IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Steganography In Images Using Pixel Value Differencing

[1]Palak Pandey, [2]Reshma Sonar

[1]Bachelor's of Engineering Student, [2]Associate Professor

[1]Department of AIML, ISBM COE

[1]ISBM COE, Pune, India

Abstract: The practice of hiding information within seemingly innocent data to maintain its anonymity and secret is known as steganography. Steganography has emerged as a critical method for protecting sensitive data in a digital age where privacy and secure communication are crucial. This abstract offers a succinct synopsis of steganography, including its methods, foundational ideas, and application in contemporary cybersecurity. Steganography allows for the covert conveyance of information by encoding secret messages into common files like text, audio, or photos. This is achieved through the application of several strategies, one of it being Pixel Value Differencing or PVD. This abstract highlight the importance of steganography in the digital era and highlights how important it is for information sharing integrity, privacy, and security. It also throws light on the various techniques used in the algorithm of PVD.

I. INTRODUCTION

The goal of steganography is to conceal the information's very existence while maintaining its similarity to non-secret material. Steganography, which comes from the Greek terms "steganos" (which means "covered") and "graphein" (which means "writing"), is the practice of hiding data on a media to protect its confidentiality.

A steganographic technique called Pixel Value Differencing (PVD) makes use of the deceptive alteration of pixel values in

digital pictures. PVD alters pixel values in a way that is unnoticeable to the human eye, in contrast to more intrusive

approaches that could noticeably alter the appearance of an image. This method makes use of the fact that small variations in

pixel values frequently go undetected, making it possible to inject hidden data covertly.

In simple words, steganography means to hide some valuable information in something common (such as text, audio, video,

images, file, spam, printed document etc.), in such a way that is not detectable by anyone whom it is not intended for.

Basically, hiding information in something so only the sender and receiver are aware that there is a hidden message in it.

As per the Pixel Value Differencing (PVD) steganogra- phy [1], an image is partitioned into distinct blocks with two

consecutive pixels. In each block a Pixel Value Difference is computed and then this difference value is replaced by a new

difference value to hide the secret data bits. Furthermore, the hiding capacity can be increased by using three directional

differences in 2 × 2 pixel blocks. [2,3,4]

The prime idea in PVD technique is that smooth regions should hide lesser number of bits and edge regions should hide a

greater number of bits, so that the distortion will not be noticed. Thus, the pixel value differences are utilized to find the

embedding capacity of a pixel block based on a range table.[5]

II. LITERATURE REVIEW

There is a significant amount of study on Pixel Value Differencing (PVD) in image steganography, according to a review of the literature. PVD is a well- known technology that can incorporate concealed data into digital photos without sacrificing the images' aesthetic appeal. Several important studies and conclusions about PVD steganography are included below:

1.) "A High-Capacity Data Hiding Scheme Using Pixel Value Differencing"

Authors: Wang et al.

An early investigation of PVD steganography is presented in this work. It presents a method that minimizes visual

distortion in the stego-images while optimizing data hiding capacity.

2.) "Adaptive Image Steganography Using Pixel Value Differencing and LSB Replacement"

Authors: Vijayakumar and Mankar

The study focuses on PVD combined with LSB (Least Significant Bit)

substitution for adaptive image steganography. It looks at methods to increase the capacity and imperceptibility of the

buried data.

3.) "A Novel Steganographic Technique for Hiding Image Using Improved Pixel Value Differencing"

Authors: Saini et al.

An enhanced PVD technique for concealing images inside other images is presented in this paper. The suggested method

improves stego-image quality and offers a safe means of sending data.

4.) "A Novel Reversible Data Hiding Scheme Based on Pixel Value Differencing and Histogram Shifting"

Authors: Wu et al.

The authors talk about how to build a reversible data concealment strategy using PVD and histogram shifting. This

method guarantees lossless data extraction.

5.) "A Secured Reversible Data Hiding Method for Medical Images Using Improved Pixel Value Differencing"

Authors: Sharma and Khanna

In the context of medical photographs, PVD steganography is examined in this work. It focuses on using enhanced PVD

techniques to secure sensitive medical data.

6.) "An Image Steganography Technique Based on Pixel-Value Differencing Using 2-Bit LSB"

Authors: Sharma and Khanna

The method that uses PVD with 2-bit LSB embedding is presented in the publication. The goal of this strategy is to

improve the hidden data's capacity and security.

7.) "Color Image Steganography Using RGB Planes and Improved Pixel Value Differencing"

Authors: Verma et al.

In order to provide secure data concealment, this research investigates color image steganography using an enhanced PVD

method and the RGB color model.

8.) "Enhanced PVD-Based Image Steganography for Secure Data Transmission"

Authors: Kumar et al.

For safe data transmission, the author suggests an improved PVD-based image steganography method that increases

security and data hiding capability. Together, these studies demonstrate the developments and adaptability of PVD

steganography in the fields of data concealing inside pictures and information security. PVD is used in a variety of fields,

such as multimedia forensics, secure data transmission, and medical imaging, illustrating the breadth of its uses and

importance in the digital age.

III. METHODOLOGY

There are two major PVD techniques, namely One Way PVD and Seven Way PVD. Let's discuss more about them below:

One Way PVD: [5]

"Edge regions of an image can hide a greater number of bits as compared to smooth regions" is the new paradigm that Wu & Tsai (2003) identified. They developed the PVD steganographic algorithm.

The image's pixels are raster scanned, and a block is defined as two consecutive pixels (P_i, P_i+1). The difference value

$d = (P_i+1 - P_i)$ is found for such a block. An example of a range table is Table 1. $W_i = (u_i - l_i+1)$ is the width of one of the Ranges R_i, to which this d value belongs. In this case, the range Ri's lower and upper bounds are denoted by l_i and u_i. This block can have a maximum of n_i bits concealed. Currently, n_i data points are extracted from the binary data stream and transformed into a decimal value of b. As in Equation (1), the new difference value is computed by hiding b in this block.

$$d' = \begin{cases} l_i + b, & \text{if } d \geq 0 \\ -l_i - b, & \text{if } d < 0 \end{cases} \quad (1)$$

Now $m = d' - d$ is calculated. If d is an odd number the stego block is $(p_i - m/2, p_{i+1} + m/2)$. If d is an even number the stego block is $(p_i - m/2, p_{i+1} + m/2)$. [5]

Range	**Width**	**No. Of bits**
$R_1 \in \{0, 7\}$	$w_1 = 8$	$n_1 = 3$
$R_2 \in \{8, 15\}$	$w_2 = 8$	$n_2 = 3$
$R_3 \in \{16, 31\}$	$w_3 = 16$	$n_3 = 4$
$R_4 \in \{32, 63\}$	$w_4 = 32$	$n_4 = 5$
$R_5 \in \{64, 127\}$	$w_5 = 64$	$n_5 = 6$
$R_6 \in \{128, 255\}$	$w_6 = 128$	$n_6 = 7$

Table 1: Range table for above [5]

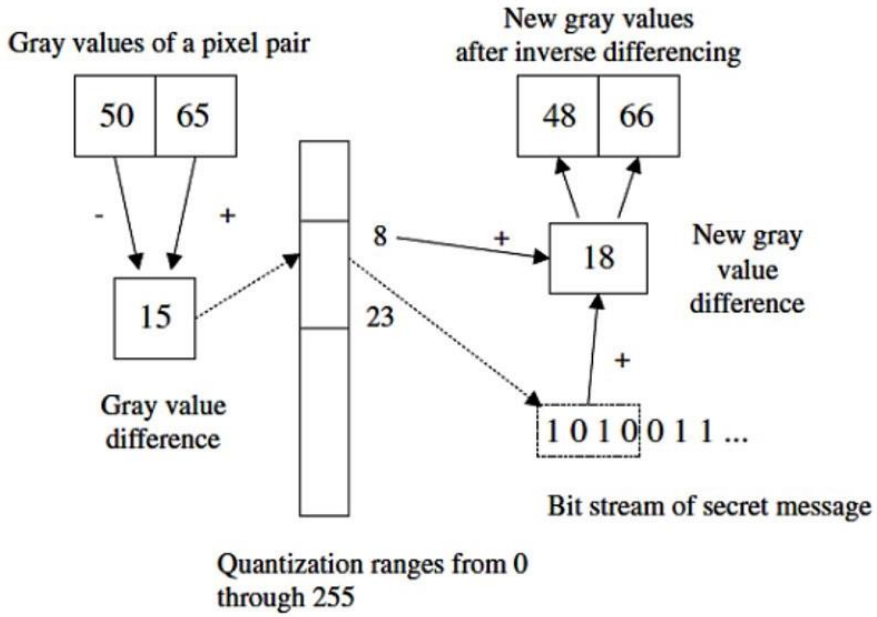

Image 1: Example of PVD

Seven Way PVD: [5]

This technique was proposed by Pradhan, Sekhar & Swain (2016). For data embedding the image is raster scanned and divided into 3×3 non-overlapping blocks, a sample block is shown in Figure .

Seven pairs are formed out of these nine pixels. Those are $P_0 = (p_{22} , p_{23})$, $P_1 =(p_{22} , p_{13})$, $P_2 =(p_{22} , p_{12})$, $P_3 =(p_{22} , p_{11})$, $P_4 =(p_{22} , p_{21})$, $P_5 =(p_{22} , p_{31})$, $P_6 =(p_{22} , p_{32})$. The pixel p_{33} is excluded from these pairs. The 7 pixel value differences, $d_0 = p_{23}- p_{22}$, $d_1=p_{13}-p_{22}$, $d_2=p_{12}-p_{22}$, $d_3=p_{11}-p_{22}$, $d_4= p_{21} -p_{22}$, $d_5 =p_{31} -p_{22}$, $d_6 =p_{32} -p_{22}$ are computed. Here, we can refer Table 1 as the range Table. For i=0 to 6, the d_i value lies in range R_{ki} , the width $w_{ki} = u_{ki} - l_{ki} +1$, wherein u_{ki} and l_{ki} are upper and lower bounds. The embedding length for each d_i is, $n_i = \log_2 w_{ki}$. For each d_i , n_i data bits from the binary data stream is taken and converted to the decimal equivalent b_i and then d'_i is calculated following the Eq. (2).

p_{11}	p_{12}	p_{13}
p_{21}	p_{22}	p_{23}
p_{31}	p_{32}	p_{33}

Table 2: A 3x3 sample block

$$d' = \begin{cases} l_{ki} + b_i & \text{, if } d_i \geq 0, \\ -l_{ki} - b_i & \text{, if } d_i < 0 \end{cases} \qquad (2)$$

Now for i=0 to 6, $m_i = d'_i - d_i$ is calculated. After data embedding, the new pairs are calculated as in Eq. (3).

$P'_0 =$ $(p_{22}-m_0/2, p_{23}+m_0/2)$, if d_0 is even,

$(p_{22}-m_0/2, p_{23}+m_0/2)$, if d_0 is odd

$P'_1 =$ $(p_{22}-m_1/2, p_{13}+m_1/2)$, if d_1 is even,

$(p_{22}-m_1/2, p_{13}+m_1/2)$, if d_1 is odd

$P'_2 =$ $(p_{22}-m_2/2, p_{12}+m_2/2)$, if d_2 is even,

$(p_{22}-m_2/2, p_{12}+m_2/2)$, if d_2 is odd

$P'_3 = (p_{22}-m_3/2, p_{11}+m_3/2)$, if d_3 is even,

$(p_{22}-m_3/2, p_{11}+m_3/2)$, if d_3 is odd (3)

$P'_4 = (p_{22}-m_4/2, p_{21}+m_4/2)$, if d_4 is even,

$(p_{22}-m_4/2, p_{21}+m_4/2)$, if d_4 is odd

$P'_5 = (p_{22}-m_5/2, p_{31}+m_5/2)$, if d_5 is even,

$(p_{22}-m_5/2, p_{31}+m_5/2)$, if d_5 is odd

$P'_6 = (p_{22}-m_6/2, p_{32}+m_6/2)$, if d_6 is even,

$(p_{22}-m_6/2, p_{32}+m_6/2)$, if d_6 is odd

In these new pairs, p_{22} has obtained seven new values, they need to converge into a single value. Suppose the seven pairs for i=0 to 6 are (x_i , y_i). The x_i value is unified to x as in Eq. (4).

$$x = (x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6) / 7 \quad (4)$$

When x value is changed to x, the y values are also changed to $y' = y_i + x - x_i$. For i=0 to 6, if the new pairs (x, y'_i) falls in range {0, 255}, the block is marked as ok by embedding 1 to LSB of p_{33} . For i=0 to 6, if the new pairs (x, y'_i) falls out of the range {0, 255}, the block is marked as unsuitable by embedding 0 to LSB of p_{33} and undoing the embedding. The data retrieval is done in the following way, by forming the blocks as was done in embedding.

IV. IMAGES

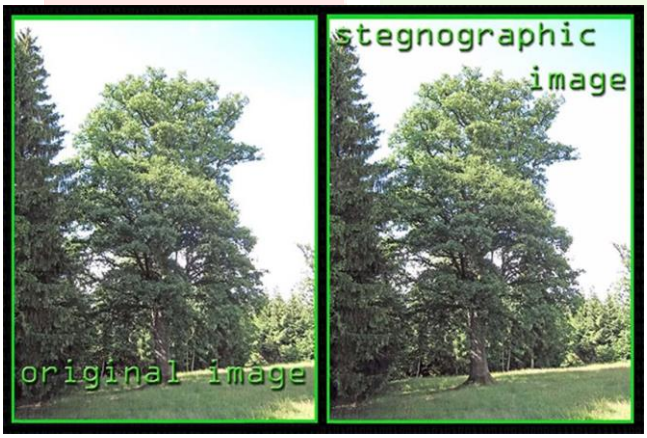

Image 2

Image 3

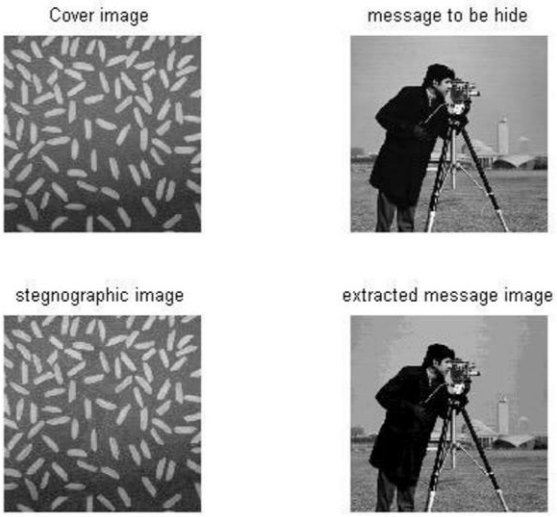

Image 4

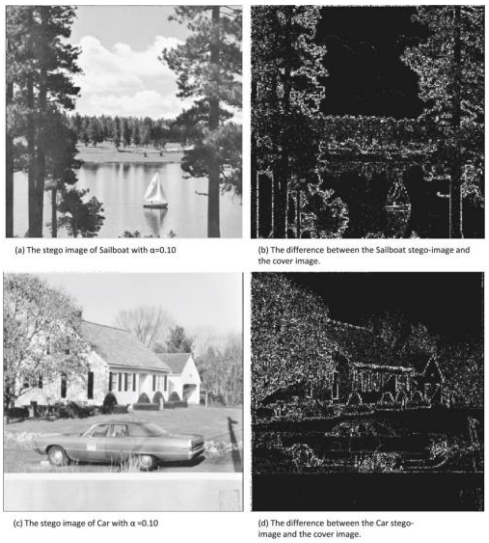

Image 5

V. FLOWCHART

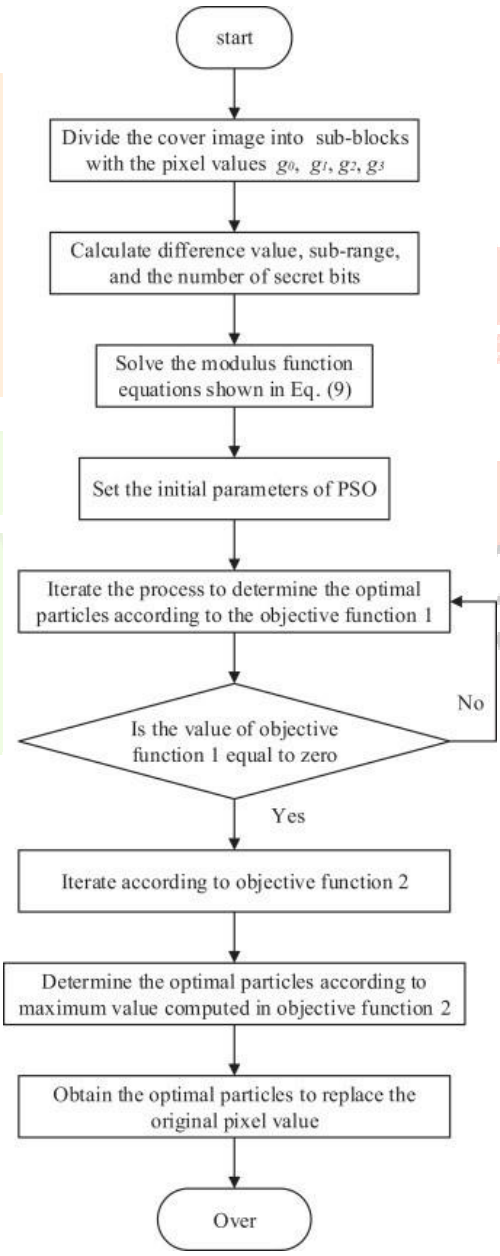

Figure 1: Flowchart of PVD algorithm

VI. RESULTS

Discussions and Findings:

Pixel Value Differencing (PVD) steganography is a rapidly developing field with opportunities and difficulties. In summary, the use and investigation of PVD steganography resulted in several significant findings and understandings:

- **Improving Data Security and Privacy:** PVD steganography has been a useful method for improving data privacy and security. Its capacity to covertly conceal data from prying eyes within digital photos provides an extra degree of defense against data breaches and illegal access.
- **Application in the Real World:** PVD steganography is useful in several fields, including watermarking, digital forensics, and covert communication. Because of its adaptability, it can be used in situations where data hiding is essential.
- **Technological Developments**: PVD steganography's capabilities have been extended by recent developments. The field is still evolving, as seen by better robustness against detection techniques and improved embedding algorithms.
- **Difficulties and Vulnerabilities:** PVD steganography has certain difficulties and weaknesses. The possibility of detection emphasizes the necessity of continued research to solve its limits, particularly in sophisticated forensic circumstances.
- **Ethical and Legal Considerations**: It is crucial to employ PVD steganography in an ethical and responsible manner. To preserve its ethical integrity, it must be aware of any potential moral conundrums and adhere to privacy and intellectual property rules.
- **Academic and Research Contribution:** The discipline has advanced thanks in large part to the efforts of the academic and research community. PVD steganography is still advancing thanks to new discoveries, creative methods, and teamwork.
- **Education and Awareness:** PVD steganography is a teaching tool that increases knowledge and awareness of the method. It serves a wide range of users, including professionals and students, by offering insights into the complexities of data hiding.

References:

1. Wu DC, Tsai WH. A steganograhic method for images by Pixel Value Differencing. Pattern Recognition Letters. 2003; 24(9-10):1613–26.
2. Chang KC, Chang CP, Huang PS, Tu TM. A novel image steganography method using tri-way Pixel Value Differencing. Journal of Multimedia. 2008; 3(2):37–44.
3. Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP. High-payload image hiding with quality recovery using tri- way Pixel Value Differencing. Information Sciences. 2012; 191:214–25.
4. Anita Pradhan, K. Raja Sekhar and Gandharba Swain:Digital Image Steganography based on Seven Way Pixel Value Differencing. October 2016 (IJST)
5. Gandharba Swain.: Pixel Value Differencing Steganography. October 2016
6. Swain Gandharba.: Digital Image Steganography using eight-directional PVD against RS analysis and PDH analysis. *Adv. Multimed.* **2018**, 1–13 (2018)