AN ENHANCEMENT OF IMAGE STEGANOGRAPHY BASED ON A PVD AND MODULO OPERATION USING HISTOGRAM ANALYSIS

A Thesis Submitted
in Partial Fulfillment of the Requirements
for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

by

MONIKA SHARMA
(Enrollment No. 150191004156)

Under the Supervision of
Mr. Manoj Kumar Sharma
Marathwada Institute of Technology, Bulandshahr

to the

FACULTY OF COMPUTER SCIENCE AND ENGINEERING

DR. APJ ABDUL KALAM TECHNICAL UNIVERSITY
LUCKNOW
(Formerly Uttar Pradesh Technical University, Lucknow)

July, *2021*

DECLARATION

I hereby declare that the work presented in this dissertation entitled "AN ENHANCEMENT OF IMAGE STEGANOGRAPHY TECHNIQUE BASED ON A PVD AND MODULO OPERATION" was carried out by me. I have not submitted the matter embodied in this dissertation for the award of any other degree or diploma of any other University or Institute.

I have given due credit to the original authors/ source for all the words, ideas, diagrams, graphics, computer programs, experiments, results, that are not my original contribution. I have used quotation marks to identify verbatim sentences and given credits to the original authors/ sources.

I affirm that no portion of my work is plagiarized, and the experiments and results reported in the dissertation are not manipulated. In the event of a complaint of plagiarism and the manipulation of the experiments and results, I shall be fully responsible and answerable.

Name : Monika Sharma

Enroll No. : 150191004156

Field : CSE

(Candidate signature)

CERTIFICATE

Certified that **Monika Sharma** (1900190105002) has carried out the research work presented in this thesis entitled "**An Enhancement of Image Steganography Technique based on a PVD and Modulo Operation Using Histogram Analysis"** for the award of **Master of Technology** from Marathawada Institute of Technology, Bulandhshahr, affiliated to DR. APJ Abdul Kalam Technical University Lucknow (Formerly Uttar Pradesh Technical University Lucknow) under our supervision. The thesis embodies results of original work, and studies are carried out by the student himself and the contents of the thesis do not from the basis for the award of any other degree to the candidate or to anybody else from this or any other University/ Institution.

Signature

Mr. Manoj Kumar Sharma

Assistant Professor

Computer Science and Engineering

Marathwada Institute of Technology, Bulandshahr

Date:

AN ENHANCEMENT OF IMAGE STEGANOGRAPHY BASED ON A PVD AND MODULO OPRATION USING HISTOGRAM ANALYSIS

MONIKA SHARMA

ABSTRACT

Environment of digital world internet is the one of the network area that not uses proper secure link for transmit information one way to another way. On the basis of digital world, security of information will be high and diminish the attacks during the sending information from host to sender. Now have a solution for this problem. So Steganography is one of the possible solutions for such types of problems. Many kinds of steganography techniques in system security, Digital image steganography is very easiest and important method to solve this problem.

In historical, many steganography methods and techniques had been used. In 2008, Yu et al. have discussed a image Steganography technique based on 2^k correction and edge detection, Ghosal [2011] discusses Steganography technique using pair wise bit based data hiding approach. Least Significant Bits (LSB) method is a broad range of embedding algorithm. LSB method embed secret bit in the least significant position of an image. This research work in an enhance security of image steganography. The desire goal is to improve image quality and protect data during the transmission.

This research work analyzes the various techniques including above mentioned Ones used for information hiding, their applications and their drawbacks. Now here propose a new enhance method- " **A Enhancement of Image Steganography Technique Based on a PVD and Modulo Operation using Histogram Analysis".** In the proposed technique, image steganography techniques are using the principle of pixel differencing modulo operation (PDMO) and average pixel value differencing (APVD). The main motive of the proposed approach is: (i) increase image quality, (ii) increase peak signal to noise ratio (PSNR), (iii) increase in hiding capacity, (iv) Avoid fall off boundary problems (FOBP). At first, histogram of the three channels RGB of the given color image is generated. The histograms are compared with that of the secret bit. The channel whose histogram matching the most with that of the secret bit is

selected to get the difference value of channel pixels and the secret bit to be embedded in RGB channels. This process leads to be high hiding capacity for the given pixels. In RGB channel, we consider five non- consecutive pixels from last two channels. First three pixels are considered from Blue Channel and last two pixels are considered from Green channels.

Then, the secret bit to be embedded in a pixel using three phases, first is Pixel Difference Modulo Operation (PDMO), second is Average Pixel Value Differencing (APVD) and the last is Pixel Value Difference (PVD). Now compute distinguish in pixel values and then apply modulus, so that we can determine the value of the difference using certain rules. This value is then used to embed the binary bits. And the last proposed method has higher PSNR value (more than 40db), increase hiding capacity, low MSE value.

ACKNOWLEDGEMENT

I would like to convey my sincere gratitude to my mentor, supervisor and guide Mr. Manoj Kumar Sharma, Assistant Professor, Department of Computer Science and Engineering, MIT, Bsr (UP) for their invaluable constant supervision and appreciation during the entire research work and preparation of manuscript.

I would also like to convey my reverence to my dear ones for their inspiration and encouragement helped me tide over the difficulties I had during the project.

Monika Sharma

Roll no. 1900190105002

TABLE OF CONTENT

List of Figures

List of Tables

List of Abbreviations

LSB	Least Significant Bit
MSE	Mean Square Error
PVD	Pixel Value Differencing
PSNR	Peak Signal Noise Ratio
APVD	Average Pixel Value Differencing
FOBP	Fall off Boundary Problem
MO	Modulo Operation
MPVD	Multi Pixel Value Differencing
EMD	Exploiting Modification Direction
PDH	Pixel Difference Histogram
PDMO	Pixel Difference Modulo Operation
BPP	Bit Per Pixel
DB	Decibel

CHAPTER 1

INTRODUCTION

1.1 Security System

Security system means that information can be protected from hacker (third party), in this the frequently terms are Computer Security and Information assurance. The information security is valuable for any organization which is provided by physical and administrative area. Initially, the Computer had less or no security that can be continued till the data importance was not realized.

Following is the example based on security mechanism:-

Firstly, User id and password is provided to all user and check the information provided by the user is authentic or not.

Secondly, Encrypted information is stored in database in particular manner, which is not visible to the user who does not have authentic permission.

In recent years, Information security grew and opens out outstandingly. The area of Specialization including security testing, securing network etc.

There are three main component used in security system:

i. Encrypt is uses for authenticity, secrecy and integrity.
ii. Digital signatures to protect information and provide corroborate, integrity and non-resident.
iii. Hashing algorithm uses to protect substantiate data and provide probity.

1.2 Basic Principles of Information Security

Some important principles for security system as shown in **Fig. 1.1**

Fig. 1.1: Principles of Information Security [1]

1.2.1 Confidential System

The Principal of confidentiality means covertness tells that only the sender and the voluntary receivers should be capable to access the content of data.

1.2.2 Integrity System

Two persons/clients (P and Q) will like to make sure that no other one can alter with the same contents of the check/ inspect (like as its amount value), data, sign etc.

1.2.3 Availability System

The principal of availability shows that resource which is information must be available to only authorized practice all the times.

1.2.4 Authenticity System

In Authentication System which helps to an initiate proof the identifications. In this authenticity process make sure to that the source of computerized message or information is correct identified.

1.2.5 Non-repudiation System

Rules and regulation if system security, non-repudiation suggest one intention to fill up his responsibility to content. It does not permit to sender of a message to disprove (refute) the declare is not sending that message.

1.3 Information Hiding Techniques

There are many techniques developed for secure data, control unauthorized data access etc. So Now some other new hiding techniques categorized for more secure data as compare to other techniques.

1. Cryptography Hiding Technique
2. Watermarking Hiding Technique
3. Steganography Hiding Technique

1.3.1 Cryptography Hiding Technique

Cryptography Hiding Technique is divided into two manners: "crypto" and "graphic". Crypto means "art" and graphic means "writing/content" i. e. the art of writing and contents. It is the information and communication behavior in the presence of adversarial behavior. In cryptography text message encode with the help of Keys. It is the conversion of original text to plain text vice-versa. The key will be private key as well as public key.

Cryptography technique show in **Fig. 1.2**

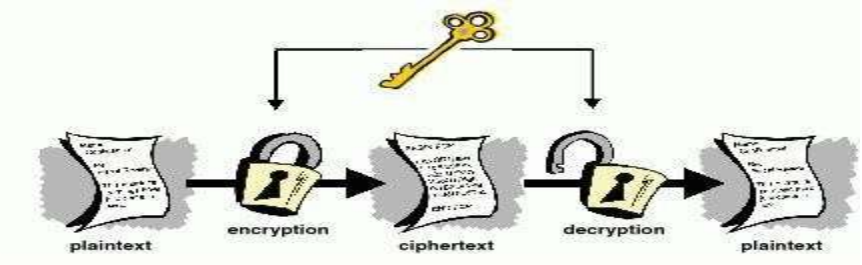


Fig. 1.2: Cryptography Concept

1.3.2 Steganography Hiding Technique

The meaning of steganos is concealed and meaning of graphia is writing. So we can say that steganography is covered writing.

1.3.2.1 Assumption of Steganography

Two assumptions according to steganography are as**:**

1. The digital image or voice changed to definite scope without reason any detectable effect to hide data in them is on them

2. The capability of human to differentiate minimum changes in color image and sound quality we can change the pixel value of an image and produced the similar image that human cannot find the detectable changes of images color.

1.3.2.2 Steganography Embedding Process

Steganography embedding process is process in which secret message/ data to be embed in cover/ original image and gives stego-image. Secret data to be any text, binary bits etc. Process will be shown in Fig. 1.3.

Firstly, original image or cover image will be selected and it passes to encode with secret data through the key. Secondly, stego-image decodes by key and generates original image and secret data.

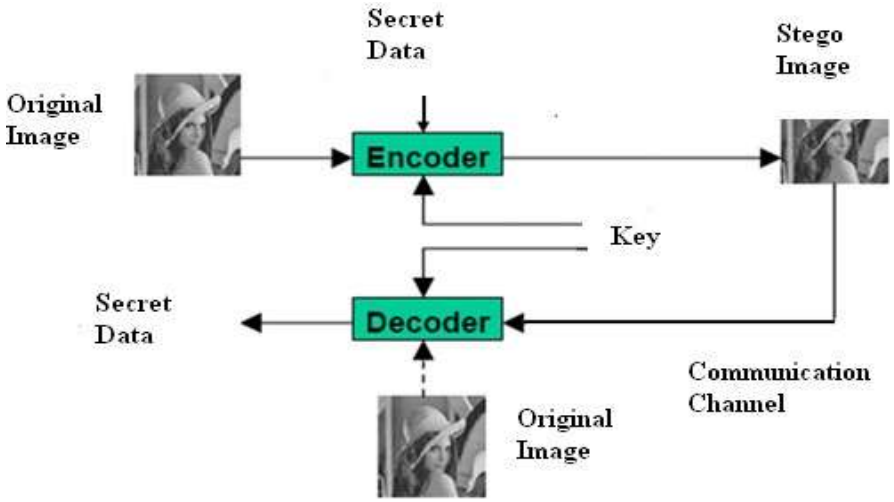


Fig. 1.3 Generic Processes of Encoding and Decoding

A secret key basically use in the cryptographic process. The key may be public key or private key, according to these key we can encrypt the data with the using of private key and receiver side decrypt the data with using of public key.

According to this technique hacker cannot get the secret data.

1.3.2.3 Different Kinds of Steganography

In Fig. 1.4 there are four important methods of file format uses in steganography.

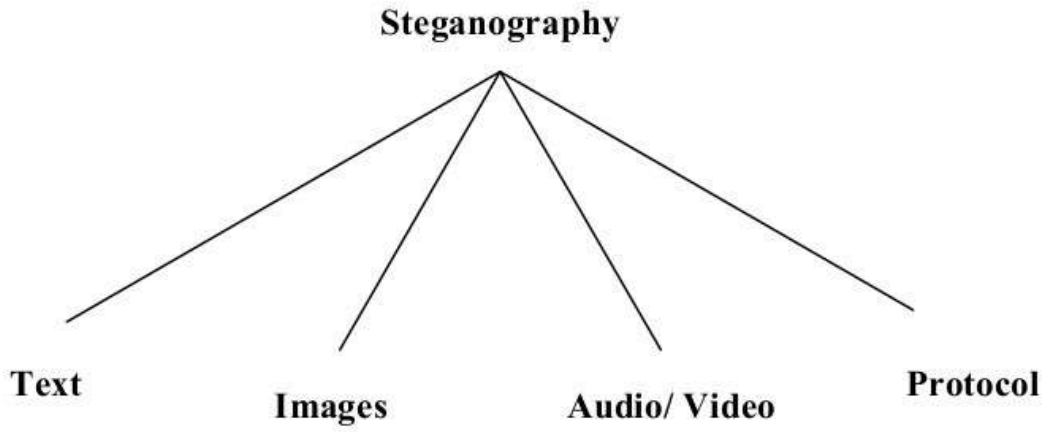


Fig. 1.4: Kinds of Steganography

Process of hiding of data in the form of text is a most important technique of steganography. According to above method we can hide a secret data in every p^{th} alphabets of every words of a text data. Basically text steganography is a traditional technique. It is no more secure comaprision to image, video and audio steganography.

1.4 Requirements of Data hide

The different rule and insertion method which ready to hide the data in a specific image. For applying steganography techniques correctly, we must satisfy the number of requirement of all protocol and techniques.

• When the data is hidden then we cannot change any extra information and cannot lose any information.

• Any stego-image cannot be changed but if any changes happens in stego-image so it means that unauthorized person access it.

• Always we suppose that the attacker knows that the stego object has invisible information inside it.

1.5 Motivation

Many of image steganography techniques method have been proposed in the literature survey. On the basis of previous work we need to improve image quality that both image (original image and stego-image) look same.

In Dissertation –**An Enhancement of Image Steganography Technique Based on a PVD and modulo operation Using Histogram Analysis** has been proposed to increase quality of stego image and provide good results as compare previous steganographic technique.

The method will be test by well known parameters namely PSNR, FOBP, MSE, BPP (Bits per Pixel).Value of PSNR are higher than the MSE value. In that case, quality of an image increases.

1.6 Problem Statement

For increasing image quality and data hiding capacity we study some important statements about many security problems.

- To research various convenient image steganography techniques.
- To research Histogram Analysis of cover image.
- To research characteristic parameters for both cover image and stego-image.
- Calculate average pixel value differencing between two images (cover and stego).
- To study how to avoid fall off boundary problem (FOBP).

1.7 Objectives of This Dissertation

In our dissertation, various steganography techniques have been studied. **An Enhancement of Image Steganography Technique Based on a PVD and Modulo Operation using Histogram Analysis** is proposed.

- To research some convenient digital image steganography techniques.
- To research Histogram Analysis of cover image in PVD.
- To research characteristics parameters of the cover image and stego-image.
- Calculate average pixel value differencing between two images (cover and stego).
- To study how to avoid fall off boundary problem (FOBP).

1.8 Proposed Framework for This Research

In this research the proposed framework on **MATLAB (2020a).**

In thesis, proposed approach increase the quality parameters like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), fall off Boundary Problem (FOBP), hiding capacity and Bits per Pixels (BPP) based on a RGB channel.

In these techniques, we consider five pixels from RGB channel, first three pixels consider from Blue channel and last two pixels consider from Green channel. In Blue channel we apply Pixel difference modulo operation (PDMO) and Average pixel value difference (APVD). Green channel pixels are used pixel value difference (PVD) [11]. The results show that high PSNR value, Lower MSE value, increasing hiding capacity, avoiding fall off boundary problems and improving image quality.

In this dissertation the proposed work divide in following three phase:

- Histogram Analysis
- Embedding Process Technique
- Extraction Technique

1.9 Dissertation Organization

The outline of this dissertation is as follows:

In chapter 2, Firstly we discuss the category of Steganography used i.e. Image Steganography and the types of image representation domains of which the spatial domain is focused, various spatial domain image Steganography techniques from 2003-2019 has been discussed, and quality metrics (PSNR, MSE) and data hiding capacity both techniques are compared for analysis of their merits and demerits. On the basis of these demerits we proposed new Steganography technique which is discussed in Chapter 3. Furthermore the code for the proposed scheme is developed by using Matlab2020a for image encoding and decoding.

In chapter 4, Result of the proposed approach and analyze using PSNR, MSE, FOBP, BPP and capacity by taking different size of secret message. Also compare the results of the proposed scheme with those some of the important Steganography techniques.

In chapter 5, the conclusions and future scope discuss on the basis of thesis.

CHAPTER 2

LITERATURE REVIEW

2. 1 Introduction

Fast enhancement in the field of computer science technology and Internet, one of the most important factors is information security. It is needed to take suitable step to protect the information.

There are three ways for hiding the secret information like cryptography, digital water marking and steganography. For authenticity, Digital water marking is used. Cryptography technique and Steganography technique are used for confidentiality and integrity.

There are many techniques in steganography like Text, image, audio and video. The main important method is image steganography. The Steganography is most common technique to us.

2.1.1 Image Steganography

Image steganography is most important technique in steganography. In this technique there are many file formats exists.

Image Definition

Image is a combination of RGB channel and each channel represent pixel matrix. And these pixel values show horizontally row by row. The bit depth ia an number of bits in RGB channel. The minimum bit depth in present color is 8-bit, means 8-bit is used to describe the each pixel of color. Basically 24 bit color size of each digital color images in RGB color model.

2.2 Image Representation Domain

Image Steganography approach can split into two groups (Image Domain and Transform Domain). Image domain merges messages in the intensity of the pixels directly, while for transform also known as frequency domain, images are first transformed and then the message is embedded in the image.

This image representation also called spatial domain. Examples of some steganographic algorithms explained, image file formats and the domain in which they are performed are discussed below. Fig. 2.1 demonstrates various categories of image Steganography.

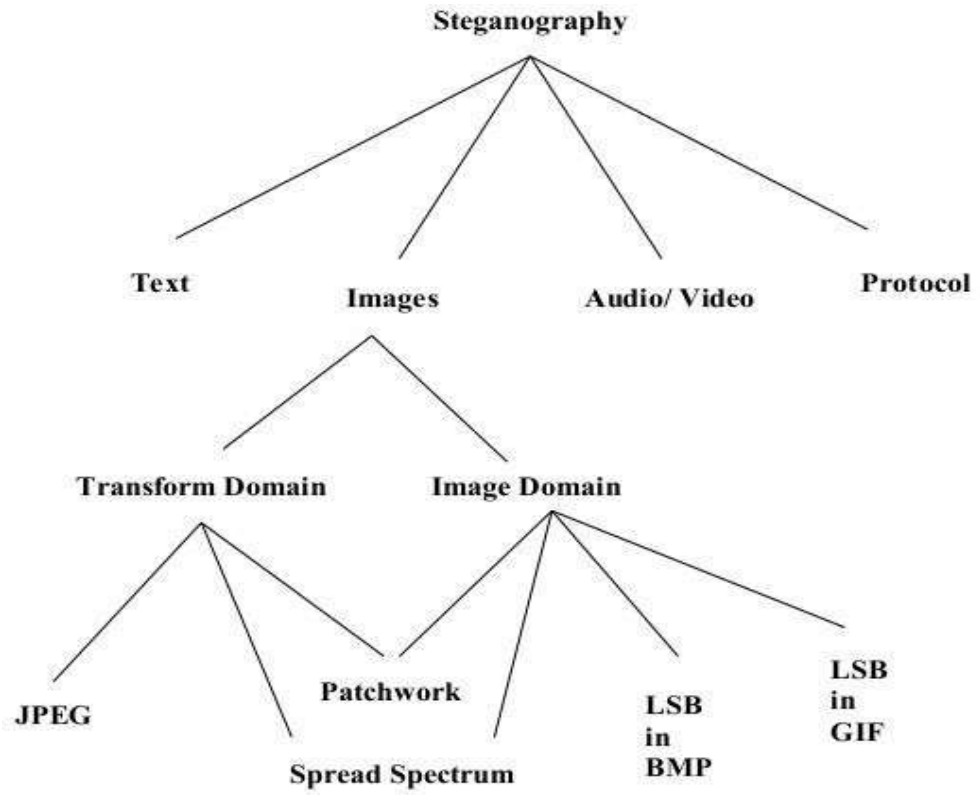


Figure 2.1: Classification of Image Steganography

2.2.1 Frequency Domain

Frequency Domain used for thrashing extra amount of data and provides giant security. It is used to change of algorithms and image transformation. This technology used to hide a message in more powerful area of the original image and create it stronger. Many frequency domain technologies are merge message and may create alterning between lossy and lossless compression.

2.2.2 Spatial Domain

Spatial domain method uses bitwise technique for applies bit insertion and noise handling. Image structure is premier for spatial domain. Steganography are lossless and the method fully depending on the image structure.

2.3 Spatial Domain Image Steganography Techniques

We explain steganography techniques in spatial domain image that are fully based on Least Significant Bit substitution, modulo operation, data hiding approach and pixel value differencing.

2.3.1 Least significant bit (LSB) substitution Method to Embed Image

Lie and Chang (1999) have given technology for embedding interactive media (consist of audio, image, video, or text compressed or non-compressed) into a server-side image. In this method, gray value pixel of cover image after embedding is beyond the human perception. The hiding capacity is increased by finding the adaptive numbers of LSBs to be changed. As, traditional LSB method hides data in a fixed number of LSBs of an image pixel thus, more the LSBs are changed the higher distorted image we get.

LSB-mapping function N (g), which gives the number of LSBs that can be embedded for each possible gray level g, is to be devised. Basically, the function N (g) is made piecewise step i.e.

$$N(g) = \begin{cases} 1 & 0 \le g < k_1 \\ 2 & k_1 \le g < k_2 \\ 3 & k_2 \le g < k_3 \\ 4 & k_3 \le g < 256 \end{cases}$$

Values four are not examining since interchanges of too many LSBs are as to produce result in perceivable change in image contrast. This procedure is main to determine the decision boundaries k1~ k3, which is explained in the following Table 2.1.

Table 2.1 Decision boundaries value

K_i	Interval	Number of LSBs used
	None	1bit
0	0~87	2bit
88	88~191	3bit
192	192~255	4bit

e.g.: Take g = 87 whose binary value is 01010111 lies in the range of k1 ~ K2, thus the number of LSBs changed that are used to embed the data are 2bits. It can hide great amount of bit (about 30%-45% of the host image) is embedded without severe degradation of the image quality (31-40 dB, depending on the volume of embedded bits). Thus, the stego image quality can be improved in near future.

2.3.2 Pixel Value Differencing (PVD) and LSB replacement Steganography

Wu et al. (2003) [11] have used technique Least Significant Bit (LSB) replacement and Pixel Value Differencing (PVD) methods in steganography. This approach uses gray scale value which is lie on 0-255. The main goal of this technique is to improve and increase image quality, hiding capacity. Data to be embed by using LSB and PVD method. There are two pixels consider for embedding data and performed by PVD approach. Differences between two pixels are carried in smooth and edge area . Smooth area of pixel embed by LSB and an edge area embed by embed by using proposed method. Lower- level and Upper- level determine how many secret bits to be embed in pixel blocks.

Flowgraph of proposed method is given in the Fig. 2.2.

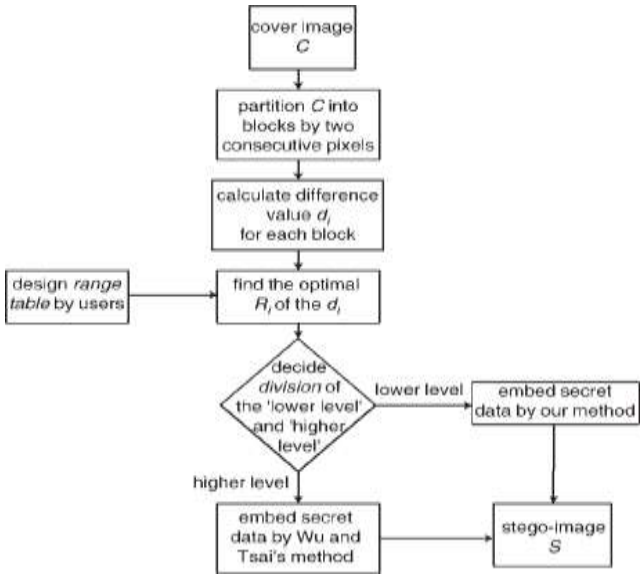


Fig. 2.2: Flowchart of the LSB replacement and PVD algorithm

The experimental results are based on the PSNR value and hiding capacity compared with the PVD methods being used alone are shown below in the Table 2.2,. PSNR value much high so proposed method used some new steganogarphy technique for increase image quality and hiding capacity.

Table 2.2: Result of the proposed and Wu-Tsai's methods

Image	**Wu-Tsai's Method PSNR(db)**	**Proposed Method PSNR(db)**
Baboon	33.43	40.1430
Peppers	37.07	44.0703
Lena	38.94	42.6485

2.3.3 PVD in multimedia images

Yang et al. (2008) work on pixel value difference for four non-concecutive pixel blocks. In this multimedia approach, hiding capacity will be improved. This approach is also called adjacent Pixel value difference. AdPVD determine adjacent pixels in form of low-level, middle-level and high-level. In case of different intervals location of pixels, secret message lie on 3, 4, and 5 bits.

2.3.4 PVD and LSB approach on steganography

Khodaei and faez (2010) proposed both methods to embed the secret bit into three non-successive pixels. The "k" numbers of secret message to be embed into starting two pixels calculate difference between two pixels and know about how many bits to be hide in cover image pixels. The difference is calculated by the lower and higher level of range value. Lower and higher value will be finding by range of pixels. After determine secret bit and embed in pixel, it generate higher PSNR value. In Table 2.3 show the PSNR value of proposed method and khodaei & faez.

Table 2.3 Proposed method and Khodaei & Faez(PSNR)

Images	**Proposed Method PSNR**	**Khodaei & Faez PSNR**
Girl	42.64	36.41
Baboon	40.14	36.27
Peppers	44.07	38.06
House	41.39	37.31

2.3.5 LSB Substitution, PVD and EMD in Steganography

Anita Pradhan (2017) has using steganography technique to embed two different pixel block image and calculate quality parameters. The key idea to this approach is that to protect two hybrid images by pixel difference, histogram analysis and RS analysis. According to embedding process, PDH analysis and RS analysis have not detected. It improves PSNR value and hiding capacity of image.

2.4 Comparison of the Proposed Methods

According to the below table, PSNR value and hiding capacity calculates based on pixel value difference techniques. PSNR value is higher than the other steganography methods. For improve quality of image and increase hiding capacity we use other new steganography methods for generate higher PSNR value.

Table 2.4 PSNR values for various methods

Images	LSB3	PVD	W.N. Lie's	J.G. Yu's
Airplane	40.87	40.6	37.71	39.31
Airport	40.85	37.2	42.64	43.36
Baboon	40.84	37.58	40.55	42.03
Boat	40.86	39.59	40.87	42.18
Lena	40.89	41.58	40.36	42.09
Man	40.9	39.18	41.54	42.65
Peppers	40.86	41.66	40.27	41.47
Stream	41.21	37.9	41.91	42.59

2.5 Comparison Quality and Hiding Capacity for Different Steganography

Table 2.5 Comparison Results of Quality of Image and Hiding Capacity for Different Steganography Techniques

Cover image	Embedding Image	LSB Technique	PVD Techniques	Proposed Techniques
1024*1024	102*102	PSNR	PSNR	PSNR
Animal1	Julogo.bump	786432	1204965	1413360
Animal 2	Julogo.bump	786432	1224055	1413360
Animal 3	Julogo.bump	786432	1233665	1456352
Animal 4	Julogo.bump	786432	1233665	1541242

2.6 SUMMARY

We discuss about different types of steganography used i.e., Image steganography and the types of image representation domains of the the spatial domain in focused, various spatial domain image steganography techniques from 2003-2017 has been discussed are shown in table 2.5 and on the basis of PSNR value and hiding capacity.

- As, the MSE error is large thus the PSNR of the following techniques lies between 30dB - 45dB. (Note: on scale of 10log.)
- The capacity to hide the data is open future work, with these techniques.
- The following techniques embedding the data in original image pixels thus the security issues to transfer the data are less reliable.

CHAPTER 3

PROPOSED METHOD

In this chapter proposed algorithm is used on Modules operation (MO), Pixel value differencing (PVD) and Average pixel value differencing (APVD) readjustment with the using of histogram analysis which enhances the quality parameters of Peak Signal to Noise Ratio (PSNR), hiding capacity, Bits per pixel (BPP) and Mean Square Error (MSE). In this technique, security features are more reliable as compare to other steganography techniques. It also provides security using Pixel differencing modulo operation (PDMO). This proposed approach can encode any image files into RGB channel. Secret bit to be embedding on the basis of difference of channel pixels. In RGB channel we consider only Green and Blue channel to embedding secret bit. Green and Blue channel are both dark channel as compare to Red channel that's why we consider these channel. Second channel pixels are used pixel difference modulo operation (PDMO) and average pixel value difference (APVD) readjustment. In RGB channels we consider five pixels, first three pixels are from Blue channel and last two pixels from Green Channel. Analysis of histogram from these channel are called selected channel. The result show that the quality parameters, PSNR, MSE, BPP, Capacity and FOBP. PSNR values are higher than the MSE value as compare to previous existing image steganography techniques.

This chapter consists of the main work proposed in this dissertation in following phases:

1. Histogram Analysis
2. Embedding Process Technique
3. Extraction Technique

3.1 Histogram Analysis

Digital images are presented in three blocks of channel (Red, Green and Blue) these blocks are called RGB channel in image steganography. In Fig.3.1 shown image pixels in different channel.

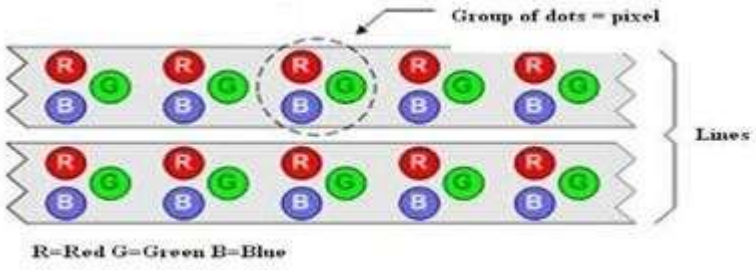


Fig. 3.1 RGB Channel of image.

Now, in this technique host collect one by one digital image (cover image or original image) and embedding secret bit in original image. These three RGB channels are separated individually in the form of matrix according to the size of cover image. Thus, each value of RGB matrix pixels shows the intensity of individual channel are present in Fig. 3.2, 3.3 and 3.4.

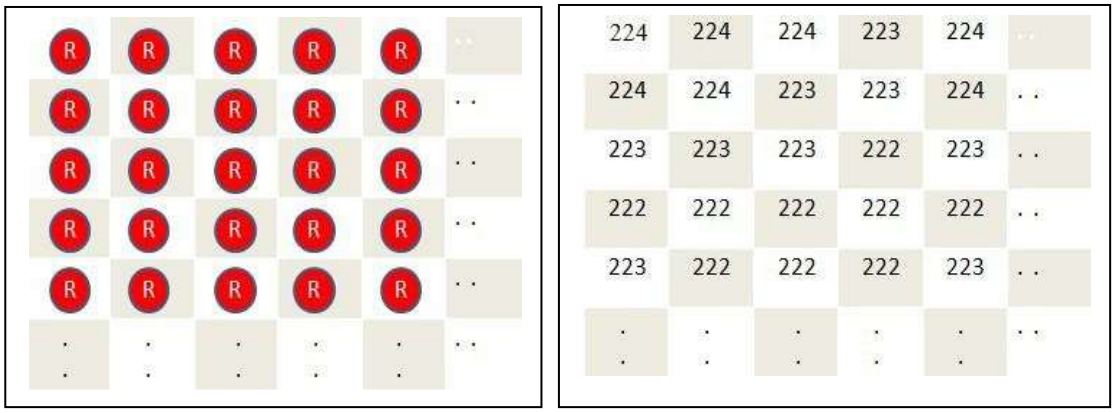


Fig. 3.2 Red plane pixel image and intensity of pixels

\

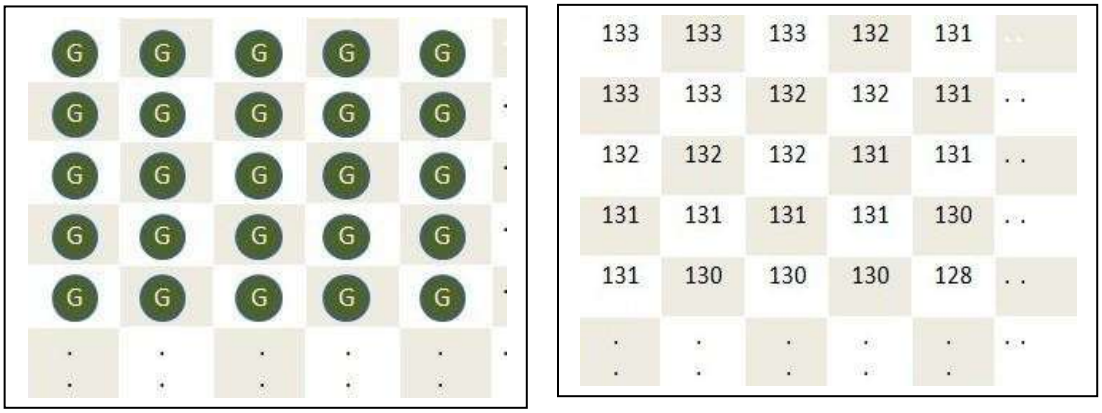


Fig. 3.3: Green plane pixel image and intensity of pixels

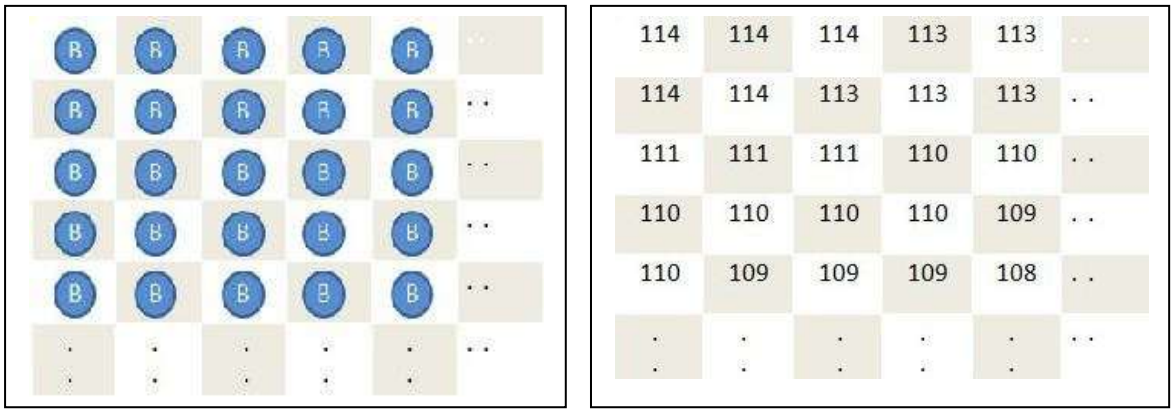


Fig. 3.4: Blue plane pixel image and intensity of pixels

After, separating the RGB channel from each other the histogram analysis is done with the secret bit insert into the cover image. The histogram of RGB channel is compared to the histogram of the secret message. Now we compare secret bit to the histogram channel, we select the channel whose histogram is most similar according to the secret bit. Green and Blue channel we selected for the embedding secret bit in to the histogram channel.

3.2 Embedding Process Technique

Now we describe three phases in an embedding process technique.

i) PDMO (Pixel Differencing Modulo Operation)

PDMO is a technique used mostly in steganography to embed or conceal a value within a picture. It is hidden in such a way that it is visually hard to determine whether the image contains any value. Compute the difference between the pixel values and then apply modulus, so that we can determine the value of the difference using certain rules, which we will cover later. This value is then used to embed the binary bits.

Assume that there are two pixels p_1, p_2 to which the PDMO approach should be applied.

The following are the specifics of the techniques:

- Calculate the difference in pixels d. Additionally, if a negative difference occurs, itwill be trivial to adjust its absolute value, as symmetry dictates that

all conceivablevalues are equally relevant. $d_{12} = |p_1 - p_2|$.

- Consider n_1 and n_2 is secret data bit number to be implanted on the pixels p_1 and p_2. Based on difference value d_{12}, determine $n_1$and n_2 as $n_1 = t$ and $n_2 = t$ bits, respectively, from range table.

Table 3.1 Proposed method range table

Range $(R_n) = (L_n, U_n)$	$R_1 = [0,31]$	$R_2 = [32,255]$
Capacity, t	$log_2(U_n - L_n) - 2$	$log_2(U_n - L_n) - 2$

- Find the remainders r_{md1} and r_{md2} using following rules:

$$r_{md1} = \begin{cases} p_1 \ mod\ 8, d_{12} \in R_1 \\ p_1 \ mod\ 16, d_{12} \in R_2 \end{cases}$$

$$r_{md2} = \begin{cases} p_2 \ mod\ 8, d_{12} \in R_1 \\ p_2 \ mod\ 16, d_{12} \in R_2 \end{cases}$$

- Convert n_1 and n_2 which is a part of binary secret message, to decimal say b_1 and b_2 respectively. Compute the difference values dv_1, dv_2, dv_3 and dv_4 as

$$dv_1 = r_{md1} - n_1$$
$$dv_2 = n_1 - r_{md1}$$
$$dv_3 = r_{md2} - n_2$$
$$dv_4 = n_2 - r_{md2}$$

- Apply the specified criteria to the pixels p_1 and p_2 at the first level to obtain theconsequent pixels p_1' and p_2'.

$$p_1' = \begin{cases} p_1, if\ r_{md1} = n_1 \\ p_1 - dv_1, if\ r_{md1} < n_1\ and\ |dv_1| < 2^{t-1} \\ p_1 + dv_2, if\ r_{md1} > n_1\ and\ |dv_2| < 2^{t-1} \\ p_1 - e, if\ r_{md1} < n_1\ and\ |dv_1| \geq 2^{t-1}\ where\ e = 2^t + dv_1 \\ p_1 + e, if\ r_{md_1} > n_1\ and\ |dv_1| \geq 2^{t-1}\ where\ e = 2^t + dv_2 \end{cases}$$

$$p2' = \begin{cases} p_2, if\ r_{md2} = n_2 \\ p_2 - dv_3, if\ r_{md2} < n_2\ and\ |dv_3| < 2^{t-1} \\ p_2 + dv_4, if\ r_{md2} > n_2\ and\ |dv_4| < 2^{t-1} \\ p_2 - ee, if\ r_{md2} < n_2\ and\ |dv_3| \geq 2^{t-1}\ where\ ee = 2^t + dv_3 \\ p_2 + ee, if\ r_{md_2} > n_2\ and\ |dv_4| \geq 2^{t-1}\ where\ ee = 2^t + dv_4 \end{cases}$$

- Calculate $d_{12} = |p'_1 - p'_2|$ as new difference value. If $d_{12} \in R_1$ apply following,

$$(p1*,p2*) = \begin{cases} (p1',2'), if\ d12 \in R1' \\ (p1'-2t,2'+2t), if\ d12' \in R2\ and\ p1' \geq p2' \\ (p1'+2t,2'-2t), if\ d12' \in R2\ and\ p1' < p2' \end{cases}$$

and if $d_{12} \in R_2$ apply following,

$$(p_{1*},p2_*) = \begin{cases} (p1',2'), if\ d_{12} \in R2' \\ (p1'+2_t,2'-2_t), if\ d_{12}' \in R_1\ and\ p1' \geq p2' \\ (p1'-2_t,2'+2_t), if\ d_{12}' \in R_2\ and\ p1' < p2' \end{cases}$$

- To resolve the condition of FOB, apply the following:

$$(p_{1*},p2_*) = \begin{cases} (p_{1*}+2_{t,2*}+2_t), if\ p_{1*}\ or\ p_{2*} < 0 \\ (p_{1*}-2_{t,2*}-2_t), if\ p_{1*}\ or\ p_{2*} > 255 \end{cases}$$

- The modified pixels are p_{1*} and p_{2*}.

ii) APVD (Average Pixel Value Differencing)

Subsequently, two pixels (p_1 and p_2) are required for computing the average of the pixels'values (p_{avg}), and a third pixel (p_3) is required for applying PVD. Thus, we will want three pixels in total. The following are the steps for applying the APVD:

- The average (p_{avg}) of two pixels (p_1 and p_2) is calculated

$$P_{avg} = \frac{\lfloor (P1 + P2) \rfloor}{2}$$

- Apply PVD to p_{avg} and p_3. Suppose p'_{avg} and p'_r is the altered pixels after using PVD in modified pixels.

- Calculate the difference value d_{avg} between p_{avg} and p'_{avg} as

$$d_{avg} = |p_{avg} - p'_{avg}|$$

- Now compute p^*_{avg} and p^*_r using

$$P^*_{avg} = P'_{avg} + d_{avg},$$

$$P_r^* = Pr' + d_{avg}$$

iii) <u>PVD (Pixel Value Differencing)</u>

- Assume p_1 and p_2 is two block of pixels.

Table 3.2 :Range Table for Wu & Tsai[11]

Range R_j =	R_1 =	R_2 =	R_3 =	R_4 =	R_5 =	R_6 =
$[L_j, U_j]$	[0,7]	[8,15]	[16,31]	[32,63]	[64,27]	[128,255]
Capacity, n	3	3	4	5	6	7

- Say difference between p_1 and p_2 be d as

$$d = |p_1 - p_2|$$

- Refer table 3.2 for d to find range R_j. Sequence No. of bits to be embedding in a pixel blocks is computed as $n = \log_2 (U_j - L_j + 1)$, where L_j= Lower bound of the range R_j.

  U_j= Upper bound of the range Rj·
- Let dec_n to be decimal value of secret data of n-bits. Calculate new difference value for the modified pixel by $d_{new} = dec_n + L_j$.
- Now compute value of "r", r is the difference of new and original pixels difference values, i.e.,

$$r = |d_{new} - d|.$$

- The stego-pixels p'_1 and p'_2 can be obtained using

$$(p1', p2') = \begin{cases} (p1 + \lceil r2 \rceil, p2 - \lceil r2 \rceil), if\ p1 \geq p2\ and\ dnew > d \\ (p1 - \lceil r2 \rceil, p2 + \lceil r2 \rceil), if\ p1 < p2\ and\ dnew > d \\ (p1 - \lceil r2 \rceil, p2 + \lceil r2 \rceil), if\ p1 \geq p2\ and\ dnew \leq d \\ (p1 + \lceil r2 \rceil, p2 - \lceil r2 \rceil), if\ p1 < p2\ and\ dnew \leq d \end{cases}$$

iv) Overflow and Underflow case resolution

- Overflow resolution condition apply in case of pixel value goes above 255 then compute the $dove$(difference value) by using given equation . Here max ($pi*$ and $pj*$) signifies the larger value between $pi*$ and $pj*$.

$$d_{overflow} = \max (P *_i \ and \ Pj*)\text{-}255$$

Now readjust the pixels $pavg*$ and $pj*$ as

$$pi* = pi* - doverflow,$$

$$pj* = pj* - doverflow$$

- Underflow resolution condition apply in case of pixel value goes less 0 then compute $d_{underflow}$(difference value) by using given equation, Here ($pi*$ and $pj*$) signifies the smallest value between $pi*$ and $pr*$.

$$dunderflow = \min(pi* \ and \ pj*) - 0$$

Now readjust the pixel values $pi*$ and $pr*$ using,

$$pi* = pi* - dunderflow$$

$$pj* = pj* - dunderflow$$

3.3 Extraction Process

Extraction technique is essentially reversing an embedding process. This approache find out the bit embedded in the proceeding steps. The following methods havebeen applied to retrieve the embedded bits.

i) Reverse PDMO(Pixel Differencing Modulo Operation)

PDMO is an operation to embed secret bit in the given pixels which is mentioned in the text by Sahu & Swain. Let $p1*$ and $p2*$ are two stego-pixels of a block as represent.

P1*	P2*	P3*

- Calculate the difference value $ds = p1* - p2*$. Now obtain the remainder values $rmd1*$ and $rmd1*$ using following equations:

$$r_{md1*}=\begin{cases} P1 \bmod 8, \text{if } ds\in R1 \\ P1 \bmod 16, \text{if } ds\in R2 \end{cases}$$

$$r_{md2*}=\begin{cases} P2 \bmod 8, \text{if } ds\in R1 \\ P2 \bmod 16, \text{if } ds\in R2 \end{cases}$$

- If $ds\epsilon R1$ then represent $rmd1*$ and $rmd2*$ (n= 3-bits), otherwise, $rmd1*$ and $rmd2*$ represent (n=4-bits). Both are extracted binary bits from stego-pixels $p1*$ and $p2*$.

ii) Reverse PVD (Pixel Value Differencing)

Let the stego-pixels $p1'$ and $p1'$, find the difference as $ds= |p1'- p2'|$. The" ds" value lies any one range of the range table. The range table given in Table 3.2. Compute s for the difference value and s be the difference between ds and lower bound Lj.

$$s= |d_s - L_j|.$$

Represent s to n bits, which are extracted bits.

iii) Reverse APVD (Average Pixel Value Differencing)

It basically works with some other algorithms which are either used to modify the pixel values or to embed bit of message value into pixels as it may be. Initially Let $p1*$ and $p2*$ and $p3*$ are three stego-pixels of a channel. Pixels are represent in given below:

P1*	P2*	P3*

The average stego-pixel $pavg*$ can be found using,

$$pavg*= \frac{\lfloor p1*+ p1 \rfloor}{2}$$

Next step is to apply reverse PVD to find the bits embedded in the $pavg*$ and $p3*$.

3.4 Proposed Algorithm

Algorithm follows as:

1. Select the pixels as p_1, p_2, p_3, p_4 and p_5. Secret Message $secretmsg$.

2. $[p1^*, p2^*, endpt] = PD(p_1, p_2, secretmsg, startpt)$

3. Argument list:

4. p_1, p_2 input pixels for Pixel Differencing Modulo Operation

5. $secretmsg$ is secret message in binary form.

6. $startpt$ is starting point of the secret message.Returning values:
   $p1^*$, $p2^*$ modified pixels which are altered by PDMO function.

   $endpt$ is end point of secret message which already embedded using PDMO.

7. Average pixels, $pavg = p1* + p2*2$

8. $[p^*, endpt] = (p_{avg}, p_3, secertmg, startpt)$

   Argument's list:

   p_{avg}, p_3 is input pixel for Average Pixel Value Differencing.

   $startpt$ is starting point for secret message to embed.Return's list:

3 p_3^* altered pixels by APVD

   $endpt$ is end point of secret message.

9. $[p4*, 5*, ndpt] = PVD(p4, p5, secretmsg, startpt)$

   Argument's List:

   $p4$, 5 is input pixels for Pixel Value Differencing

   $secretmsg$ is secret message.

$startpt$ is starting point for secret message.

Return's List: $p4*$,$5*$ is altered pixels by PVD,

$endpt$ is end point of secret message.

10. *Stego-pixels:* $p1*$, $p2*$, $p3*$, $p4*$,$5*$

ii) Extraction Algorithm

1. The Stego-pixels: $p1*$, $p2*$, $p3*$, $p4*$,$5*$
2. [binarymsgPart1] = $ReversePDMO$

   ($p1*$,$2*$) $p1*$,$2*$ is argument for Reverse PDMO.

   binarymsgPart1 first part extracted secret message
3. $pavg*$= $\lfloor p1*+p2*2 \rfloor$
4. [binarymsgPart2]= $ReverseA$PVD($pavg*$,$p3*$)

   $p3*$ is argument for Reverse APVD.

   binarymsgPart2 first part extracted secret message
5. [binarymsgPart3]= ReversePVD($p4*$,$p5*$)

   $p4*$,$5*$ is argument for Reverse PVD.

   binarymsgPart2 first part extracted secret message
6. Concatenate the 3 parts of secret message

   binarysecretmsg = binarymsgPart1+ binarymsgPart2+ binarymsgPart3
7. Extraction is completed.

3.5 Summary

In this thesis, Steganography technique has been proposed according to the literature survey. Here the histogram analysis is performed after which the algorithm is presented to embed the secret bit in images. Reverse technique is uses extracting the data by stego-image. Proposed technique result show the better result as compare to previous methods. Result will be computed with different cover images and analysis many quality parameters are given in Chapter 4.

Chapter 4

RESULT AND ANALYSIS

4.1 Quality Parameters of Image

Quality parameters of image are able to analyze of imaging system or processes. There are two parts categories in an image quality parameters i.e. subjective image quality is a technique which is used to examine image reliability and image clarity. Objective image quality are used for determine quality parameters between stego-image and cover image.

1. Mean Square Error (MSE).
2. Peak Signal Noise Ratio (PSNR).

4.1.1 Mean Square Error (MSE)

MSE value of the image is: -

$$\text{MSE}=\frac{1}{M*N}\sum_{x=1}^{M} \quad \sum_{y=1}^{N} \quad \{x(m,n)-y(m,n)\}2$$

Where two image size M*N are X(m, n) and Y(m, n).

X = original image.

Y = stego-image.

Minimum value of MSE gives error free an image (stego-image).

4.1.2 Peak Signal Noise Ratio (PSNR)

For compute the quality of stego-image we calculate PSNR value.

$$\text{PSNR}=20\log 10\left[\frac{MAXPIX}{MSE}\right]$$

MAXPIX = It is an average sum of distortion in each pixel of the stego image.

$$\text{RMSE}=\sqrt{MSE}$$

Mathematically:

PSNR value show the higher value as compare the MSE value of stego-image. Results of proposed approach are discussed in the next section 4.2 on the basis of the quality metrics parameters.

4.2 Result of Proposed Techniques

Result will be calculated in this thesis with six original images Girl, Baboon, Peppers, House, Plane and Face 1. Original image and stego-image for Girls, Peppers, House, Plane, Baboon and tree are presenting in below figures 4.1 and 4.2. Proposed Results depend on the quality parameters (PSNR. BPP, Capacity, FOBP etc.) are shown in Table 4.1, 4.2, and 4.3.

(1) Girl (ii) Peppers (iii) House

(iv) Plane (v) Baboon (vi) Plane

Fig. 4.1 Cover image (i-vi)

(i) Girl (ii) Peppers (iii) House

(iv) Plane (v) Baboon (vi) Tree

Fig. 4.2 Stego-image (i-vi)

Table 4.1 PSNR, FOBP, Capacity and BPP Value

Images	**Proposed PSNR**	**Proposed FOBP**	**Proposed BPP**	**Hiding capacity**
Girl	42.6485	0	4.02	144,871.00
Peppers	44.0703	0	4.01	258,898.00
House	41.3964	0	4.12	122,471.00
Plane	41.0127	0	3.91	208,535.00
Baboon	40.1430	0	3.45	93,461.00
Tree	39.9150	0	4.05	184,393.00

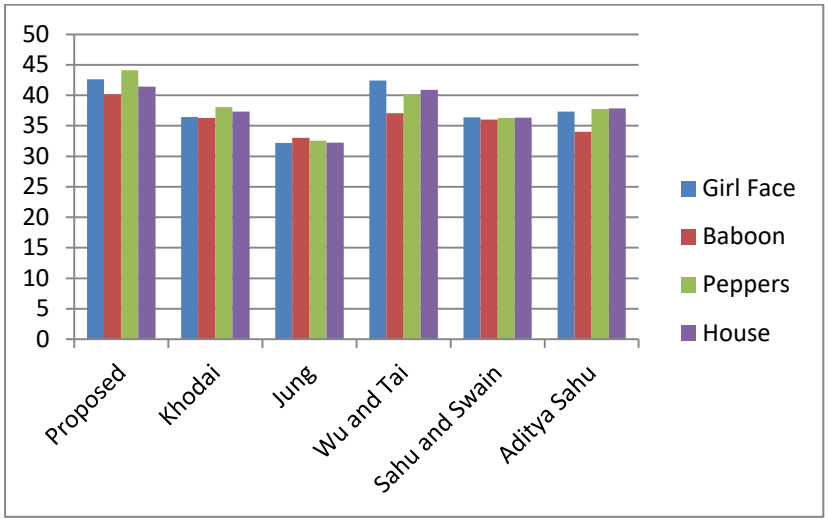


Fig. 4.3 Comparision of PSNR

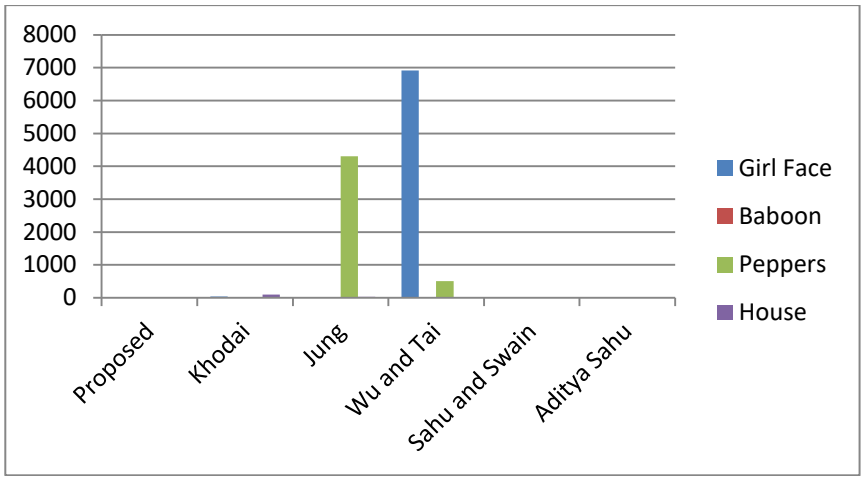


Fig. 4.4 FOBP counts (bits)

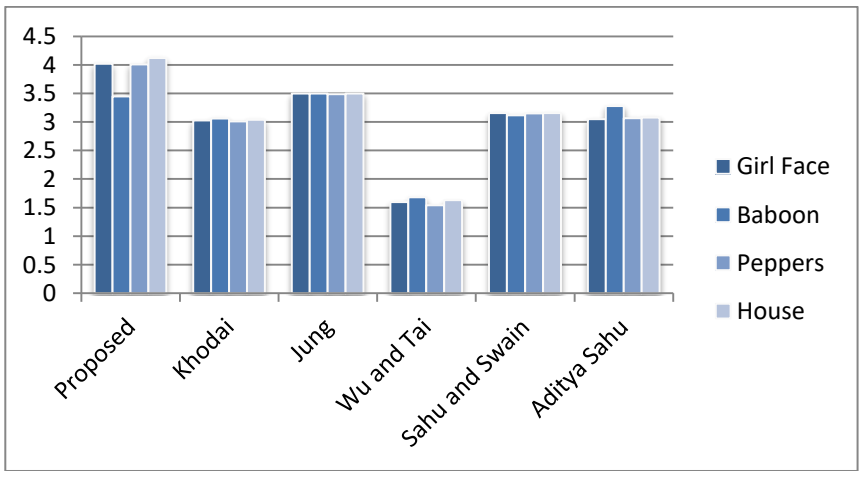


Fig. 4.5 Bits Per Pixel count

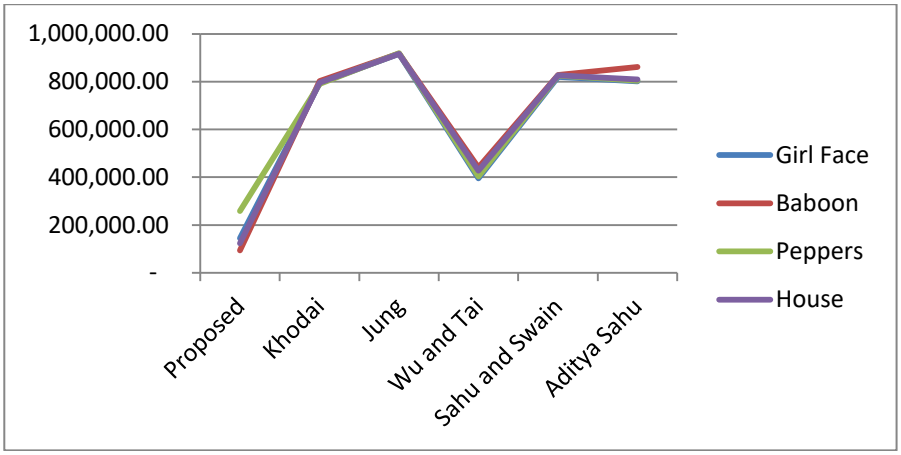


Fig. 4.6 Comparison hiding Capacity

Table 4.2 Result of the proposed approach, Khodaei and fez, Jung

Image (512*512)	Proposed ap roach				Khodaei and Faez [19]				Jung [2 3]			
	PSNR	Capacity	BPP	FOBP	PSNR	Capacity	BPP	FOBP	PSNR	Capacity	BPP	FOBP
Baboon	40.143	861,004	4.02	0	36.27	801,902	3.06	0	33.01	918,039	3.5	0
Couple	45.402	820,286	401	0	36.09	799,026	3.05	98	33.03	917,040	3.5	893
Girlface	42.648	800,592	4.01	0	36.41	794,492	3.03	0	32.19	916,540	3.5	0
House	41.396	808,520	4.12	0	37.31	795,649	3.04	0	32.21	916,773	3.5	23
Peppers	44.070	804,236	4.01	0	38.06	790,006	3.01	0	32.53	918,987	3.51	4308

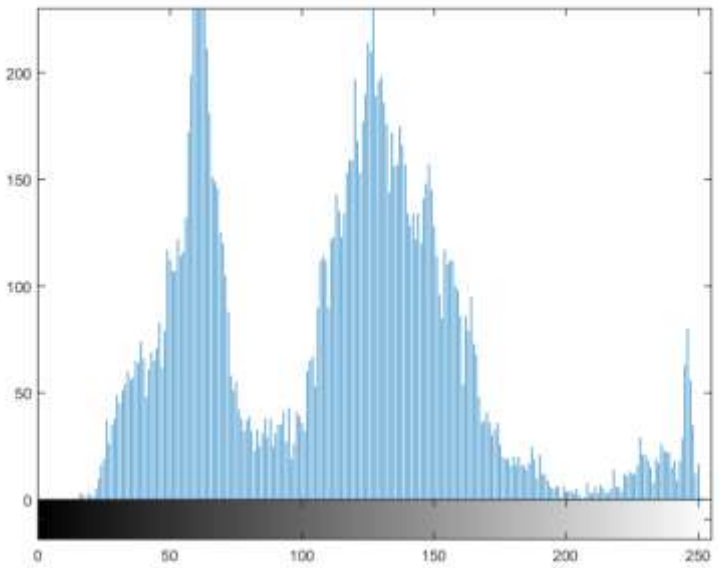
Table 4.3 Result of Wu and Tsai, Sahu and swain, Shen and sang

Image (512*512)	Wu and Tsai [11]				Sahu and Swain [35				Shen and Hu	ang [29		
	PSNR	Capacity	BPP	FOBP	PSNR	Capacity	BPP	FOBP	PSNR	Capacity	BPP	FOBP
Baboon	38.01	441,098	1.68	0	36.03	828,367	3.16	0	40.40	453,768	1.73	0
Couple	39.09	423,549	1.62	230	36.31	825,498	3.15	0	40.49	444,287	1.69	0
Girlface	42.44	394,904	1.51	6918	36.39	820,009	3.13	0	40.51	421,389	1.61	0
House	40.88	427,490	1.63	0	36.32	826,776	3.16	0	40.47	441,310	1.68	0
Peppers	40.11	402,756	1.54	503	36.29	825,002	3.15	0	40.43	439,029	1.67	0

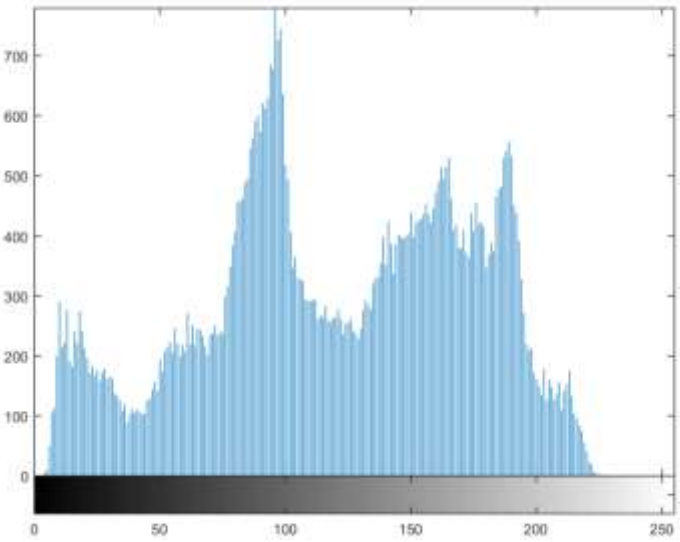
In this above diagram and table, proposed work calculates many quality parameters and compare with previous approaches with the help of cover image. We compare capacity, BPP, FOBP and PSNR with pervious approach. Capacity is the sequence of secret bits. BPP stands for bits per pixel, it measure average pixel number. FOBP is a fall off boundary problem in an image. In this proposed work capacity, BPP gives higher value as compare to previous approach [11, 19, and 23]. Some pervious approach gives highest capacity but not calculate higher PSNR value. PSNR and capacity produce similar values as compare to some previous approach [42]. The main advantage of our proposed work is it does not suffer from fall off boundary problem in an image pixel. Above Fig. 4.3, 4.4, 4.5 4.6 show these comparison result.

Analysis: The cover image and the stego image of Girl, baboon, peppers, house and palne appears to be the same in the Fig. 4.1. This is proved by the value of PSNR which is above 52 dB and the MSE which is in the span of 0 - 1 which shown that finer quality of stego-image.

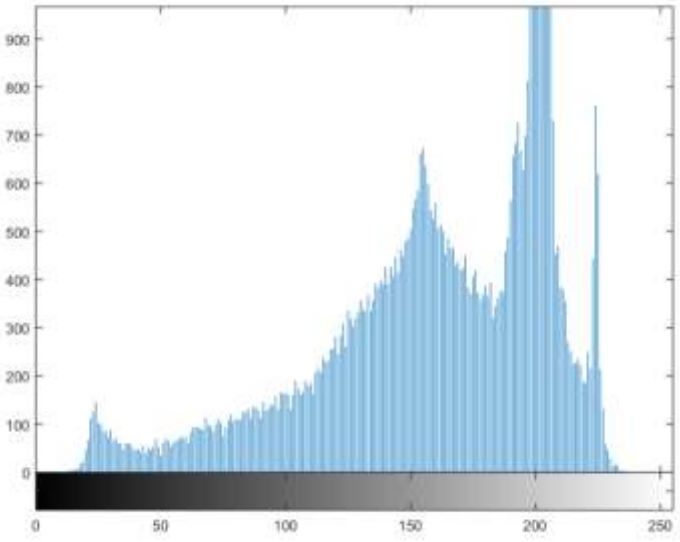
Histogram exploration of the both images (original image and stego-image), (Girl, Baboon, Peppers, House and Plane) are presenting in Fig. 4.7



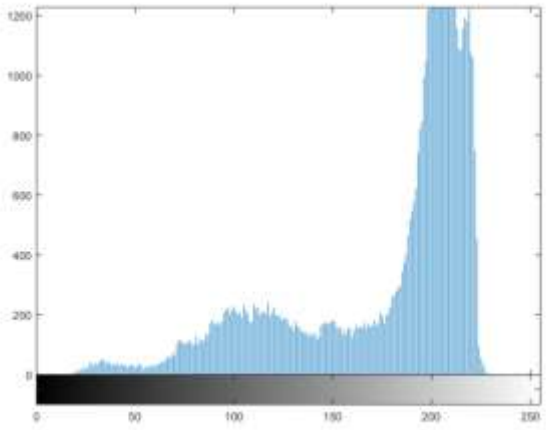
(i) Girl



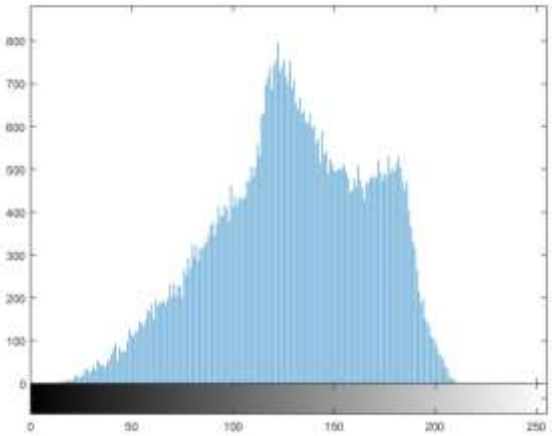
(ii) Peppers



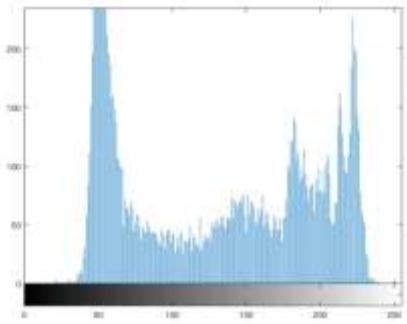
(iii) House



(iv) Plane



(v) Baboon



(vi) Tree

Fig. 4.7 Histogram of Stego images**.**

Finally, the security of this technique is far much better than existing ones which uses external securities such as cryptography with Steganography, but here it‘s the in-built characteristic i.e. we are embedding the difference of the selected Channel pixel and secret data into the other channel of cover image. Thus, if the attacker has doubt of the existence of the secret message in the image he is not able to extract from it as the difference of secret message with the selected channel has been hidden and not the actual message.

4.3 Summary

In this chapter, we have discussed about results and analysis on the basis of proposed work. We have found that the results of our proposed work are much better than those of the existing ones.

CHAPTER 5

CONCLUSION AND FUTURE WORK

In this thesis we proposed "**An Enhancement of Image Steganography Technique based on a PVD and Modulo Operation using of Histogram Analysis"**, and we use a spatial domain method .In this technique have many advantages as compare to another methods present in literature survey.

In this work we enhance data hiding technique depend on Pixel value differencing and Modulo Operation has been put forward. The data insertion is done with the using of three techniques as follow:

i) Pixel difference modulo operation (PDMO) technique.

ii) Average PVD (APVD) acclimatization technique. In this technique the first two successive pixels are observe for inserting using the pixel difference and modulo operation. In the second technique, we found the first two pixel average and PVD is acquire to find the average pixel along with the third pixel value to insert secure data. The capacity and PSNR value for the proposed technique are 44.07db and 825056 bits approximately.

Additionally the proposed methods discard the FOBP and RS attack completely

iii) Pixel Value differencing.

In future, our goal to enhance the proposed method by expands the averaging method from more than pixel value to enhance the hiding volume without decreasing the image quality. In future, as the proposed technique using averaging method to improve the work in the direction of reversible data hiding for providing higher security.

REFRENCES

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

[2]. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication, 65*, 46-66.

[3]. Pradhan, A., Sahu, A. K., Swain, G., & Sekhar, K. R. (2016). Performance evaluation parameters of image steganography techniques. *In: IEEE International Conference on Research Advances in Integrated Navigation Systems*, 1-8.

[4]. Sahu, A. K., & Swain, G. (2016). A Review on LSB Substitution and PVD Based Image Steganography Techniques. *Indonesian Journal of Electrical Engineering and Computer Science, 2*(3), 712-719.

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

[6]. Sahu, A. K., Swain, G., & Babu, E. S., (2018). Digital Image Steganography Using Bit Flipping. *Cybernetics and Information Technologies, 18*(1), 69-80.

[7]. Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern recognition*, *34*(3), 671-683.

[8]. Wu, N.I. & Hwang, M.S. (2017). A novel LSB data hiding scheme with the lowest distortion. *The Imaging Science Journal, 65*(6), 371-378.

[9]. Sahu, A. K., & Swain, G. (2018). An Improved Data Hiding Technique Using Bit Differencing and LSB Matching. *Internetworking Indonesia Journal*, *10*(1), 17-21.

[10]. Hussain, M., Abdul Wahab, A.W., Javed, N. & Jung, K. H. (2016). Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. *Symmetry*, *8*(6), 41.

[11]. Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*(9-10), 1613-1626.

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

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

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

[15]. Swain, G. (2015). Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimedia Tools and Applications*, *75*(21), 13541-13556.

[16]. Hussain, M., Wahab, A. W. A., Ho, A. T., Javed, N., & Jung, K. H. (2017). A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. *Signal Processing: Image Communication*, *50*, 44-57.

[17]. Hameed, M. A., Aly, S., & Hassaballah, M. (2017). An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). *Multimedia Tools and Applications*, *77*(12), 14705-14723.

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

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

[20]. Khodaei, M., Sadeghi Bigham, B., & Faez, K., (2016). Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution. *Cybernetics and Systems*, *47*(8), 617-628.

[21]. Swain, G. (2018). Adaptive and Non-adaptive PVD Steganography Using Overlapped Pixel Blocks. *Arabian Journal for Science and Engineering*, 1-14. (Article in press). https://doi.org/10.1007/s13369- 018-3163-9

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

[23]. Jung, K. H. (2018). Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. *Journal of Real-Time Image Processing*, *14*(1), 127-136.

[24]. Swain, G. (2018). Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. *Arabian Journal for Science and Engineering*, (Article in press). https://doi.org/10.1007/s13369-018-3372

[25]. Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, *81*(1), 150-158.

[26]. Joo, J. C., Lee, H. Y., & Lee, H. K. (2010). Improved steganographic method preserving pixel-value differencing histogram with modulus function. *EURASIP Journal on Advances in Signal Processing*, *2010*(1), 249826.

[27]. Maleki, N., Jalali, M. & Jahan, M. V. (2014). Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function. *Egyptian Informatics Journal*, *15*(2), 115-127.

[28]. Liao, X., Wen, Q., & Zhang, J. (2013). Improving the Adaptive Steganographic methods Based on Modulus Function. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *96*(12), 2731-2734.

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

[30]. Liao, X., Wen, Q. Y., Zhao, Z. L., & Zhang, J. (2012). A novel steganographic method with four-pixel differencing and modulus function. *Fundamenta Informaticae*, *118*(3), 281-289.

[31]. Thien, C. C., & Lin, J. C. (2003). A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. *Pattern recognition*, *36*(12), 2875-2881.

[32]. Lee, C. F., & Chen, H. L. (2010). A novel data hiding scheme based on modulus function. *Journal of Systems and Software*, *83*(5), 832-843.

[33]. Liao, X., Guo, S., Yin, J., Wang, H., Li, X., & Sangaiah, A. K. (2017). New cubic reference table based image steganography. *Multimedia Tools and Applications*, 1-18. DOI 10.1007/s11042-017-4946-9.

[34]. Liao, X., Qin, Z., & Ding, L. (2017). Data embedding in digital images using critical functions. *Signal Processing: Image Communication*, *58*, 146-156.

[35]. Sahu, A. K., & Swain, G. (2018). Pixel Overlapping Image Steganography Using PVD and Modulus Function. *3D Research, 9(*3*),* 1-14. https://doi.org/10. 1007/s13319-018-0188-5.

[36]. Sahu, A.K., & Swain, G. (2017). Information Hiding Using Group of Bits Substitution. *International Journal on Communications Antenna and Propagation, 7*(2), 162-167.

[37]. Sahu, A.K., & Swain, G. (2018). Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis. *International Journal of Electronic Security and Digital Forensics*. (In press).

[38]. Sahu, A. K., & Swain, G. (2019). A Novel n-Rightmost Bit Replacement Image Steganography Technique. *3D Research, 10*(1), 1-18.

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

[40]. USC-SIPI Image Database. [Online]. Available:http://sipi.usc.edu/database/database.php?volume=misc.

[41]. http://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm.

[42]. Aditya Kumar sahu and Gandharba Swain (2019). Digital Image Steganography using PVD and Modulo Operation. Internetworking Indonesia Journal, February 2019. Vol. 10/No.2.

LIST OF PUBLICATION

A paper " An Enhancement of Digital Image Steganography Based on a PVD and Modulo Operation " Monika Sharma, Manoj Kumar Sharma, P.K Gautam (April, 2021), publish in International Journal of Engineering Research in Computer Science and Engineering, IJERCSE (ISSN 2394-6849) Journal for Volume 8, Issue 4.

CONFERENCE PAPER

A Conference paper" An Analysis of Different Techniques of Security System for Hiding Images" Monika Sharma, Manoj Kumar Sharma, P.K Gautam (June, 2020) publish in IIMT College, Meerut

CURRICULUM VITAE

MONIKA SHARMA
Email: monika1512015@gmail.com
Phone: +91- 8126031982

Academic Credentials:

- Pursuing **M.Tech (CSE)** from Marathwada Institute of Technology, Bulandshhar, Dr. APJ Abdul Kalam Technical University, Lucknow.
- B.Tech from Marathwada Institute of Technology, Bulandshahr, DR. APJ Abdul Kalam Technical University, Lucknow.

Software Skills:

Operating System: Windows
Programming: C, Java, Java Script, HTML

Personal Details:

NAME: Monika Sharma
Father's Name: Late. Shri Ram Prakash Sharma
Mother's Name: Mradula Sharma
Date of Birth: 05-July-1998
Nationality: Indian
Marital Status: Unmarried
Language Know: Hindi, English

Declaration:
I declare that the given details are true and correct to the best of my knowledge.

Place: Khurja, Bsr (UP)