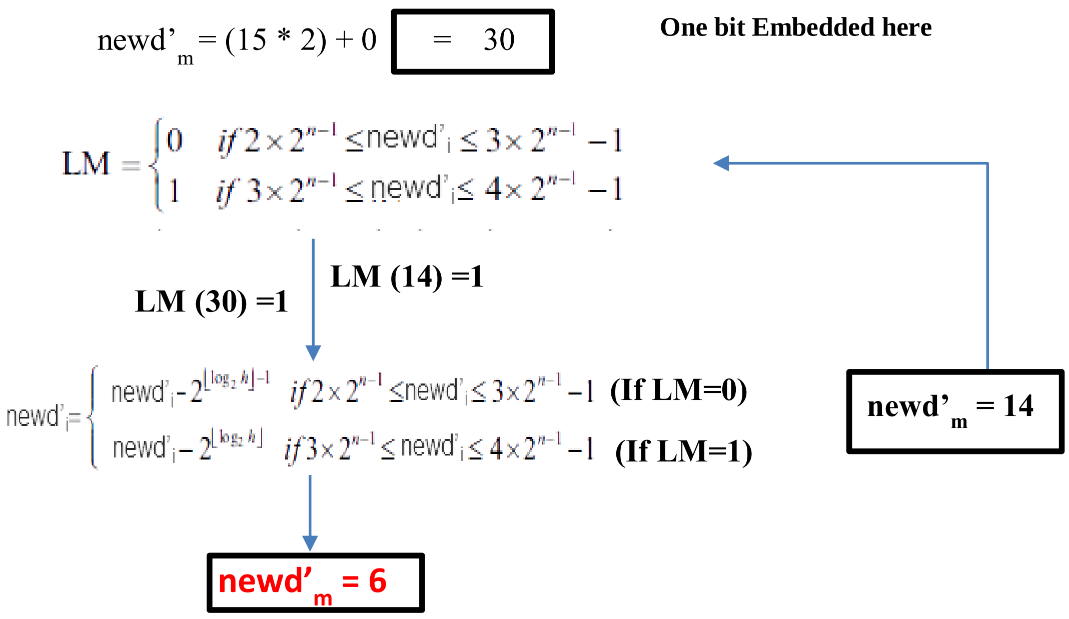
$$\boxed{\mathbf{newd'_m = 31}}$$

$$\boxed{\mathbf{newd'_m = 15}}$$

Now 15 is near to 11

- Now we can embed **one more data bit using LSB** because we reduced the

newd’$_m$ = (newd’$_m$ * 2) +nextbit (nextbit ∈ 0,1) Need to create space of one bit



newd’$_m$ = (15 * 2) + 0 $\boxed{= \quad 30}$ **One bit Embedded here**

$$LM = \begin{cases} 0 & if\ 2\times 2^{n-1} \le newd'_i \le 3\times 2^{n-1} - 1 \\ 1 & if\ 3\times 2^{n-1} \le newd'_i \le 4\times 2^{n-1} - 1 \end{cases}$$

LM (30) =1

LM (14) =1

$$newd'_i = \begin{cases} newd'_i - 2^{\lfloor \log_2 h \rfloor - 1} & if\ 2\times 2^{n-1} \le newd'_i \le 3\times 2^{n-1} - 1 \quad \textbf{(If LM=0)} \\ newd'_i - 2^{\lfloor \log_2 h \rfloor} & if\ 3\times 2^{n-1} \le newd'_i \le 4\times 2^{n-1} - 1 \quad \textbf{(If LM=1)} \end{cases}$$

newd’$_m$ = 14

newd’$_m$ = 6

Calculated pixels (P’$_i$, P’$_{i+1}$) = (31 , 42) with difference 11 we need to recreate the pixels with new difference **newd’$_m$ = 6**

$$L = \lfloor (31+42) /2 \rfloor \quad = \quad 36$$

$$x' = L + \left\lfloor \frac{\textbf{newd'}_m \textbf{+1}}{\textbf{2}} \right\rfloor \quad , \quad y' = L - \left\lfloor \frac{\textbf{newd'}_m}{\textbf{2}} \right\rfloor$$

$$x' = 36 + \left\lfloor \frac{6+1}{2} \right\rfloor \quad , \quad y' = 36 - \left\lfloor \frac{6}{2} \right\rfloor$$

$$x' = 36 + 3 \quad , \quad y' = 36 - 3$$

$$\textbf{(p'}_{i}\textbf{, p'}_{i+1}\textbf{) = (39, 33)}$$

(p$_i$, p$_{i+1}$)

32	41

Original pixels

(p$'_i$, p’$_{i+1}$)

39	33

Calculated pixels

$$\text{If } (\mathbf{p'_i} > \mathbf{p_i})$$

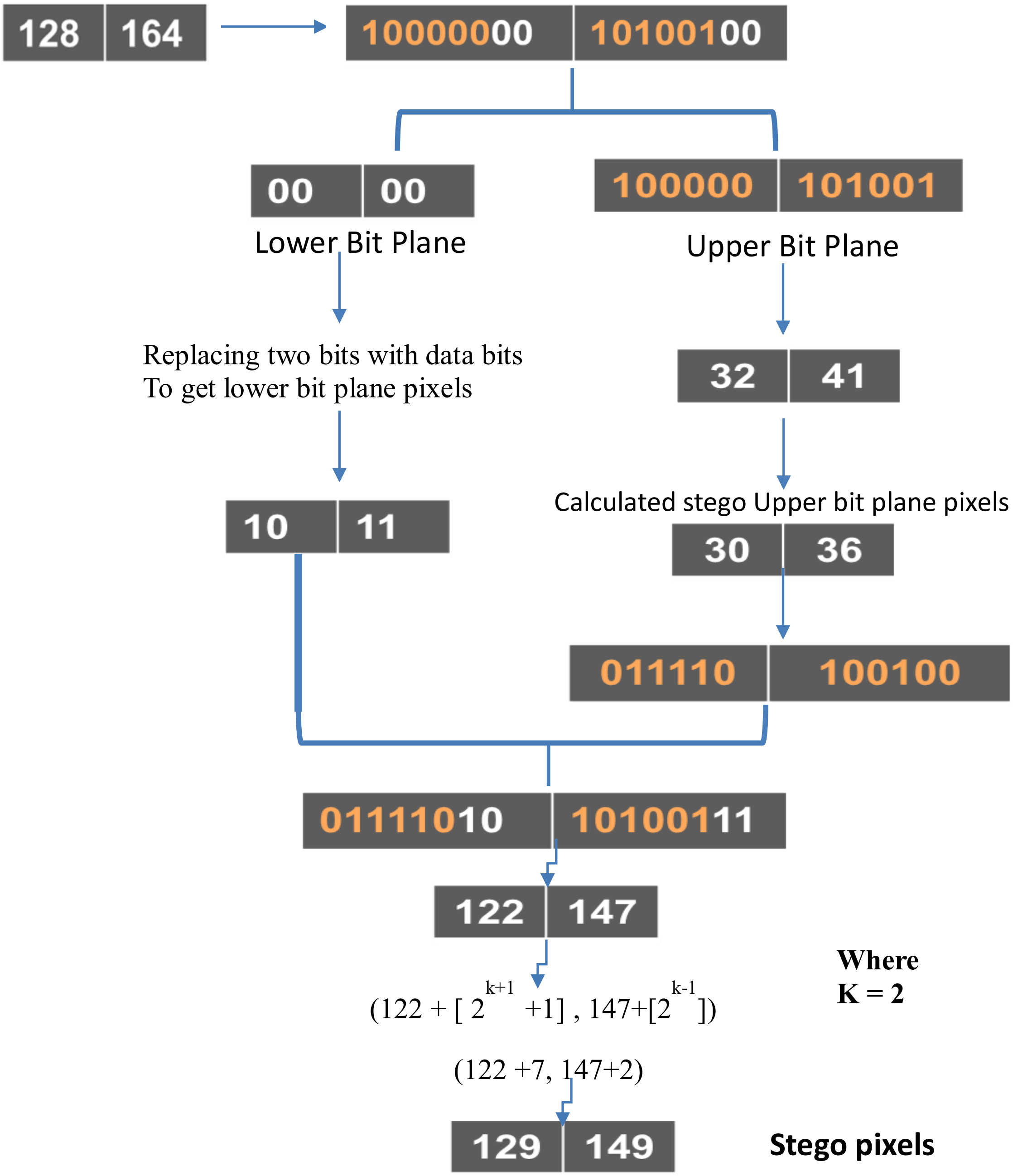
$$R = | 39 - 32 | = 6$$

$$p'_i = p_i - 2,\ p'_{i+1} = p_i - 2 + R$$

$$\mathbf{p'_i},\ \mathbf{p'_{i+1}} = (32 - 2, 32 - 2 + 6)$$

$$\boxed{\mathbf{p'_i},\ \mathbf{p'_{i+1}} = (30, 36)}$$

Stego Upper Plane I'


128
164
10000000
10100100
00
00
Lower Bit Plane
100000
101001
Upper Bit Plane
Replacing two bits with data bits
To get lower bit plane pixels
32
41
10
11
Calculated stego Upper bit plane pixels
30
36
011110
100100
01111010
10100111
122
147
$(122 + [2^{k+1} + 1], 147 + [2^{k-1}])$
$(122 + 7, 147 + 2)$
129
149

Where
K = 2

Stego pixels

Input: Grayscale 8-bit Image *I* of 512 x 512 and Secret data bit streams S

Secret data Bit's stream: 0111101011……

Output: Stegoimage I' size of 512 x 512 that is also called data embedded image.

Step 1: Choosing two consecutive pixels ($P_{i,} P_{i+1}$) = (128,164) from 8 bit image.

Step 2: Converting that consecutive pixel's values into binary (10000000, 10100100).

Step 3: After that separate (10000000, 10100100) into two bits plane one is lower bits plane and other is upper bits plane. upper bits plane contains 6 MSB bits that is first 6 bits from left to right side of the pixels binary that are (100000, 101001) denoted as I_1 and lower bits plane contains remaining 2 LSB bits that are two most right-side bits of the pixels binary that are (00, 00) denoted as I_2.

Step 4: Now starts by applying the Set of data embedding Operations on only Upper bits plane I_1 first and then lower bits plane I_2 is considered for data embedding at last once data incorporation is finished in upper bits plane.

Step 5: Convert upper bits plane binary (100000, 101001) into decimal that is equal to

$$(UP_{i,} UPi_{+1}) = (32,41)$$

Step 6: After that applying modified pixel value difference (PVD) technique on I_1 that contain 6 MSB bits.

Starts by taking the difference of original two-pixel $d_m = |UP_{i+1\,-}\ UP_i|$.

$$d_m = |\ 41 - 32\ |$$

$$\mathbf{d_m = 9}$$

Step 7: There is a range table that is used in pixel value difference (PVD) technique in order to determine that how much secret data can be hide in the form of bits and that calculation is truly based on the difference between the upper bits plane $d_{m.}$ If the difference is high, then maximum 5 secret data bits are chosen to embed in upper bits plane of two consecutive pixels of the image. And if the difference is low then minimum 3 secret data bits are chosen to embed in upper bits plane of two consecutive pixels of the image. High difference d_m also indicates that both upper bits plane pixels values are far from each other and there is dramatic difference of color can be existing in the image and lower difference d_m indicates that both upper bits plane pixels values are much closer to each other and there is small space available to hide the data in the form of bits. Range table is used to get two bounds upper bound U_i and lower bound l_i of the upper plane pixels. Range table quantization range is [0 - 7], [8 - 15], [16 - 31], [32 – 63]

Determining the number of embedding bits n using range table by looking upper bound U_i and lower bound l_i of the difference d_m.

```
$d_m = 9$      // already calculated in step 6
If   $d_m >= 0$ && $d_m <= 7$
    then  $U_i=7;$  $l_i=0;$
elseif   $d_m >= 8$ && $d_m <= 15$
    then  $U_i=15;$  $l_i=8;$
elseif   $d_m >= 16$ && $d_m <= 31$
    then  $U_i=31;$  $l_i=16;$
elseif   $d_m >= 32$ && $d_m <= 63$
    then  $U_i=63;$  $l_i=32;$
end
```

so $U_i=8;$ $l_i=15;$ *for* $d_m = 9$

Step 8: After that determine the number of bits that can be embed in available space using $U_i=8;$ $l_i=15$ by applying following rule

$$n=\log_2(\mathbf{U_i} - \mathbf{l_i} +1); \quad \textit{// calculating the number of bits to embed}$$

$$n=\log_2(\mathbf{15}- \mathbf{8} +1);$$

$$\mathbf{n= 3}$$

n=3 means choose first three bits from secret data bit stream (S) **0111101011** to embed.

Step 9: Then calculating binary to decimal of 011 bits and denoted as $\mathbf{b_i^m}$ from n bits streams of secret data.

$$\mathbf{b_i^m = 3}$$

Step 10: Calculate the new difference value based on n data bits streams.

$$\mathbf{d'_m= \boldsymbol{l_i} + \boldsymbol{b_i^m}}$$

$$\mathbf{d'_m= \boldsymbol{8}+ \boldsymbol{3}}$$

$$\mathbf{d'_m = 11}$$

Step 11: Now Calculate new Pair pixels based on new difference d'_m by following rules.

$$m=| d'_m - d_m |$$

$$m = | 11 - 9 |$$

$$m = 2$$

m is the difference between the original upper bits plane pixels and the new generated difference that incorporated the first three bits of the data.

Step 11: Now calculating new two upper bits plane pixels with new difference and m by using original upper bits plane pixels values because by using those new generated pixels on the extraction side it's become easy to retrieve these three bits.

$$(P'_i , P'_{i+1}) = (P_i – \text{ceil}(m/2)) , P_{i+1} + \text{floor}(m/2)) \text{ for } (d'_m \text{ mod } 2 =1)$$

or

$$(P'_i , P'_{i+1}) = (P_i – \text{floor}(m/2)) , P_{i+1} + \text{ceil}(m/2)) \text{ for } (d'_m \text{ mod } 2 =0)$$

As $d'_m = 11$

$(P'_i , P'_{i+1}) = (P_i – \text{ceil}(m/2)) , P_{i+1} + \text{floor}(m/2))$ // because 11 mod 2 is equal to 1

$(P'_i , P'_{i+1}) = (32 – \text{ceil}(2/2)) , 41 + \text{floor}(2/2))$

$(P'_i , P'_{i+1}) = (32 -1 , 41 + 1)$

$\mathbf{(P'_i , P'_{i+1}) = (31, 42)}$ // this is new upper bit plane pixels with new difference 11.

Step 12: Now there is space needed to embed more secret data in the form of bits by using Least significant bits LSB technique because there is no space available in d'_m new difference yet.

If convert the d'_m that is 11 into binary 1011 .As seen 11 is the LSB bits so for now it's impossible to embed more bits in 1011 because if we do this 11 that is LSB bits are replace with next secret data bits and then it's impossible to retrieve the first three secret data bits that we embedded using pvd so in order to embed more secret bits we need to create a space for two bits so in order to do this Make a space in order to embed two more data bits in new difference d'_m and embed two bits by converting decimal to binary and placing in last two bits.

$$h= d'_m * 4$$

$$h= 11 * 4$$

$$h= 44$$

Now convert h=44 into binary that is 101100 so as we can last two bits are 00 so it mean we have successfully created a space to embed two more secret data bits.

Step 13: Now embed the next two bits by replacing the LSB of the h=44 binary 101100 with next secret data bits streams S **0111101011** that is **1 1**

$newd'_{m}$= bin(h) + n where n is next to bits 1 1

$newd'_{m}$= binary(1 0 1 1 0 0) + 1 1

$newd'_{m}$ = 1011 11

1011**00** **// replacing these two LSB with secret data bits**

↓

$newd'_{m}$ =1011**11** **// replaced with next secret data bits that are 11**

Step 14: Now Convert the $newd'_{m}$ binary to decimal

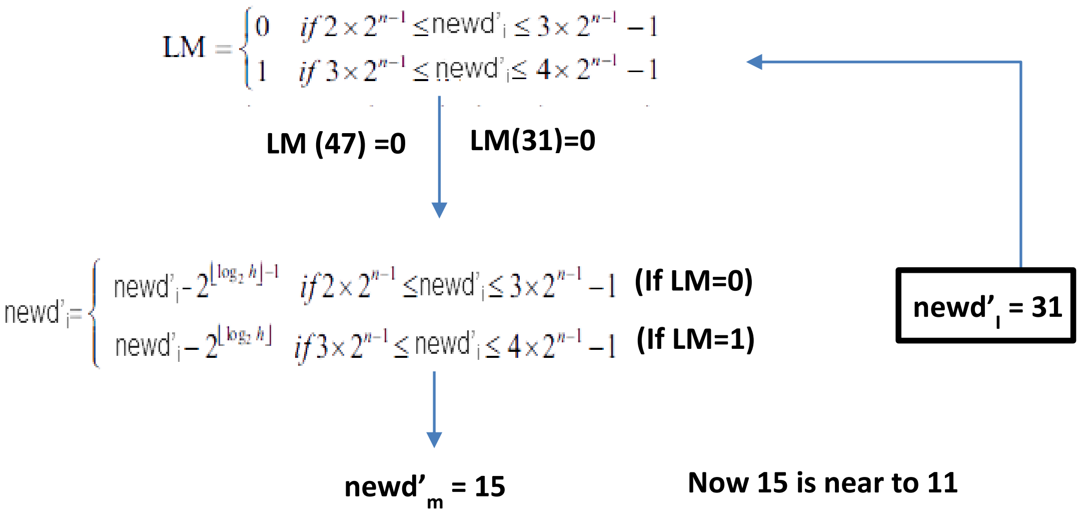
$newd'_{m}$ = (1011**11** **)**$_{\mathbf{2}}$

$newd'_{m}$ **=** **47**

Step 15: Now as seen $newd'_{m}$ is 47 that is huge from original difference that is 9 and the PVD generated difference that is 11. so, there is a reversible technique is required that reduce the difference near to the original difference because if the difference is not reduced properly through some reversible mechanism, then the new generated pixels are far from original pair pixels of upper bits plane that is directly affect the visual quality of the Embedded image and secondly, it is extremely easy to detect everybody to judge about the existence of the secret data bits inside the image. So to achieve the better visual quality then there is tire need of solution that reduce the difference so in order to do this we apply the reversible Difference Reduce (RDE) technique. RDE have main aim to reduce the $newd'_{m}$ that is 47 near to original difference 9 or PVD generated difference d'_{m}.

Step 16: Twice Reduce the $newd'_{m}$ 47 near to d'_{m} by calculating the Location Map (LM) first Location map Belong to {0,1}. Location map is used to decide which rule we need to apply, and it is all based on the difference range. After Location map calculation then Applying the Reduce Difference Expansion to get reduced $newd'_{m}$.

For 1st iteration out of 2 calculating the LM of 47 that is calculated 0 and after that calculate the reduced new difference 31 and then again pass that calculated difference 31 again to LM function to calculate the Location map that is calculated equal to 0 and again in 2nd iteration out of 2 on the bases of Calculated LM 0 again reduce it to get the final reduced new difference 15.



$$LM = \begin{cases} 0 & if\ 2\times 2^{n-1} \leq newd'_i \leq 3\times 2^{n-1} - 1 \\ 1 & if\ 3\times 2^{n-1} \leq newd'_i \leq 4\times 2^{n-1} - 1 \end{cases}$$

LM (47) =0 **LM(31)=0**

$$newd'_i = \begin{cases} newd'_i - 2^{\lfloor \log_2 h \rfloor - 1} & if\ 2\times 2^{n-1} \leq newd'_i \leq 3\times 2^{n-1} - 1 \quad \textbf{(If LM=0)} \\ newd'_i - 2^{\lfloor \log_2 h \rfloor} & if\ 3\times 2^{n-1} \leq newd'_i \leq 4\times 2^{n-1} - 1 \quad \textbf{(If LM=1)} \end{cases}$$

newd'$_l$ = 31

newd'$_m$ = 15 **Now 15 is near to 11**

Now $newd'_m$ =15 is much closer to PVD generated difference that is 11 than the previous calculated difference that is 47.

Step 17: Now one more bit of secret data is required to embed in $newd'_m$ =15. So in order to do this there is space needed to embed more secret data in the form of bit by using Least significant bits LSB technique because there is no space available in $newd'_m$ new difference yet .

If convert the $newd'_m$ =15 into binary 1111 .As seen 11 is the LSB bits so for now it's impossible to embed more bits in 1111 because if we do this 11 that is LSB bits are replace with next secret data bits and then it's impossible to retrieve the rest of the previous embedded secret data bits that we embedded using pvd and LSB so in order to embed more secret bit we need to create a space for one bit so in order to do this Make a space in order to embed one more data bit in new difference $newd'_m$ =15 and embed one bit by converting decimal to binary and adding with the binary value of $newd'_m$ =15 .

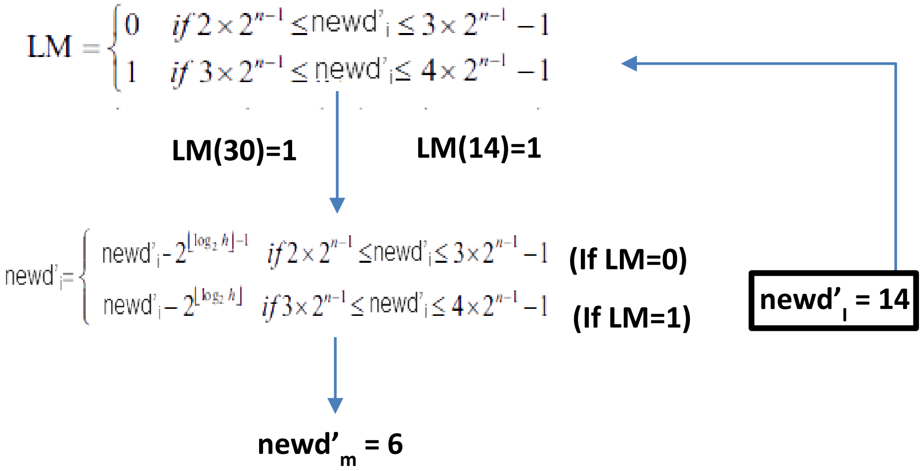
Embed One More secret data bit from bit stream in new reduced difference by making one bit space and adding bit.

$$newd'_m = (newd'_m *2) + nextbit \qquad (nextbit \in S)$$

$$newd'_m = (15 *2) + 0 \qquad (\text{nextbit is } \mathbf{0} \in \mathbf{0111101011})$$

$$newd'_m = 30$$

Step 18: Again need to twice Reduce the newd$'_{m}$ =30 near to d$'_{m}$ =11 because whenever embed the secret data bits using LSB we need to create a space that is the main reason if such huge differences between the newd$'_{m}$ and d$'_{m}$ and secondly when we replace the LSB with secret data bits the size of the difference also become larger so that's why we need to reduce it twicely by calculating the Location Map first and then Applying the Reduce Difference Expansion to get reduced newd$'_{m}$. For 1st iteration out of 2 calculating the LM of 30 that is calculated 1 and after that calculate the reduced new difference 14 and then again pass that calculated difference 14 again to LM function to calculate the Location map that is calculated equal to 1 and again in 2nd iteration out of 2 on the bases of Calculated LM 1 again reduce it to get the final reduced new difference 6.



$LM = \begin{cases} 0 & if\, 2\times 2^{n-1} \le newd'_{i} \le 3\times 2^{n-1} - 1 \\ 1 & if\, 3\times 2^{n-1} \le newd'_{i} \le 4\times 2^{n-1} - 1 \end{cases}$
LM(30)=1
LM(14)=1
$newd'_{i} = \begin{cases} newd'_{i} - 2^{\lfloor \log_2 h \rfloor - 1} & if\, 2\times 2^{n-1} \le newd'_{i} \le 3\times 2^{n-1} - 1 \\ newd'_{i} - 2^{\lfloor \log_2 h \rfloor} & if\, 3\times 2^{n-1} \le newd'_{i} \le 4\times 2^{n-1} - 1 \end{cases}$
(If LM=0)
(If LM=1)
newd'$_{I}$ = 14
newd'$_{m}$ = 6

Step 19: Calculate updated pair pixel with new difference newd$'_{m}$ using previous calculated pair pixel. Starts with calculating the average value of the pixels that helps to generate the new pixels for upper bits plane by using new difference that is recently calculated newd'$_{m}$ = 6 .

$$L = \lfloor (P'_{i} , P'_{i+1}) /2 \rfloor$$ // Formula for calculation for average of pixels

$$X = L + \left\lfloor \frac{newd'_{i} +1}{2} \right\rfloor \quad , \quad Y = L - \left\lfloor \frac{newd'_{i}}{2} \right\rfloor$$ // Formula for calculating new pixels.

$$L = \lfloor (31 , 42) /2 \rfloor$$ // calculating average value

$L = 36$ // calculated average value

$x' = 36 + \lfloor (6+1)/2 \rfloor$, $y' = 36 - \lfloor 6/2 \rfloor$ // calculating new pixels values

$P'_i , P'_{i+1} = (39, 33)$

Step 20: Now Calculating the final I_1 new upper bits plane pixels of the image by calculating the new pair pixel (x, y) difference with two consecutive pixels (P_i, P_{i+1}) of image in such a way that the difference between the pixels should be according to the new difference that is newd'$_m$ = 6. We need to do this for better visual quality so that the existence of the message is not suspicions. Because as described more embed the secret data bits in image pixel. Then image may degrade so we need to reduce degradation as much as possible so that the similarity index become high between the cover image that is chosen for hide the data and stego image that is data embedded image. X =39 that is one of new upper plane pixel value and P_i is the first original upper plane value that is 32. Starts with checking that if first new upper plane pixel is greater than the original one then it means we need to do some adjustment in such a way that the quality of the image should be maintained significantly. After that calculate R that is difference between the new and original upper bit plane 39-32.

If $39 > 32$

Then $R = | 39 - 32 | = 6$

$X'_i = 32 - 2$; $Y'_i = 32 - 2 + 6$

$[X'_i , Y'_i] = (30, 36)$ final I'_1 *(Upper plane pixels)*

Step 21: After finishing the upper bits plane with (30, 36) by embedding 6 bits of secret data bits. Now remaining data bits are embedded in Lower bits plane of the Image by simply replacing the bits with the secret data bits by apply the LSB Least significant Bit's technique. On Lower bit plane of original image data bits are (00, 00) so next data bits that are (10, 11) are simply replaced. So I_2 = (10, 11)

(00 , 00)

↓

(10 , 11) // (10 ,11) ∈ **0111101011**

Step 22: Now combine both upper bit plane and Lower bit plane to get Stego Pixel. Before combining both planes convert upper bits plane into binary and Lower bits plane is already in binary. So upper bit plane pixels are (30, 36) so the binary are (**011110, 100100**)

Upper bit plane in binary (***I'₁***) = (**011110, 100100**)

Lower bit Plane in binary (***I'₂***) = (**10, 11**)

$$I' = I'_1 + I'_2$$

$$I' = (011110,\ 100100) + (10,\ 11)$$

$$I' = 01111010,\ 10010011$$

Converting *I' into decimal to get the stego pixels*

$[X'_i\ ,\ Y'_i\ ] = (122, 147)$

Step 23: Now Need to Normalize each $[X'_i\ ,\ Y'_i\ ]$ pixel for further better visual quality so in order to do this applying modified formula that contain k=2 because k is the total bits that are replaced using Lower bit plane. So, we need to normalize it according to the lower bits plane just like the operations performed on upper bit plane.

$$P'_i = X'_i + [2^{k+1} + 1\ ];\ \ P'_{i+1} = Y'_i + +[2^{k-1}\ ];$$

(122 +7, 147+2)

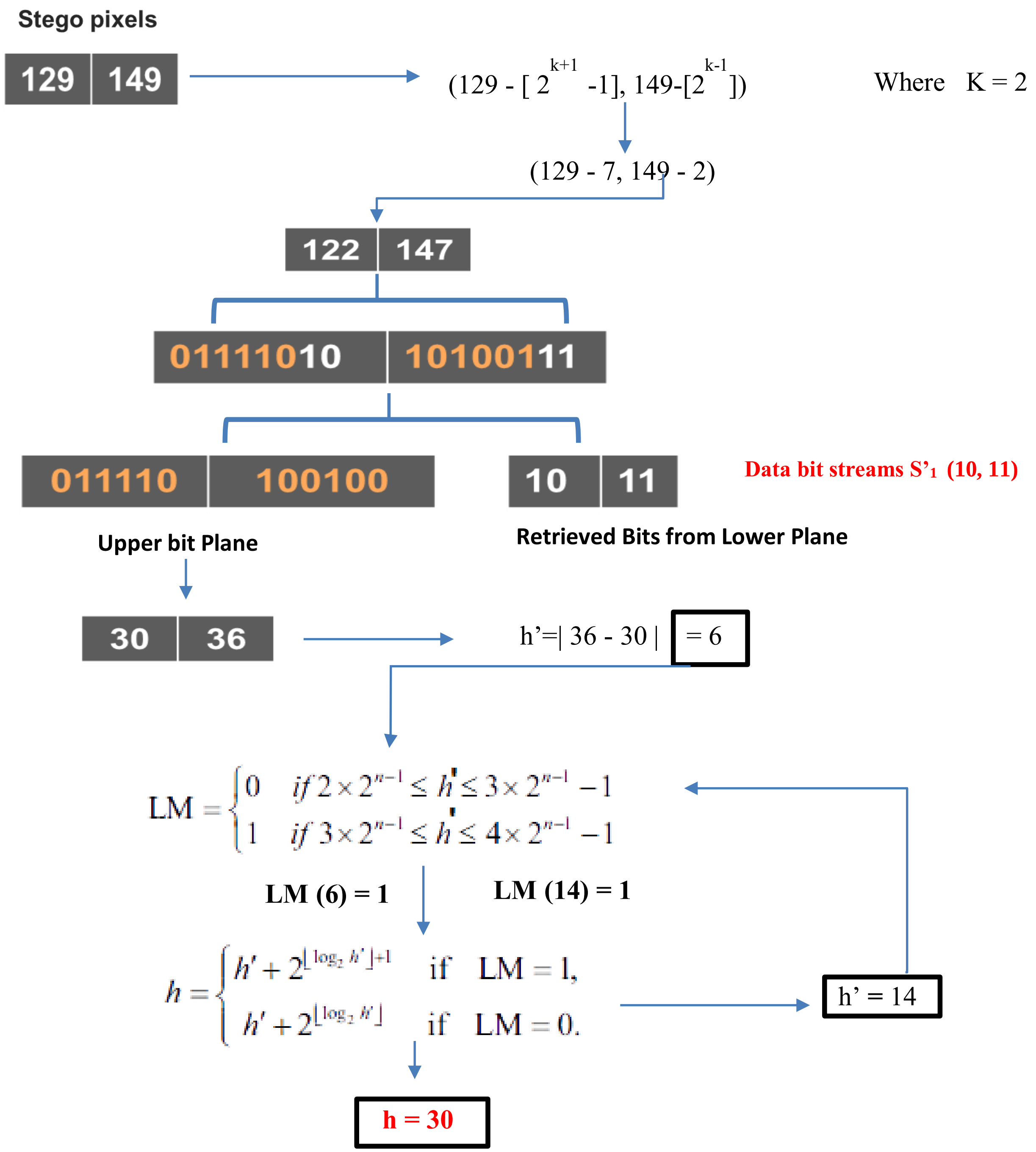
Stego pixel = (129 , 149) // final sego pixel.

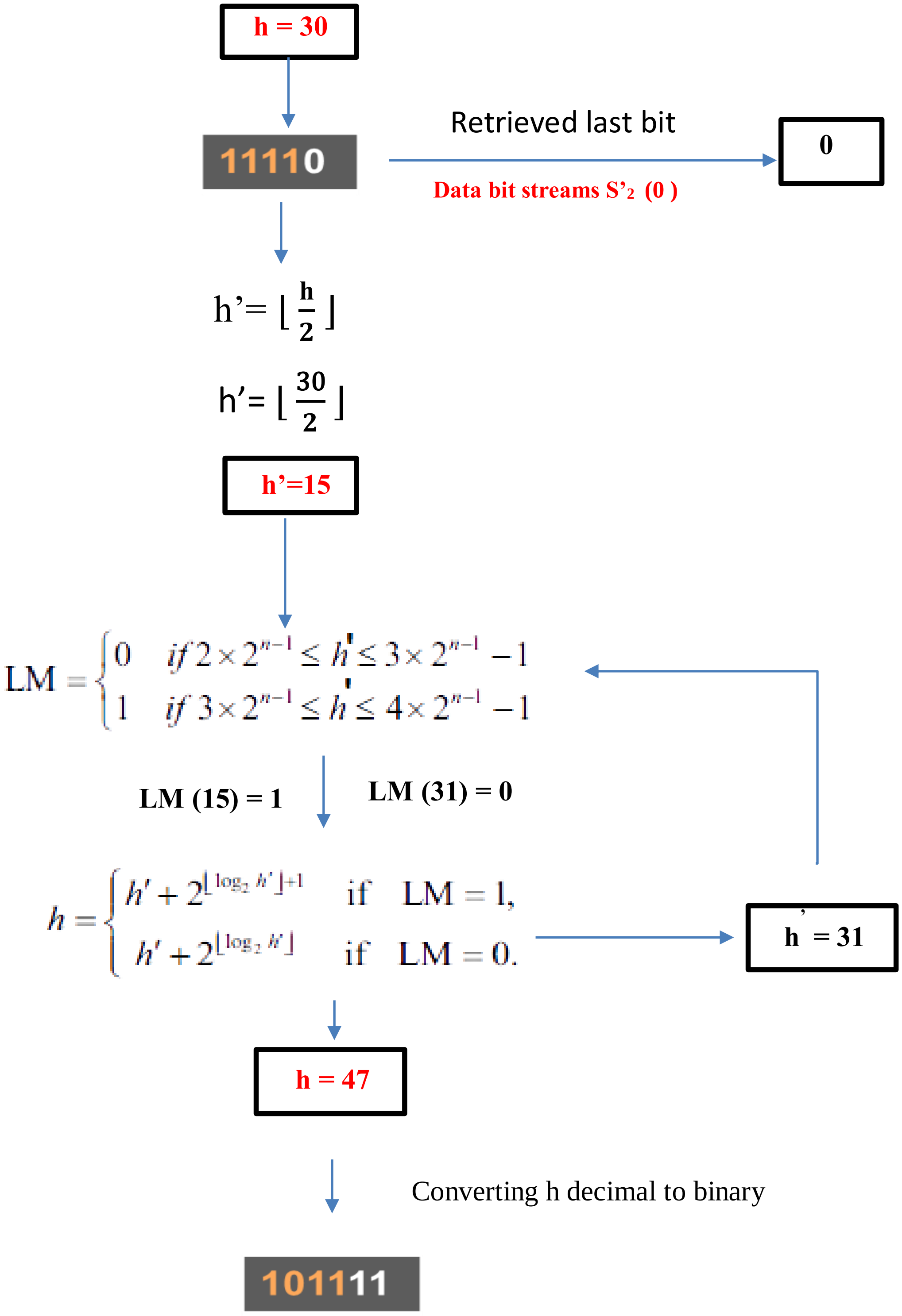
4.2 Data Extraction Validation

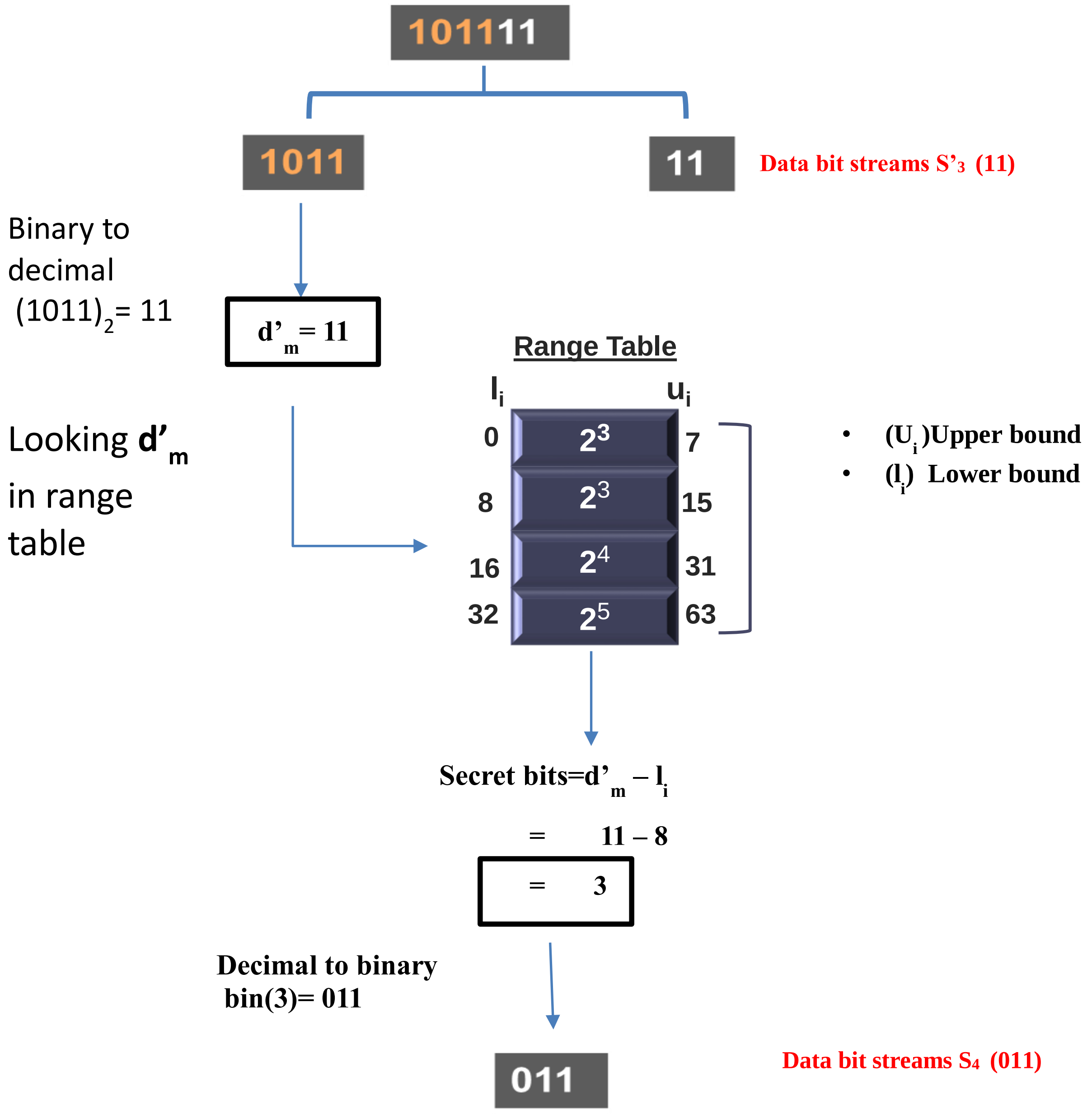
Input: Stego Image ***I' Size:*** 512x 512 8-bit resolution

Output: Data bit Streams S

Process: Start with choosing two consecutive pixels from stego image ***I'*** for denormalizing the pixels and converting that pixel's values into bits and separate the bits into 6:2 first 6 MSB bits are upper bit plane and Lower bit plane is last 2 LSB bits and these LSB bits are retrieved data bits.


Stego pixels
129
149
(129 - [2^{k+1} -1], 149-[2^{k-1}])
Where K = 2
(129 - 7, 149 - 2)
122
147
01111010
10100111
011110
100100
10
11
Data bit streams S’₁ (10, 11)
Upper bit Plane
Retrieved Bits from Lower Plane
30
36
h’=| 36 - 30 |
= 6
$LM = \begin{cases} 0 & if\, 2\times 2^{n-1} \le h' \le 3\times 2^{n-1} - 1 \\ 1 & if\, 3\times 2^{n-1} \le h' \le 4\times 2^{n-1} - 1 \end{cases}$
LM (6) = 1
LM (14) = 1
$h = \begin{cases} h' + 2^{\lfloor \log_2 h' \rfloor + 1} & \text{if} \quad LM = 1, \\ h' + 2^{\lfloor \log_2 h' \rfloor} & \text{if} \quad LM = 0. \end{cases}$
h’ = 14
h = 30


h = 30
11110
Retrieved last bit
0
Data bit streams S'_2 (0)
$h' = \lfloor \frac{h}{2} \rfloor$
$h' = \lfloor \frac{30}{2} \rfloor$
h'=15
$LM = \begin{cases} 0 & if\, 2 \times 2^{n-1} \leq h' \leq 3 \times 2^{n-1} - 1 \\ 1 & if\, 3 \times 2^{n-1} \leq h' \leq 4 \times 2^{n-1} - 1 \end{cases}$
LM (15) = 1
LM (31) = 0
$h = \begin{cases} h' + 2^{\lfloor \log_2 h' \rfloor + 1} & \text{if} \quad LM = 1, \\ h' + 2^{\lfloor \log_2 h' \rfloor} & \text{if} \quad LM = 0. \end{cases}$
h' = 31
h = 47
Converting h decimal to binary
101111



Data bit streams S'_3 (11)

Binary to decimal $(1011)_2 = 11$

$d'_m = 11$

Looking $\mathbf{d'_m}$ in range table

Range Table

l_i		u_i
0	2^3	7
8	2^3	15
16	2^4	31
32	2^5	63

- (U_i)Upper bound
- (l_i) Lower bound

Secret bits=$d'_m - l_i$

$= \quad 11 - 8$

$= \quad 3$

Decimal to binary
bin(3)= 011

Data bit streams S_4 (011)

Now reversing the each set of bits that retrieved

S= S_4+ S_3+ S_2+ S_1 *// S is retrieved Secret bit Stream*

S= *0111101011*

0111101011 = **0111101011**

Embedded bits
Using data embedding

Retrieved bits
Using data extraction

Input: Stego Image I' of (512 x 512) 8-bit pixels.

Output: Retrieve Secret data Bit's stream: 0111101011……

Step 1: Starts with choosing two consecutive pair pixels (P'_{i}, P'_{i+1}) from 8 bit I' from size of 512 pixels rows x 512 pixels columns data embedded image that is also called as stego image. Decoding or data extraction technique is exactly the reversible of data embedding system each and every terminology and operation are applied just like the embedded system but in reversible manner. From Embedded System we got Stego pixels **(P'_{i}, P'_{i+1}) = (129, 149)** upon which different operations and terminologies are reversibly applied in this section.

Step 2: Now Need to denormalize the each and every pair pixels of the image (P'_{i}, P'_{i+1}) that are normalized for further better visual quality of the stego image and the original cover image so that the image should not appeal itself to any hacker or intruder about the existence of the data by using the embedded system terminologies .Denormalization is required to get those pair pixels that are used for the further extraction of the secret data bits streams from pixels (129, 149) .so in order to do this applying reversible modified formula that contain **k=2 .**k is the total bits that replaced in Lower bits plane using the Least significant bit Technique that is 2 bits in the above Embedded Scheme. Here denormalization operation is performed on Stego pixels = (129, 149) that we got from applied several operations in embedded system.

Denormalization formula

$$P'_{i} = P'_{i} + [2^{k+1} - 1]; \quad P'_{i+1} = P'_{i+1} - [2^{k-1}];$$

$$P'_{i} = 129 + [2^{2+1} - 1]; \quad P'_{i+1} = 149 - [2^{2-1}]; \text{ //applying formula on pixels (129, 149)}$$

$$P'_{i} = 129 + [8 - 1]; \quad P'_{i+1} = 149 - [2]; \text{ //Calculation}$$

$$P'_{i} = 129 + [7]; \quad P'_{i+1} = 149 - [2]; \text{ //Calculation}$$

$$(P'_{i}, P'_{i+1}) = (122, 147)$$

Now (P'_{i}, P'_{i+1}) = (122, 147) is original stego pixels that contain the secret data bits stream (S) 0111101011 So from step 3 to onward operations are performed to retrieve that secret data.

Step 3: Convert the (P'_{i}, P'_{i+1}) = (122, 147) into binary number that is (01111010, 10100111).

Step 4: After that Split, up the Received binary bits of (P'_{i}, P'_{i+1}) in Step 3 into two bits plane stego upper bits Plane and the stego lower bits Plane. Splitting up Ratio is 6: 2 of the bits. Which means First left most six bits of (01111010, 10100111) are called stego upper bits plane that are

(011110, 101001) and last two least Significant bits of (01111010, 10100111) are called stego lower bits plane that are (10, 11).

Step 5: Stego lower bits plane (10, 11) of (P'_i, P'_{i+1}) = (122, 147) = (01111010, 10100111) are the bits of secret data bits and it is denoted as $\mathbf{S_1}$ and lower bit plane also denoted as I'_1 .

Step 6: Now till now the 4 secret data bits that embedded in lower bit plane is retrieved and now retrieving rest of the remaining secret data bits from stego upper bit plane (011110, 101001).so convert (011110, 101001) into decimal number and denoted as (i,j) that are (i,j)=(30,36).

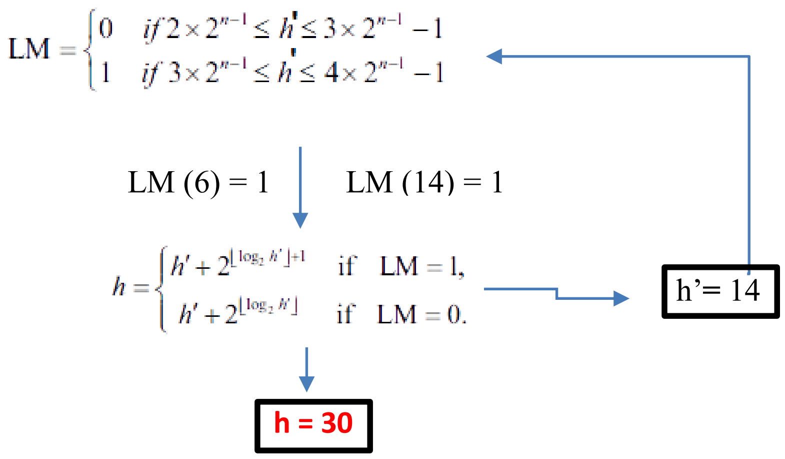
Step 7: After that take difference of stego upper bit plane pixels and denoted as h'.

$$h' = | j - i |$$

$$h' = | 36-30 |$$

$$h' = 6 \quad // \text{ difference}$$

Step 8: Now retrieve the difference value for secret data extraction that is reduced in embedded scheme by applying the reversible Difference expansion Reeducation (RDE) technique. In embedded system we already reduced the difference near to the original difference that enhanced the visual quality of the stego image. On the other hand, in data extraction scheme the reverse process is followed to retrieve the original difference from reduced difference. So, in order to do this we need to calculate the Location Map denoted as LM just like the data embedding scheme.



$$LM = \begin{cases} 0 & if\, 2\times 2^{n-1} \leq h' \leq 3\times 2^{n-1} - 1 \\ 1 & if\, 3\times 2^{n-1} \leq h' \leq 4\times 2^{n-1} - 1 \end{cases}$$

$$h = \begin{cases} h' + 2^{\lfloor \log_2 h' \rfloor + 1} & \text{if} \quad LM = 1, \\ h' + 2^{\lfloor \log_2 h' \rfloor} & \text{if} \quad LM = 0. \end{cases}$$

RDE technique is applied twice on the reduced difference starts by calculating the Location Map LM for 6 and calculated LM of 6 is 1. So, LM is 1 applying the formula $h=h'+2^{floor(log2\ h')\ +1}$ .So temporary h’ is equal to 14. But still we need to apply again the RDE on h’=14 for further difference retrieval that will be used for data bits extraction. Location Map of h’=14 is calculated as 1 Now applying the formula h=h’+$2^{\text{floor(log2 h')} +1}$ calculated original difference is 30 that is denoted as h. so h =30.

Step 9: After that h=30 is converted into decimal to binary to retrieve the secret data by retrieving the Least significant bit LSB of 30. Binary of 30 is 11110 and extracting last most right bit that is **0** and this retrieved bit is denoted as **S_2** **.**

Step 10: In order to retrieve remaining secret data bits streams then still need to retrieve the further difference by simply dividing h by 2 and taking floor on it and got h’ and then again apply the retrieve reduced difference reversely by again calculating Location Map of h=30 decimal value.

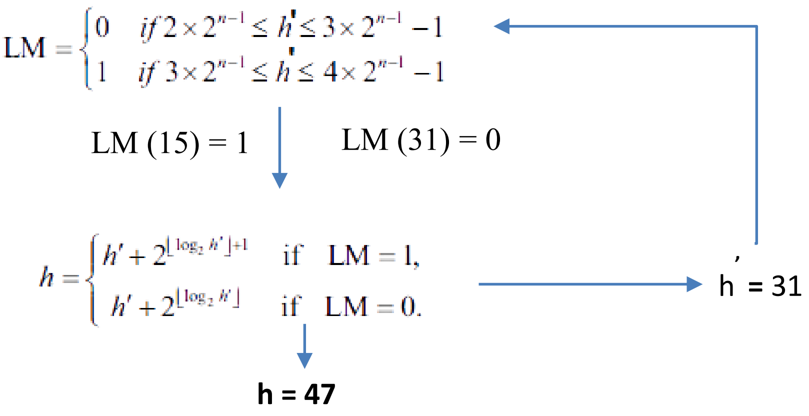
$$h' = \left\lfloor \frac{\mathbf{h}}{\mathbf{2}} \right\rfloor$$

$$h' = \left\lfloor \frac{\mathbf{30}}{\mathbf{2}} \right\rfloor$$

$$h' = 15$$

Now new difference is h’=15 is used for further remaining extraction of the secret data stream bits.

Step 11: After that again need to twice apply the RDE technique to retrieve the difference by using Calculating the Location Map and applying formula again .Starts by calculating Location map h’=15 that is 1.


$LM = \begin{cases} 0 & if\, 2\times 2^{n-1} \le h' \le 3\times 2^{n-1} - 1 \\ 1 & if\, 3\times 2^{n-1} \le h' \le 4\times 2^{n-1} - 1 \end{cases}$
LM (15) = 1
LM (31) = 0
$h = \begin{cases} h' + 2^{\lfloor \log_2 h' \rfloor + 1} & \text{if} \quad LM = 1, \\ h' + 2^{\lfloor \log_2 h' \rfloor} & \text{if} \quad LM = 0. \end{cases}$
h' = 31
h = 47

Now Location Map is 1 so applying formula h= h’ + $2^{\text{floor(log2 h')} +1}$ and on result h’ =15 is override with h’ = 31 .Now again calculate the Location Map for h’ = 31 and on result 0 is received and for LM=0 apply the formula h= h + $2^{\text{floor(log2 h')}}$ so h is basically the original retrieved difference become 47 .Now new difference is 47 that is used for further extraction of the secret data that is embedded using Least significant bit (LSB) technique and pixel value difference (PVD) technique.

Step 12: Now h=47 that is new difference is used to extract two bits of secret data bits from LSB bits of the 47. So, in order to do this first need to convert the 47 into binary that is equal to 101111.

Step 13: Now convert the binary of 47 that is equal to 00101111. So, we need to split and convert into two bits plane in order to extract the data from both bit planes upper bit plane and the lower bit planes. Last two LSB bits of 00101111 is 11 are lower bits plane and rest of the first 6 MSB bits is 001011 is called upper bits plane.

Step 14: Lower bits plane bits 11 is retrieved secret data bits denoted as ***S_3*.**

Step 15: Now the secret data bits that embedded using Pixel value difference (PVD) technique need to be retrieved by applying the reverse technique of the PVD so in order to do this upper bit's plane 001011 are used for further extraction of secret data stream bits. So, in order to do this convert the upper bits plane from binary to decimal value that is equal to $(1011)_2$= 11 that is denoted as **d'_m** is used for further processing.

Step 16: Apply Reverse PVD in order to Determining/Extracting the Secret data bits ***S_4*** using range table on PVD difference that is 11. Range table is used to get two bounds upper bound *Ui* and lower bound *li* of the upper plane pixels. Range table quantization range is [0 - 7], [8 - 15], [16 - 31], [32 – 63].

Determining the number of embedding bits n using range table by looking upper bound U_i and lower bound l_i of the difference d'_m

```
                Where  $d'_m = 11$   //As calculated
        If  $d'_m >= 0$ && $d'_m <= 7$
            then  $U_i=7;$  $l_i=0;$
        elseif  $d'_m >= 8$ && $d'_m <= 15$
            then  $U_i=15;$  $l_i=8;$
        elseif  $d'_m >= 16$ && $d'_m <= 31$
            then  $U_i=31;$  $l_i=16;$
        elseif  $d'_m >= 32$ && $d'_m <= 63$
            then  $U_i=63;$  $l_i=32;$
```

end

so $U_i=8;\ l_i=15;$ *for* $d'_m = 11$

Step 17: Now retrieving the number of secret data bits S_4 that are embedded using PVD So in order to this subtract the difference value $d'_m = 11$ from calculated lower bound of the $l_i=15$.

$$v = d'_m - l_i \quad \textit{// Retrieving the secret data bit streams from PVD}$$

$$v = |\, 11 - 8 \,| = 3$$

Now need to convert *v* that is number of bits are used need to convert it in binary to retrieve and that bits are the retrieved bits and denoted as S_4

$$S_{4=}\ bin\ (v) \quad \textit{// Convert v decimal to binary}$$

$$S_{4=}\ bin\ (3) = 011$$

Step 9: At last, need to Combine and organize ***S1, S2, S3, S4*** all retrieved secret data bits in Reverse order so that the retrieved data is completed.

As we know : $S_1 = 10\ 11$, $S_2 = 0$, $S_3 = 11$, $S_4 = 011$

$$S = S_4 + S_3 + S_2 + S_1$$

$$S = 011 + 11 + 0 + 1011 \quad \textit{// Combining is retrieved Secret bit Stream}$$

$$S = 0111101011 \quad \textit{// S is retrieved Secret bit Stream}$$

Retrieved secret data bit stream is 0111101011 is equal to the secret data bit streams 0111101011 that is embedded using embedded scheme.

4.3 Evaluation and Comparison

In this Section, Results of proposed scheme for data encoding and data extraction is compared with the previous work that have done by different researchers like Wu &Tsai [23], Shen et al [24], Xu et al. scheme [25] and KH Jung in [9]. The 512x512 8-bit greyscale test images are used for results comparison and these images are collected form SIPI (Signal and Image Processing Institute) database [26]. The Results are achieved from proposed system was got using i3 CPU

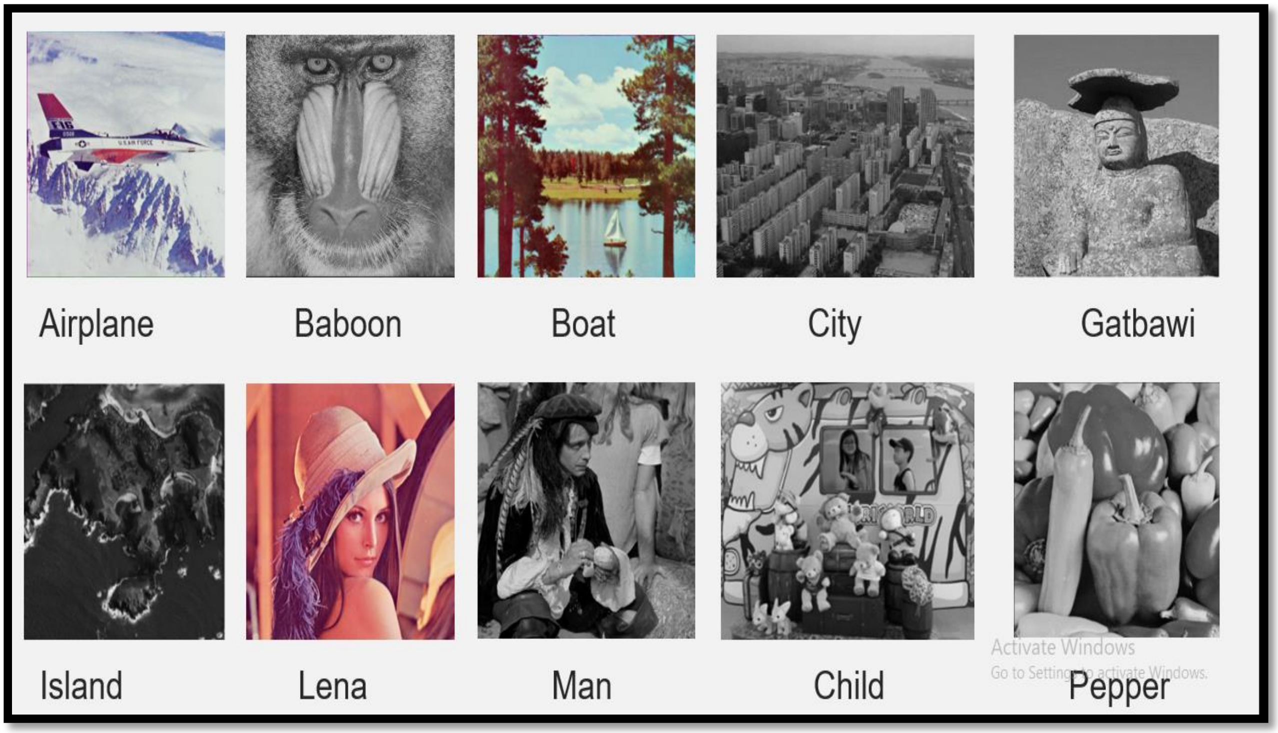


Figure 7 : SIPI Database Dataset

(Central Processing Unit) 3.33 GHz core 2 and 4GB RAM (Random Access Memory) by using MATLAB R2017.Secret Data is generated using pseudorandom generator function of Matlab to Encoding/ Decoding from the cover images. Evaluation of the proposed scheme is based upon two parameters PSNR (Peak Signal to Noise Ratio) related to visual quality of the image and second parameter is Embedding Capacity that is related to calculate the ratio of secret data embedded in the form of bits and this parameter is also used to calculate the total pixels that incorporate the secret data in the form of bits. Generally, the PSNR (Visual Quality) of the stego image compared with the cover image by using mathematical formula. Generally, if greater the PSNR then it’s indicated that the visual quality of the stego image is better and almost similar to the original cover image. The mathematical formula for PSNR calculation is

$$\boldsymbol{PSNR = 10\, log10 \frac{(255)\hat{}2}{MSE}}$$

$$\boldsymbol{MSE = \frac{1}{RxC} \sum_{k=0}^{R\,x\,C} (stegopixel'_K - coverpixel_K)}$$

Where, k denotes the location of the ***S'*** stego image pixel and the ***S*** Cover image pixel from each rows and columns of sized images (R =512) × (C = 512).

Achieved results from the proposed scheme and already previously proposed schemes by different researchers are shown in Table 1 like K. H. Jung scheme [19], Wu & Tsai scheme [23], Shen et al. scheme [24], Xu et al. scheme [25] in terms of visual quality PSNR (dB) and Secret data embedding capacity in the form of bits. As Seen in Table 1 the results achieved from proposed scheme shows the better performance than any previous studies that are shown in Table 1 and it is clearly seen that on average the proposed scheme

Table 8: Comparisons of the embedding capacity (EC) and the (PSNR) visual image quality

Cover Image	**Metrics**	**Wu & Tsai Scheme**	**Shen et al.**	**Xu et al. Scheme**	**K. H. Jung Scheme**	**Proposed Scheme**
Airplane	PSNR	40.06	37.14	37.63	33.19	34.5596
	Capacity	409,778	403,701	960,100	1,050,973	1,053,858
Baboon	PSNR	37.00	36.46	37.66	31.74	36.4730
	Capacity	457,087	458,752	960,100	1,054,327	1,056,768
Boat	PSNR	39.56	36.21	37.69	32.84	33.7846
	Capacity	421,965	408,944	960,100	1,051,124	1,057,008
City	PSNR	40.19	37.34	37.68	32.06	32.3775
	Capacity	421,866	387,834	960,100	1,049,284	1,053,474
Gatbawi	PSNR	36.41	37.38	37.58	30.66	34.3345
	Capacity	459,947	424,673	960,100	1,057,086	1,061,248
Island	PSNR	38.81	36.48	37.66	32.84	35.0146
	Capacity	426,299	416,808	960,100	1,052,513	1,057,748
Lena	PSNR	41.18	36.85	37.64	33.21	33.9879
	Capacity	409,807	406,323	960,100	1,049,742	1,053,094
Man	PSNR	39.09	36.48	37.59	32.72	33.6830
	Capacity	424,585	439,825	960,100	1,052,264	1,053,052
Peppers	PSNR	40.86	39.01	37.67	33.55	35.5479
	Capacity	407,479	397,634	960,100	1,050,571	1,057,260

Embedding capacity incremented range is 0.274% to 0.63 % in each image of dataset. Explicitly on average from KH Jung [19] hybrid scheme embedding capacity is 2.294 % enhanced while from Wu & Tsai scheme [23] up to 113.708%, from Shen et al. scheme [24] it is 112.01% and from Xu et al. scheme [25] up to 156.44% and According to the studies related to this domain of image steganography in digital image processing the visual quality PSNR of the image is denoted as less distortion and exceedingly difficult to detect it by humans with naked eyes if the PSNR is greater than the 30 dB in the human visual system. In Table 1 also shows that the PSNR visual quality range is 1.69 dB to 5.21 dB incremented respectively to the previous studies as well and PSNR is much higher than 33dB on average that is difficult to detect by the human eye. Therefore, based on the above discussion, we can say that the proposed method produces much better/superior results than previous works in sense of better data embedding capacity as well maintaining the good enough visual quality of the stego image simultaneously. Concept behind achieving better results of embedding capacity and PSNR visual quality is by maintain the difference between the pixels basically the proposed scheme is based on hybrid approach of modified techniques of steganography so the classic PVD approach is used to hide the data and generate a new difference so Our proposed framework use that difference to embed more secret data bit using two bit and One bit LSB along with modified difference Expansion to maintain the original difference with closed pixels that will enable to hide maximum amount of data in such a way the similarity index between the stego image and cover image is good enough. Thus, the proposed scheme incorporates the huge amount of important data without any perceived change in the image so proposed framework provides robustness as well. Thus, it is exceedingly difficult for any hacker and the intruder to get access to the original data bits due to its complexity of the framework and due to its higher PSNR value it is obviously appeal less to intruder to detect the difference between the stego image and the cover image. Therefore, the proposed scheme performs much better than the existing schemes.

4.4 Summary

In this Chapter, Proposed Framework (Data encoding, Data extraction) was validated via real world case study. In Section 4.1 secret data was incorporated in the form of bits by using cover image and In Section 4.2 data extracted from stego image. So, step by step procedure was adopted in corresponding sections of this chapter by following the proposed framework and it was demonstrated that the data was successfully incorporated and extracted from the images. Outcomes and the efficiency of proposed framework (encoding, extraction) was evaluated with the previous studies by comparing steganography parameters i.e., embedding capacity and peak signal to noise ratio (PSNR). It was discovered that the novel framework efficiency and results are much better than the reported researches. Thus, proposed framework gives hard hand to hackers and intruder to know about the existence of confidential data.

CHAPTER 5 CONCLUSION AND FUTURE WORK

The chapter contains two sections. In Section 5.1 provides conclusion of Research work. While Section 5.2 discusses about the Future Work Related to Research.

5.1 Conclusion

Data transmission over open networks, such as the Internet, has generated a range of security challenges. Steganography is one of the most powerful techniques of the information security for protecting and hiding the presence of data in a cover of multimedia file or carrier such as image, video, audio files. In this research, while conducting systematic literature review, we explored the existing spatial domain approaches for digital image steganography based on least significant bit techniques, the LSB data hiding method was evaluated and addressed, along with the integration of other related methods such as pixel value difference and difference expansion and evaluate those latest studies where LSB was an integral part of each study. Moreover, another important aspect that are highlighted is that the LSB based image steganography approaches are particularly hard to find in literature. Therefore, there is a dire need that the latest LSB based Image steganography approaches may be explored and summarized. This would definitely aid in the identification of the targeted image steganography regions where contemporary LSB techniques have been used till now. We conducted a series of experiments to see how well the existing studies performed in the domain of steganography in terms of parameters embedding capacity, visual quality, mean square error, CPU consumption, and security. After the extensive exploration while performing the SLR and experimentation of the studies we detected many loopholes and the research areas that need to be consider for further work such as in term of embedding capacity and the visual quality. Based on our findings, observations, and familiarity of how different image steganography algorithms work, then we introduced a new steganography framework that comprises primarily of three main techniques of digital image steganography approaches that can be used separately or in combination for greater versatility. In this work, a new hybrid data embedding, and extraction framework is proposed that is combination of modified PVD, LSB and DE approach for enhancing the secret data embedding in such a way that the similarity index or a visual quality of the stego image should be maintained that are measured in term of PSNR. The proposed scheme uses PVD, LSB and DE schemes simultaneously and hides the secret data in the pair pixel differences and maintaining the difference by using RDE to achieve high embedding capacity and visual quality.

According to the studies related to this domain of image steganography in digital image processing the visual quality PSNR of the image is denoted as less distortion and very difficult to detect it by humans with naked eyes if the PSNR is greater than the 30 dB in the human visual system. In Table 1 also shows that the PSNR visual quality range is 1.69 dB to 5.21 dB incremented respectively to the previous studies as well and PSNR is much higher than 33dB on average that is difficult to detect by the human eye. Achieved results shows also that the data embedding capacity of the proposed scheme is also enhanced and increased in the range of 0.27% to 0.63% in each image from dataset and the existing K. H. Jung scheme, respectively. Main Concept behind achieving better results are also discussed in Chapter 4 in term of embedding capacity and PSNR visual quality is by maintain the difference between the pixels basically the proposed scheme is based on hybrid approach of modified techniques of steganography so the classic PVD approach is used to hide the data and generate a new difference so Our proposed framework use that difference to embed more secret data bit using two bit and One bit LSB along with modified difference Expansion to maintain the original difference with closed pixels that will enable to hide maximum amount of data in such a way the similarity index between the stego image and cover image is good enough. Thus, the performance of the proposed scheme is more efficient and better than any existing work that is mentioned in Table 1 in terms of both data hiding capacity and image quality by hiding a large amount of secret data without any perceived change in the image.

5.2 Future Work

As a future work, I will make sure to enhance the proposed image steganographic system further. I plan to incorporate the more numbers of secret data bits adaptively and in order to do this I will modify the pixel value difference approach by changing and restricting the levels of the range table to hide minimum and maximum of 5 bits instead of 3 bits .That will obviously increase the embedding capacity but effect on the visual quality so in order to improve the visual appearance of the stego image .I will apply the histogram adjustment technique in such a way that the histogram of stego image should be almost near to the original cover image that will not only enhance the visual quality but also prevent from active and passive attacks like statistical and visual attacks from the hackers or intruders.

5.3 Summary

In this Chapter, Overall concepts of research work was summarized that describe the novel contribution in image steganography area by enhancing the embedding capacity and the visual quality of the images while hiding the secret data. In section 6.2 Future Work was discussed to incorporate more secret data by restricting the levels in PVD and do histogram adjustment to get better visual quality in future.

REFERENCES

[1] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319263.

[2] M. S. Sreekutty and P. S. Baiju, "Security enhancement in image steganography for medical integrity verification system," 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, 2017, pp. 1-5, doi: 10.1109/ICCPCT.2017.8074197.

[3] K. S. Seethalakshmi, Usha B A and Sangeetha K N, "Security enhancement in image steganography using neural networks and visual cryptography," 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, 2016, pp. 396-403, doi: 10.1109/CSITSS.2016.7779393.

[4] E. Gedkhaw, N. Soodtoetong and M. Ketcham, "The Performance of Cover Image Steganography for Hidden Information within Image File using Least Significant bit algorithm," 2018 18th International Symposium on Communications and Information Technologies (ISCIT), Bangkok, 2018, pp. 504-508, doi: 10.1109/ISCIT.2018.8588011.

[5] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 2016, pp. 400-404, doi: 10.1109/CIST.2016.7805079.

[6] Y. Yiğit and M. Karabatak, "A Stenography Application for Hiding Student Information into an Image," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-4, doi: 10.1109/ISDFS.2019.8757516.

[7] A. AlWatyan, W. Mater, O. Almutairi, M. Almutairi, A. Al-Noori and S. Abed, "Security approach for LSB steganography based FPGA implementation," 2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Sharjah, 2017, pp. 1-5, doi: 10.1109/ICMSAO.2017.7934929.

[8] A. Arora, M. P. Singh, P. Thakral and N. Jarwal, "Image steganography using enhanced LSB substitution technique," 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, 2016, pp. 386-389, doi: 10.1109/PDGC.2016.7913225.

[9] O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2020, pp. 131-135, doi: 10.1109/ICIoT48696.2020.9089566.

[10] X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, 2016, pp. 1-4, doi: 10.1109/ICIS.2016.7550955.

[11] Stella D. Muyco and Alexander A. Hernandez. 2019. A Modified Hash Based Least Significant Bits Algorithm for Steganography. In Proceedings of the 2019 4th International Conference on Big Data and Computing (ICBDC 2019). Association for Computing Machinery, New York, NY, USA, 215–220. DOI:https://doi.org/10.1145/3335484.3335514

[12] G. G. Rajput and Ramesh Chavan. 2017. A Novel Approach for Image Steganography based on LSB Technique. In Proceedings of the International Conference on Compute and Data Analysis (ICCDA '17). Association for Computing Machinery, New York, NY, USA, 167–170. DOI:https://doi.org/10.1145/3093241.3093247

[13] Antoniya Tasheva, Zhaneta Tasheva, and Plamen Nakov. 2017. Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretching. In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech'17). Association for Computing Machinery, New York, NY, USA, 233–240. DOI:https://doi.org/10.1145/3134302.3134325

[14] Mark Rennel D. Molato and Bobby D. Gerardo. 2018. Cover Image Selection Technique for Secured LSB-based Image Steganography. In Proceedings of the 2018 International Conference on Algorithms, Computing and Artificial Intelligence (ACAI 2018). Association for Computing Machinery, New York, NY, USA, Article 17, 1–6. DOI:https://doi.org/10.1145/3302425.3302456

[15] S. Sugathan, "An improved LSB embedding technique for image steganography," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 609-612, doi: 10.1109/ICATCCT.2016.7912072.

[16] Bhardwaj, R., &amp; Sharma, V. (2016). Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution. Procedia Computer Science, 93, 832-838. doi:10.1016/j.procs.2016.07.245

[17] C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and securing message on edge areas of image using LSB steganography and OTP encryption," 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), Semarang, 2017, pp. 1-6, doi: 10.1109/ICICOS.2017.8276328.

[18] Cem kasapbaşi, M., Elmasry, W. New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. Sādhanā 43, 68 (2018). https://doi.org/10.1007/s12046-018-0848-4

[19] Jung, K. Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. J Real-Time Image Proc 14, 127–136 (2018). https://doi.org/10.1007/s11554-017-0719-y

[20] Gutub, A., Al-Shaarani, F. Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. Arab J Sci Eng 45, 2631–2644 (2020). https://doi.org/10.1007/s13369-020-04413-w

[21] Abbas Cheddad Joan Condell, Kevin Curran and Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing Elsevier Volume 90, Issue 3, March 2010, Pages 727-752

[22] Kitchenham, B. 2004. Procedures for Performing Systematic Reviews. Elsevier. (July 2004)

[23] Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10), 1613–1626. doi:10.1016/s0167-8655(02)00402-6

[24] Shen S, Huang L, Tian Q (2015) A novel data hiding for color images based on pixel value difference and modulus function. Multimedia Tools Application 74(3):707–728

[25] Xu WL, Chang CC, Chen TS, Wang LM (2016) An improved least-significant-bit substitution method using the modulo three strategy. Displays 42:36–42

[26] The USC-SIPI Image Database: http://sipi.usc.edu/database/. Access on July 2020.

[27] Lin. 2011. An information hiding scheme with minimal image distortion.Comput. Stand. Interfaces 33, 5 (September, 2011), 477–484. DOI:https://doi.org/10.1016/j.csi.2011.02.003

[28] Tian, Jun. "Reversible data embedding using a difference expansion." IEEE transactions on circuits and systems for video technology 13.8 (2003): 890-896.

[29] J Y Hsiao, K F Chan, J. M Chang. “Block-based reversible data embedding”. Signal Processing, 89(4) (April 2009) Pages 556-569

[30] J. Tian, “Wavelet-based reversible watermarking for authentication,” in Security and Watermarking of Multimedia Contents IV—Proc. SPIE, E. J. Delp III and P. W. Wong, Eds., Jan. 2002, vol. 4675, pp. 679–690.

[31] Cheng-Hsing Yang, Shiuh-Jeng Wang, and Chi-Yao Weng. 2007. Analyses of Pixel-Value-Differencing Schemes with LSB Replacement in Stegonagraphy. In Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) - Volume 01 IEEE Computer Society, USA, 445–448.

[32] A. R. Madane and R. Khare, “Time domain steganography,” in Proc. International Workshop on Machine Intelligence Research, 2009.

[33] C. H. Huang, S. C. Chuang, and J. L. Wu, “Digital invisible ink and its applications in steganography,” in Proc. 8th Workshop on Multimedia and Security, 2006.

[34] J. Nazario, Defense and Detection Strategies against Internet Worms. Artech House, 2004.

[35] J. Mielikainen, “LSB matching revisited,” IEEE Signal Processing Letters, vol. 13, no. 5,pp. 285–287, 2006.

[36] X. Li, B. Yang, D. Cheng, and T. Zeng, “A generalization of LSB matching,” IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69–72, 2009.

[37] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and Genetic algorithm,” Pattern Recognition, vol. 34, no. 3, pp. 671–683, 2001.

[38] C. K. Chan and L. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.

[39] C. C. Chang, Y. H. Huang, H. Y. Tsai, and C. Qin, “Prediction-based reversible data hiding using the difference of neighboring pixels,” International Journal of Electronics and Communications, vol. 66, no. 9, pp. 758–766, Sep. 2012.

[40] N. Kafri and H. Y. Suleiman, “Bit-4 of frequency domain-DCT steganography technique,” in Proc. 1st International Conference on Networked Digital Technologies, 2009.

[41] J. Mandal, “A frequency domain steganography using Z transform,” in Proc. International Workshop on Embedded Computing and Communication System, 2011.

[42] A. Westfeld and A. Pfitzmann, “High capacity despite better steganalysis (F5–a steganographic algorithm),” in Proc. 4th International Workshop on Information Hiding, Pennsylvania, USA, 2001.

[43] N. Provos, “Defending against statistical steganalysis,” in Proc. 10th USENIX Security Symposium, 2001.

[44] Q. Liu and A. H. Sung, “Feature mining and nuero-fuzzy inference system for steganalysis of LSB matching steganography in grayscale images,” in Proc. 20th International joint Conference on Artificial Intelligence, 2007.

[45] T. Pevný and J. Fridrich, “Merging Markov and DCT features for multi-class JPEG steganalysis,” in Proc. Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, USA, 2007.

[46] E. Zheng, X. Ping, T. Zhang, and G. Xiong, “Steganalysis of LSB matching based on local variance histogram,” in Proc. 17th IEEE International Conference on Image Processing, Hong Kong, 2010.

[47] A. D. Ker, “Steganalysis of LSB matching in grayscale images,” IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441– 444, Jun. 2005.

[48] S. Gunawardena, D. Kulkarni and B. Gnanasekaraiyer, "A Steganography-based framework to prevent active attacks during user authentication," 2013 8th International Conference on Computer Science & Education, Colombo, Sri Lanka, 2013, pp. 383-388, doi: 10.1109/ICCSE.2013.6553942.

[49] M. A. Usman, S. Y. Shin, M. Shahid, & B. Lövström, “A no reference video quality metric based on jerkiness estimation focusing on multiple frame freezing in video streaming,” IETE Technical Review, Vol. 34, No. 3, pp: 309 – 320, May 2017.

[50] Huaiqing Wang and Shuozhong Wang. 2004. Cyber warfare: steganography vs. steganalysis. Commun. ACM 47, 10 (October 2004), 76–82. DOI:https://doi.org/10.1145/1022594.1022597

[51] A. K. Singh, N. Sharma, M. Dave and A. Mohan, "A novel technique for digital image watermarking in spatial domain," 2012 2nd IEEE International Conference on Parallel,

Distributed and Grid Computing, Solan, India, 2012, pp. 497-501, doi: 10.1109/PDGC.2012.6449871.

[52] T. Furon and P. Duhamel, "An asymmetric watermarking method," in IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 981-995, April 2003, doi: 10.1109/TSP.2003.809376.

[53] L. Kothari, R. Thakkar and S. Khara, "Data hiding on web using combination of Steganography and Cryptography," 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 2017, pp. 448-452, doi: 10.1109/COMPTELIX.2017.8004011.

[54] K. Joshi and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, India, 2015, pp. 86-90, doi: 10.1109/ICIIP.2015.7414745.

[55] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326.

[56] Indrayani, Rini, Hanung Adi Nugroho, and Risanuri Hidayat. "An evaluation of MP3 steganography based on modified LSB method." 2017 International Conference on Information Technology Systems and Innovation (ICITSI). IEEE, 2017.

[57] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205). Vol. 3. IEEE, 2001.

[58] McBride, Brent T., Gilbert L. Peterson, and Steven C. Gustafson. "A new blind method for detecting novel steganography." (2005): 50-70.

[59] S. Sriram, B. Karthikeyan, V. Vaithiyanathan and M. M. Anishin Raj, "An approach of cryptography and steganography using rotor cipher for secure transmission," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 2015, pp. 1-4, doi: 10.1109/ICCIC.2015.7435669.

[60] H. R. Sah and G. Gunasekaran, "Privacy preserving data mining using visual steganography and encryption," 2015 10th International Conference on Computer Science & Education (ICCSE), Cambridge, UK, 2015, pp. 154-158, doi: 10.1109/ICCSE.2015.7250234.

[61] Begum, M. Baritha, and Y. Venkataramani. "LSB based audio steganography based on text compression." Procedia Engineering 30 (2012): 703-710.