B.Tech (Electronics & Communication Engineering)

Yash Gupta

2024

Image Steganography with Huffman Encoding and Laguerre Transform

A PROJECT REPORT
SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF DEGREE
OF
BACHELOR OF TECHNOLOGY
IN
Electronics & Communication Engineering

Submitted By:
Yash Gupta
(2K20/EC/241)

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi – 110042

May 2024

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi - 110042

CANDIDATE'S DECLARATION

I **Yash Gupta (2K20/EC/241)),** student of B.Tech (Electronics & Communication Engineering) declare that the project report titled "**Image Steganography with Huffman Encoding and Laguerre Transform**" which is submitted by me to the Department of Electronics & Communication Engineering, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology, is original and not copied from any source without any proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi
Date:

YASH GUPTA
(2K20/EC/241)

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi – 110042

CERTIFICATE

I hereby certify that the project titled "**Image Steganography with Huffman Encoding and Laguerre Transform**", which is submitted by Yash Gupta, Roll No: 2K20/EC/241, Department of Electronics & Communication Engineering, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology, is a record of project work carried out by students under my supervision. To the best of my knowledge, this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi
Date:

ACKNOWLEDGEMENT

The successful completion of any task is incomplete and meaningless without giving any due credit to the people who made it possible without which the project would not have been successful and would have existed in theory. First and foremost, we are grateful to HOD, Department of Electronics & Communication Engineering, Delhi Technological University, and all other faculty members of our department for their constant guidance and support, constant motivation and sincere support and gratitude for this project work. We owe a lot of thanks to our supervisor, Department of Electronics & Communication Engineering, Delhi Technological University for igniting and constantly motivating us and guiding us in the idea of a creatively and amazingly performed Major Project in undertaking this endeavour and challenge and also for being there whenever we needed their guidance or assistance. We would also like to take this opportunity to express our gratitude to everyone who has helped us with this difficult endeavour, whether indirectly or directly. We are delighted, joyful, and content to convey our gratitude to everyone who assisted and directed us in providing this project work for our major project. Last but not least, we appreciate our well-wishers and parents for always being there for us and supporting us in any way they could.

Yash Gupta
(2K20/EC/241)

ABSTRACT

In this study, we will investigate how Huffman encoding and Laguerre transform can be used to encode images in the steganography domain. We analyse the evolution, approaches, challenges, and the future possibilities of several image steganographic techniques by thoroughly analysing multiple academic articles. Our review focuses on the role of Huffman encoding and Laguerre transform in improving robustness, embedding capacity, and security of the image steganography, as well as resolving the computing challenges by comparing it to other investigated approaches. Furthermore, we evaluate our findings using a range of parameters to determine the quality of the generated steganographic image. Moreover, this study explored a variety of image steganography techniques intending to fully comprehend their unique characteristics and applications. The literature review emphasized the need to use a variety of approaches, each with pros and cons of its own while implementing image steganography. Through this investigation, more was learned about the wide spectrum of uses for image steganography, including covert operations, digital watermarking, and secure communication. Moreover, this study demonstrated the intrinsic trade-off between perceived quality and payload capacity. This inverse relationship in which a higher chance of detectability was often associated with an increase in payload capacity was noticed when various steganographic techniques were investigated. This result emphasises the necessity of striking a precise balance between the ability to conceal data and preserving the cover image's visual integrity. In summary, this study offered a thorough analysis of image steganography, stressing its importance, uses, and the trade-offs associated with different methods, while demonstrating that the proposed method yields better stego image quality, as evaluated using PSNR and SSIM metrics, and offers a greater payload capacity.

CONTENTS

TABLE OF CONTENTS **PAGE NO**

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BER	Bit Error Ratio
BPP	Bits per Pixel
CI	Cover Image
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HI	Hidden Image
ILT	Inverse Laguerre Transform
IWT	Inverse Wavelet Transform
LSB	Least Significant Bit
LT	Laguerre Transform
MSE	Mean Square Error
PSNR	Peak Signal-to-Noise Ratio
SI	Stego Image
SSIM	Structural Similarity Index Measure

CHAPTER 1
INTRODUCTION

1.1 Background and Motivation

In this digital age, image security and confidentiality have become paramount, prompting the development of sophisticated methods to protect sensitive data. Image steganography, the method of concealing information within images, is a crucial technique in this regard. Traditional transformation methods like the DCT, DFT, and DWT have been widely utilized to embed hidden data. However, there remains a constant demand for more secure and efficient techniques. This is where the combination of the Laguerre transform and Huffman encoding offers a novel approach to enhancing steganographic method

The motivation for using the Laguerre transform and Huffman encoding in image steganography arises from the necessity to improve upon traditional techniques. Security is a primary concern, as widely studied methods like DCT, DFT, and DWT have known vulnerabilities. The Laguerre transform, being less commonly used, can provide an additional layer of security through its unique transformation properties. Furthermore, preserving the perceptual quality of the image while embedding data is crucial. The Laguerre transform may offer improved imperceptibility, ensuring that the hidden information does not deteriorate the visual image quality.

A further crucial element is embedding capacity. Huffman encoding, renowned for its effectiveness in data compression, can maximise the amount of space needed for embedding, enabling the concealment of more data inside the picture. This combination can strengthen the steganographic system's resistance to a number of attacks, including as cropping, noise addition, and compression.

In practical applications, image steganography is vital for secure communication across multiple domains. In military and government communications, it ensures that sensitive information is transmitted securely. In the corporate sector, it protects intellectual property and confidential business strategies. Healthcare applications include the secure transmission of medical records, ensuring patient privacy. Additionally, in the digital forensics field, steganography is used to embed watermarking information to verify the authenticity of digital evidence. Therefore, it enhances productivity and facilitates decision-making across a wide range of industries and domains.

The Laguerre transform and Huffman encoding method's efficacy and potential benefits can be better understood by contrasting it with more established methods like DCT, DFT, and DWT. Understanding the benefits and drawbacks of various approaches is made possible by this comparative analysis, which also advances the field's current study and growth in the areas of secure communication and information concealment.

Thus, the motivation for exploring the Laguerre transform and Huffman encoding in image steganography is driven by the need for enhanced security, improved image quality, higher embedding capacity, and robust performance. These improvements are critical in tackling the issues faced by the growing demand for secure and efficient data hiding strategies in our digital age. By developing more sophisticated and resilient steganographic methods, we can better protect sensitive information, ensure the privacy and integrity of digital communications, and maintain the trust and security essential in various applications, including personal privacy protection, national security, and corporate confidentiality.

1.2 Image Steganography

The method of hiding secret data inside an image so that it is invisible to the human eye is known as image steganography. The primary focus is to conceal a secret message without changing the image's appearance inside a cover photo. This is accomplished by modifying the pixel values of the images in order to embed the hidden data. Since alterations to these bits have a minute effect on the overall quality of the image, the secret data is usually embedded in the least significant bits (LSBs) of the image pixels. An audio file, another image, or text can all contain a concealed message. The hidden information can only be extracted and interpreted by individuals who are aware of the embedding technique when the steganographic image is transmitted.

Image steganography has numerous important and varied uses in many different industries. It improves security and privacy in secure communication by offering a means of sending private information without drawing notice to itself. In order to safeguard intellectual property, it is also utilised in digital watermarking, which embeds copyright data into digital media. Furthermore, image steganography is essential to clandestine operations since it permits the safe sharing of data in intelligence and military settings. Moreover, digital forensics uses it to incorporate authentication data, guaranteeing the validity and integrity of digital evidence. The goal of steganographic technology development is to continuously enhance the resilience, capability, and imperceptibility of the concealed data, making it an indispensable instrument in the dynamic field of data security.

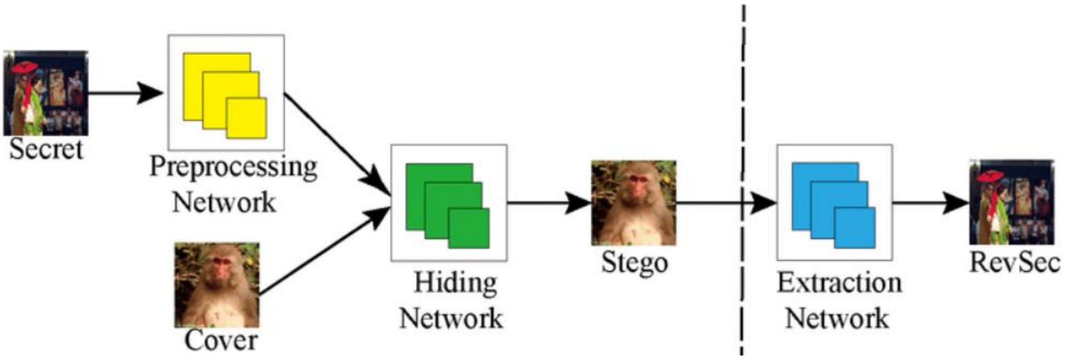


Figure 1.1 Image Steganography Architecture

1.3 Methods of Image Steganography

Image steganography is the umbrella term for a variety of techniques, each of which has a unique mechanism for encoding secret information into images. These methods fall into two basic categories: spatial domain methods and transform domain methods.

Spatial Domain Techniques

These techniques involve directly changing the pixel values of the cover image to embed the secret data. These techniques are straightforward and can be easily put into practice. Some common spatial domain techniques include:

Least Significant Bit (LSB) Insertion:

This is the most popular way in which the secret data bits are substituted for the least important bits of the pixel values. The secret information is invisible to the human eye because alterations to the LSBs cause very little distortion in the visual field. LSB matching and LSB substitution are two LSB insertion variations.

Pixel Value Differencing (PVD):

This technique modifies the disparities between neighbouring pixel values to incorporate data. The strategy makes sure that the hidden data is less visible, especially in areas of the image with considerable fluctuations, by carefully altering the differences.

Random Pixel Embedding:

In this approach, the secret data is encoded in randomly selected pixels, making it more resistant to steganalysis. The randomization makes it difficult for attackers to determine which pixels contain the secret data.

Transform Domain Techniques

Transform domain approaches incorporate data in the image's frequency domain. These approaches are often more resilient against image processing assaults such as compression and filtering. Common transform domain approaches include the following:

Discrete Cosine Transform (DCT):

It is widely employed in JPEG compression, converts a picture into frequency components. Secret data is contained in high-frequency components that are less visible to the human eye but can withstand a variety of compression methods.

Discrete Wavelet Transform (DWT):

DWT breaks down the image into numerous resolution levels, collecting both spatial and frequency information. Data may be embedded in the wavelet coefficients of these sub bands, resulting in high embedding capacity and resilience to image processing processes.

Discrete Fourier Transform (DFT):

DFT converts the spatial domain image into its frequency domain representation. By embedding data in the magnitude and phase components of the frequency domain, DFT-based steganography can achieve good imperceptibility and robustness.

1.4 Research Goal

In our literature study, we seek to look into prior image steganography approaches, including their evolution throughout time, methodology used, difficulties faced, and future directions. This assessment will consider both the advantages and disadvantages of these approaches.

1.5 Organisation Of Report

The succeeding chapters of the thesis include:

Chapter 2 of the thesis will explore similar work in image steganography. Here, we look at the breadth and limits of past literature reviews, as well as how our study will build on them. **Chapter 3** describes in detail the framework of our literature review and the method that we proposed. It also goes into detail on the obtained output and the evaluation metrics used. **Chapter 4** presents the generated results, contrasts the models investigated, and derives conclusions from them. **Chapter 5** finishes the analysis and outlines future research directions for the topic.

CHAPTER 2

LITERATURE SURVEY

This section evaluates newly published research and outlines the advantages and disadvantages of the algorithms suggested in these studies.

Ghosal et al. [1] emphasis on the LT in image steganography instead of typical methods. They gave insights into the benefits of LT over traditional techniques and several alternative transformations, but security concerns, embedding capacity, and SI quality were some areas that needed to be addressed.

Kalita et al.'s [2] approach is based on IWT and LSB. They show that, while no data was lost and the algorithm was resilient, the visual distortion was significant and there was a lack of payload capacity.

The Nazari et al. [3] technique uses FIS and DCT with HVS settings to improve imperceptibility and optimise the number of FIS rules. However, the payload is not satisfactory.

Ghosal et al. [4] proposed a quicker and more robust technique based on the Lah transform, although it does not handle compressed picture formats like JPEG.

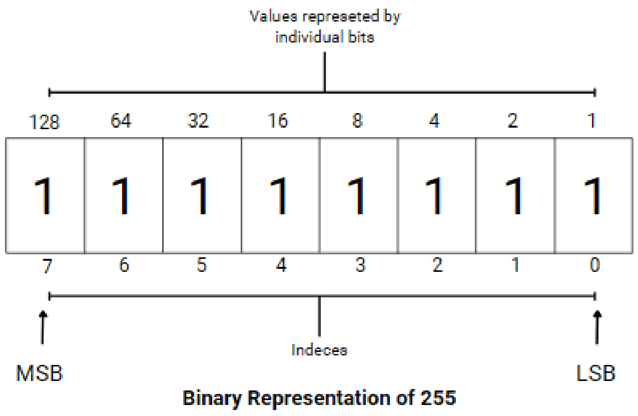
While these studies cover the many approaches, advantages, drawbacks, and difficulties associated with picture steganography, we were unable to locate any that really addressed the thorough optimization of embedding capacity while preserving the least amount of distortion. Therefore, the purpose of our literature analysis is to investigate modern methods that may be utilised in steganography, with an emphasis on enhancing the aforementioned critical areas. Our discussion will encompass the development, approaches, obstacles, and potential paths of these methods, with the goal of tackling security issues and useful implementations in various image formats.

CHAPTER 3

METHODOLOGY

3.1 Least Significant Bits (LSB)

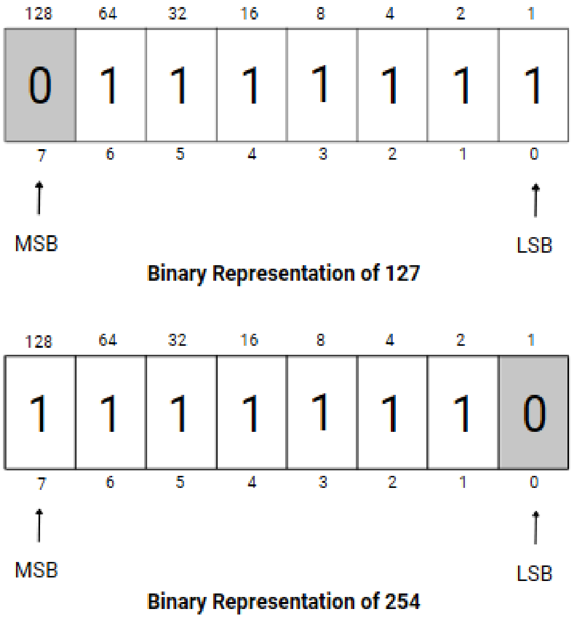
LSBs, or Least Significant Bits, are the bits in a binary number with the lowest value and the smallest influence on the total value. In digital photographs, each pixel's colour may be represented by a binary value, with the LSB being the rightmost bit. In the context of image steganography, the LSB approach entails changing the pixel value's least significant bits to contain hidden information. This approach allows for small alterations that are usually invisible to the human eye, making it an efficient means to conceal information.



Values represeted by individual bits
128
64
32
16
8
4
2
1
1
1
1
1
1
1
1
1
7
6
5
4
3
2
1
0
Indeces
MSB
LSB
Binary Representation of 255

Figure 3.1 Binary Representation of a Decimal Number

In image steganography, for example, changing the LSB of a pixel value from 11111111 to 11111110 to incorporate a bit of data causes minimal observable change as contrasted to that of MSB, as demonstrated in Fig 3.2, where altering the MSB creates a massive difference. The LSB approach is simple and provides great imperceptibility, but it is susceptible to assaults and changes such as lossy compression, which may readily disturb the concealed data. Furthermore, the quantity of pixels in the image limits the ability to hide data. Despite these drawbacks, LSB steganography is still a common method for concealing data since it is simple and effective.



Binary Representation of 127

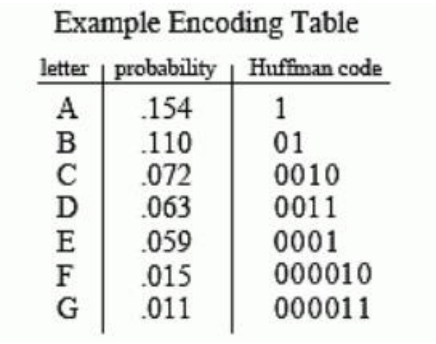
Binary Representation of 254

Figure 3.2 Bit Embedding in MSB and LSB

3.2 Huffman Encoding

David A. Huffman created Huffman encoding, a prominent method of lossless data compression, in 1952. It is used to minimise data size while retaining all information by assigning shorter binary codes to more often appearing characters and longer codes to less frequently occurring ones. This variable-length coding system guarantees that the most popular characters utilise fewer bits, hence reducing the amount of space required to store or transmit data.

Huffman encoding requires numerous processes. First, the frequency of each character in the supplied data is calculated. These frequencies are then used to create a binary tree called the Huffman tree (refer to Fig 3.3 & Fig 3.4), in which each leaf node represents a letter and its frequency. The Huffman tree is built by periodically joining the two nodes with the lowest frequencies until only one remains. The last node serves as the Huffman tree's root. Each character's binary code is then assigned by traversing the tree from root to leaf, with left edges commonly allocated a '0' and right edges assigned a '1'



Example Encoding Table

letter	probability	Huffman code
A	.154	1
B	.110	01
C	.072	0010
D	.063	0011
E	.059	0001
F	.015	000010
G	.011	000011

Figure 3.3 Example of Huffman Table

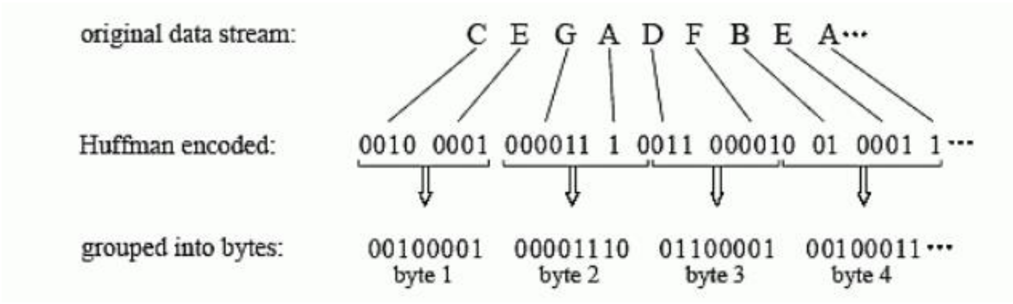


Figure 3.4 Example of Huffman Encoded data

Huffman encoding is a very efficient algorithm that is extensively utilised in a variety of applications, including file compression (e.g., ZIP files), picture formats (e.g., JPEG), and even network data transfer to optimise bandwidth utilisation. Its key benefit is its capacity to modify code lengths to the actual distribution of characters in the data, resulting in high compression ratios. However, the efficiency of Huffman encoding is determined on the accuracy of the frequency analysis and the nature of the data; it performs best when the character frequencies vary widely. Despite its advantages, it may be surpassed by other sophisticated compression algorithms for some types of data, especially when more complicated patterns and redundancies are present.

3.3 Laguerre Transform

Originally, LT was published in continuous form; it was later modified to a discrete integer matrix version, allowing it to be used in image steganography. The Laguerre transform is based on pixel value addition and coefficient multiplication. LT for a matrix is provided by the following equation:

$$Lag = \left[\frac{1}{1-x}, \frac{x}{1-x}\right] \tag{1}$$

The ILT is calculated using:

$$Lag^{-1} = \left[\frac{1}{1+x'}\frac{x}{1+x}\right] \qquad (2)$$

The equation for the general term of LT is given below:

$$Lag(n,k) = \frac{n!}{k!} n_{C_k} \qquad (3)$$

Similarly, the equation for ILT is given below:

$$p_n = (-1)^{n-k}\frac{n!}{k!}\binom{n}{k} t_n \qquad (4)$$

Consider a pixel group of size m of the Cover Image, let $p_0, p_1 \; . \, . \, . \, . \, . \, . \, . \; p_n$ represent the pixels in the m-pixel group. If t_n represents the LT coefficients for the m-pixel group p_0, $p_1 \; . \, . \, . \, . \, . \, . \, . \; p_n$, we get:

$$t_n = \sum_{k=0}^{n} \frac{n!}{k!}\binom{n}{k} p_n \qquad (5)$$

Where n varies between 0 and m-1.

Therefore, if we consider 2-pixel groups at once and then apply LT on it the transformed components would be

$$t_i = \begin{cases} p_0 & \text{if } i = 0 \\ p_0 + p_1 & \text{if } i = 1 \end{cases} \qquad (6)$$

To retrieve the pixels of the 2-pixel group components, we use ILT on the modified components.

$$p_i = \begin{cases} t_0 & \text{if } i = 0 \\ -t_0 + t_1 & \text{if } i = 1 \end{cases} \qquad (7)$$

Similarly, if we consider 3-pixel groups at once and then apply LT on it the transformed components would be

$$l_i = \begin{cases} p_0 & \text{if } i = 0 \\ p_0 + p_1 & \text{if } i = 1 \\ 2p_0 + 4p_1 + p_2 & \text{if } i = 2 \end{cases} \tag{8}$$

To retrieve the pixels of the -pixel group components, we use ILT on the modified components.

$$p_i = \begin{cases} l_0 & \text{if } i = 0 \\ -l_0 + l_1 & \text{if } i = 1 \\ 2l_0 - 4l_1 + l_2 & \text{if } i = 2 \end{cases} \tag{9}$$

3.4 Proposed Algorithm

So, this technique is based on LT and Huffman encoding. LT is applied to CI non-intersecting pixel groups of size m taken in row-wise order, and the encoded secret message of the HI, generated by transforming the pixel matrix of the HI into a 1D row vector and applying Huffman encoding to it, is embedded by changing the cover image's LSBs. The number of bits encoded in each pixel can be adjusted appropriately. Once the embedding method is completed, we apply ILT to the embedded pixel group to retrieve the pixels to construct the SI, and then we utilize the adjustment technique to correct any excessive distortion without modifying the embedded data. Similarly, we use the same approach to extract the hidden bits from the Stego image. The retrieved secret bits are then rearranged to obtain the secret image.

In the next two sections, Section 3.4.1 and Section 3.4.2, we take a deep dive into the embedding and extraction technique. In the final section, section 3.4.3, we demonstrate the procedure using an example.

3.4.1 Embedding Algorithm

So, in the embedding technique, the first step is to reshape the CI based on the number of pixels in the pixel group, ensuring that the CI is correctly divided into these non-overlapping groups. After reshaping the CI, the HI is reshaped from a pixel matrix into a 1D row vector, and then Huffman encoding is applied to the 1D row vector to produce the Huffman dictionary and Huffman encoded data. So, to begin embedding the Huffman encoded data, we break the reshaped CI into m-pixel groups and alter the LSB of the pixels. The amount of changed bits per pixel is determined by the size of the pixel grouping and the bits per pixel (bpp) required for the Stego image. Once the embedding is complete, we adjust the pixel values if feasible without affecting the concealed data. After pixel correction, we use ILT to obtain and rearrange the pixel groups to create the Stego Image.

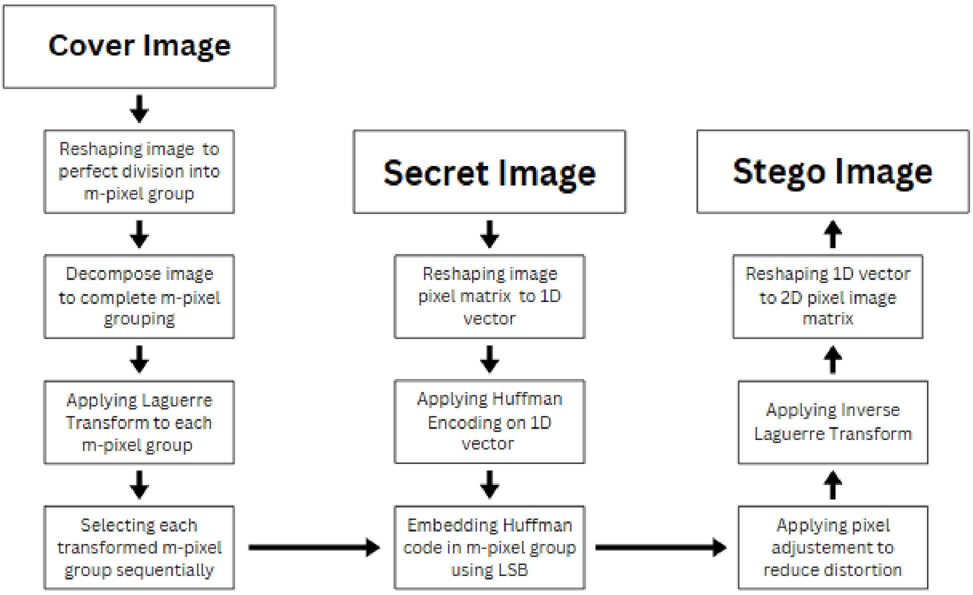

Cover Image
Reshaping image to perfect division into m-pixel group
Decompose image to complete m-pixel grouping
Applying Laguerre Transform to each m-pixel group
Selecting each transformed m-pixel group sequentially
Secret Image
Reshaping image pixel matrix to 1D vector
Applying Huffman Encoding on 1D vector
Embedding Huffman code in m-pixel group using LSB
Stego Image
Reshaping 1D vector to 2D pixel image matrix
Applying Inverse Laguerre Transform
Applying pixel adjustement to reduce distortion

Figure 3.5 Flow diagram of the Embedding Algorithm

To obtain the desired b bits per pixel (bpp), we use the following format:

- If the pixel group size is 2 and we require b bits per pixel (bpp, we embed b bits in both the pixels of the pixel group, ensuring the same tolerance level of both the pixels.

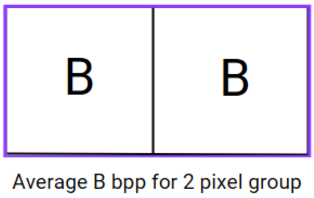


Figure 3.6 LSB embedding format for 2-pixel group

- If the pixel group size is 3 and we require b bits per pixel (bpp) embedded, we follow the [b, b-1, b+1] order, which ensures the average of b bits per pixel (bpp) for the SI and the third pixel has higher tolerance level against distortion as compared to the second pixel.

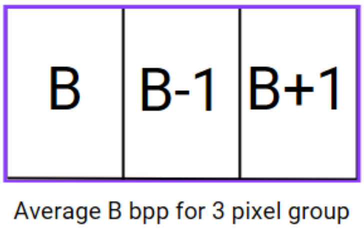


Figure 3.7 LSB embedding format for 3-pixel group

3.4.2 Extraction Algorithm

In the extraction technique, the initial step is to deconstruct the SI into nonintersecting pixel groups, following that we use LT on the groups followed by the extraction of bits. Once all the secret bits are retrieved they are decoded using the Huffman dictionary and we retrieve the original 1D pixel row vector that is reshaped to the 2D-pixel matrix based upon the size of the HI.

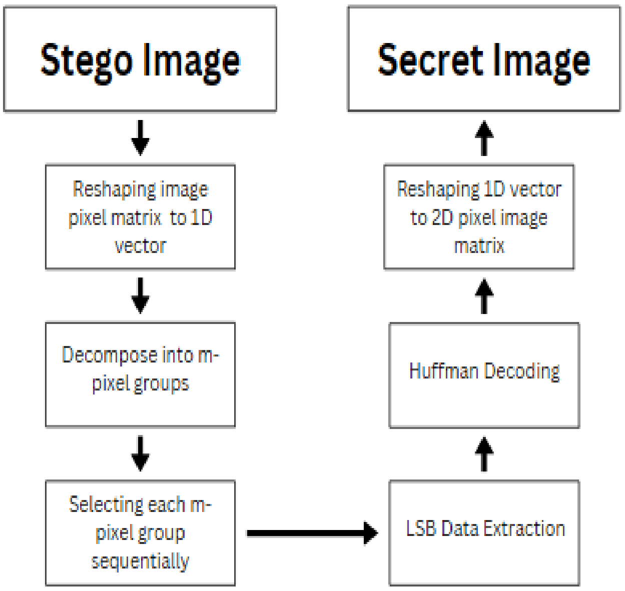

Stego Image
Reshaping image pixel matrix to 1D vector
Decompose into m-pixel groups
Selecting each m-pixel group sequentially
LSB Data Extraction
Huffman Decoding
Reshaping 1D vector to 2D pixel image matrix
Secret Image

Figure 3.8 Flow diagram of the Extraction Algorithm

3.4.3 Example

Embedding

Consider a 3-pixel group (x, y, z), we need to embed the secret data (101101010) and the bits per pixel (bpp) considered is 3. Consequently, we will embed (3,2,4) bits, in accordance with the embedding format.

(x, y, z) = [72, 185, 240]

Applying LT on the 3-pixel group is the initial step, from which we obtain the altered values (a, b, c).

(a, b, c) = LT(x, y, z) = LT(72 , 185, 240) = [72, 257,1124]

The respective binary representation of LT is

(a, b, c) = (0100 1000, 0001 0000 0001, 100 0110 0100)

Now embedding the secret data (101101010) w.r.t (3,2,4) format in (a, b, c)

(a, b, c) = LSB(0100 1**101**, 0001 0000 00**10**, 100 0110 **1010**)
= (77, 258, 1130)

Now ILT is applied to retrieve the pixel group for Stego image

(x_o, y_o, z_o) = ILT(77, 258, 1130)
= (77, 181, 252)

Now the retrieved values are compared with the original values and if the distortion is significant the we will apply pixel adjustment

(i) As $| x - x_o | = 0 < 2^3$, no pixel adjustment is required

(ii) As $| y - y_o | = 4 = 2^2$, no pixel adjustment is required

(iii) As | z - z_O | = 12 < 2^4, no pixel adjustment is required.

After embedding our secret data, the final pixel values are (x_o, y_o, z_o) = [77, 181, 252].

Extraction

We will now apply LT on the bits in order to extract the secret data, and we will do it using the same format, which is [3 2 4]. We retrieve the hidden bits (101101010).

(i) x_O - 0100 1**101** → LSBExtraction(0100 1101,3) = 101

(ii) y_O - 0001 0000 00**10** → LSBExtraction(0001 0000 0010,2) = 10

(iii) z_O - 100 0110 **1010** → LSBExtraction(100 0110 1010,4) = 1010

So in the following part, we will analyse the outcomes of the proposed method and the parameters utilised for the evaluation of the findings.

3.5 Evaluation Metrics

PSNR (Peak Signal-to-Noise Ratio)

Peak Signal-to-Noise Ratio, or PSNR, is a commonly used statistic to assess the quality of steganographic pictures. It calculates the ratio of an image's maximal potential power to the level of noise distortion that reduces the representational quality of the image. PSNR is a metric used in image steganography to measure the degree to which the cover image has been compromised during the embedding process.

The mean squared error (MSE) between the original and stego images is used to compute the PSNR. The equation is:

$$PSNR = 10 \cdot \log\left(\frac{MAX^2}{MSE} \right) \qquad (11)$$

Where MSE is the mean squared error between the original and stego pictures, and MAX is the maximum possible pixel value of the image (for example, 255 for an 8-bit image). Greater image quality is indicated by a higher PSNR value, which also means that the embedded data is less noticeable and the stego image is more comparable to the cover image. For the majority of steganographic applications, PSNR values more than 30 dB are usually regarded as appropriate, guaranteeing that the hidden data does not materially impair the image's visual quality. Consequently, the formula below is used to determine PSNR for stego images.

$$PSNR = 10 \ \cdot \log\left(\frac{255^2}{MSE} \right) \tag{12}$$

Structural Similarity Index (SSIM)

A fundamental parameter for assessing picture quality in steganography is the Structural Similarity Index (SSIM). SSIM evaluates the perceived resemblance between the cover picture and the stego image by taking changes in structural information, brightness, and contrast into account, in contrast to PSNR, which measures absolute mistakes. The goal of SSIM is to more closely simulate how the human visual system perceives picture quality. The SSIM value can vary in between -1 and 1., where a value of 1 denotes perfect image similarity. An image with a higher SSIM value is less recognisable as a steganographic image since it preserves more of the original image's structural information. This metric is especially useful since it is a better measure of perceived picture quality because it is more in line with human visual perception. Using SSIM to assess stego image in image steganography helps guarantee that the embedded data does not materially change the image's visual content, preserving the legitimacy and use of the cover image.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+ C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma^2{}_x+\sigma^2{}_y+ C_2)} \tag{13}$$

Where:

μ_x and μ_y are the mean intensities of the two images x and y being compared

$\sigma^2{}_x$ and $\sigma^2{}_y$ are the variances of images x and y, respectively.

σ_{xy} is the variances of images x and y, respectively.

C_1 and C_2 are two constants

CHAPTER 4

Results and Conclusion

4.1 Results

The initial analysis is conducted using the Lena image (512 x 512) as the cover image (CI) and the Male.bmp image as the hidden image (HI). We varied the bits per pixel from 1 to 4 and experimented with 2-pixel and 3-pixel groups.

Cover Image 512 x 512	Bits Per Pixel (bpp)	Hidden Image	Resultant Image 512 x 512 2-pixel group	Resultant Image 512 x 512 3-pixel group	Retrieved Hidden Image 2-pixel group	Retrieved Hidden Image 3-pixel group
 Lena (512 x 512)	1	 Male (181 x 181)	 PSNR = 49.6438 MSE = 0.7058 SSIM = 0.9938	 PSNR = 46.2180 MSE = 1.5534 SSIM = 0.9867	 Male (181 x 181)	 Male (181 x 181)
	2	 Male (256 x 256)	 PSNR = 43.9024 MSE = 2.6514 SSIM = 0.9799	 PSNR = 38.5912 MSE = 8.9942 SSIM = 0.9308	 Male (256 x 256)	 Male (256 x 256)
	3	 Male (313 x 313)	 PSNR = 37.8773 MSE = 10.6012 SSIM = 0.9186	 PSNR = 32.7167 MSE = 34.7863 SSIM = 0.7935	 Male (313 x 313)	 Male (313 x 313)
	4	 Male (362 x 362)	 PSNR = 32.0206 MSE = 40.8340 SSIM = 0.7662	 PSNR = 26.8132 MSE = 135.4450 SSIM = 0.5534	 Male (362 x 362)	 Male (362 x 362)

Table 4.1 Initial Results of the proposed algorithm

We used five sets of photos from the USC-SIPI database as the CI for a more thorough study. The images used were resized to three different resolutions: 128 x 128, 256 x 256, and 512 x 512 pixels. The bits per pixel varied from one to four, and we utilised 2 and 3-pixel groups for LT.

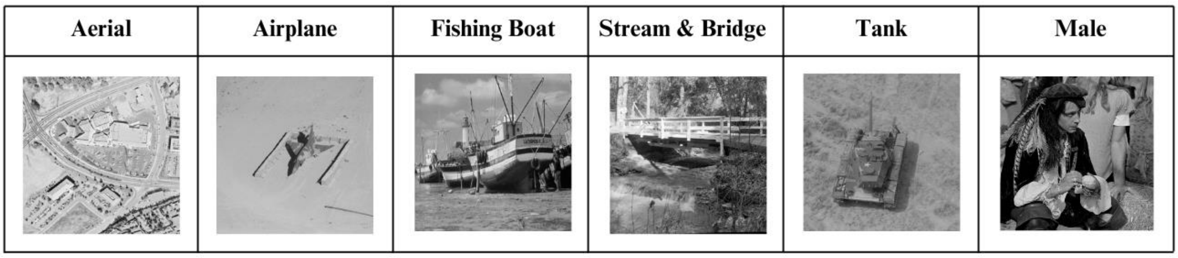
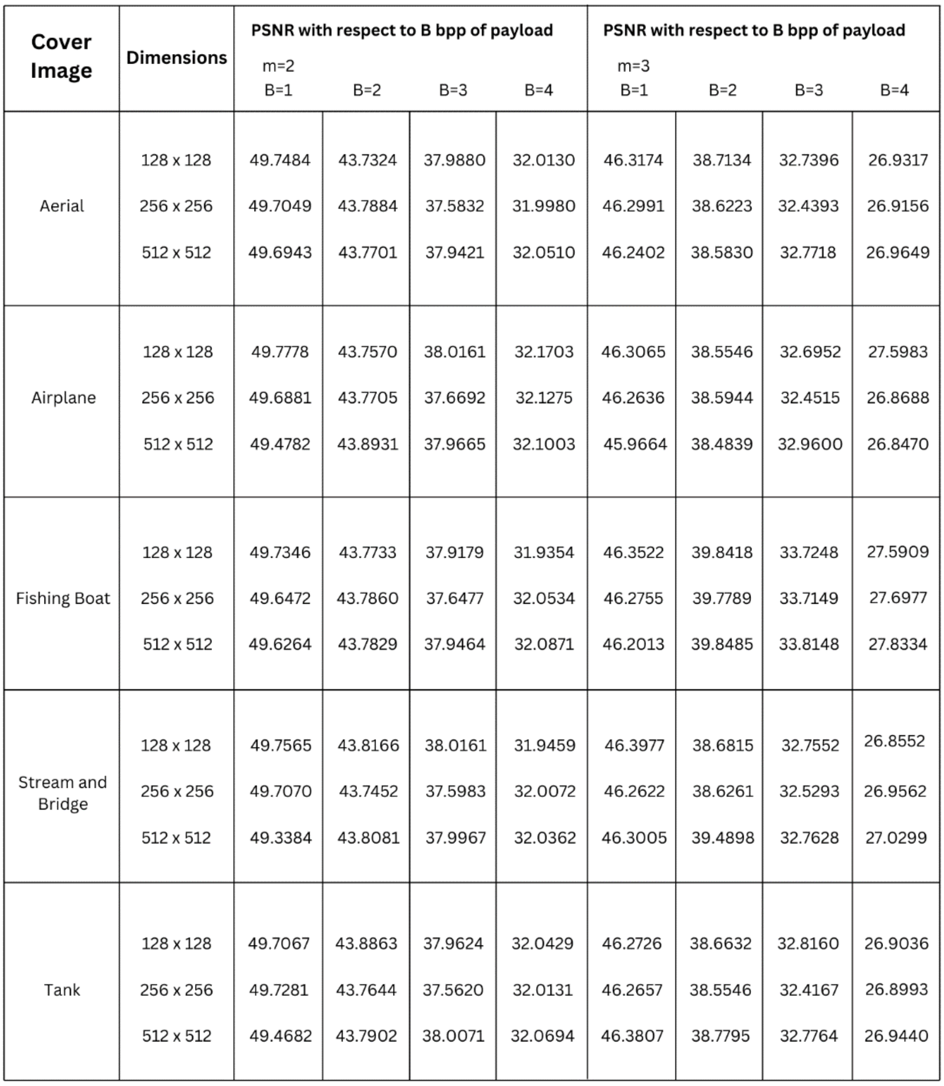


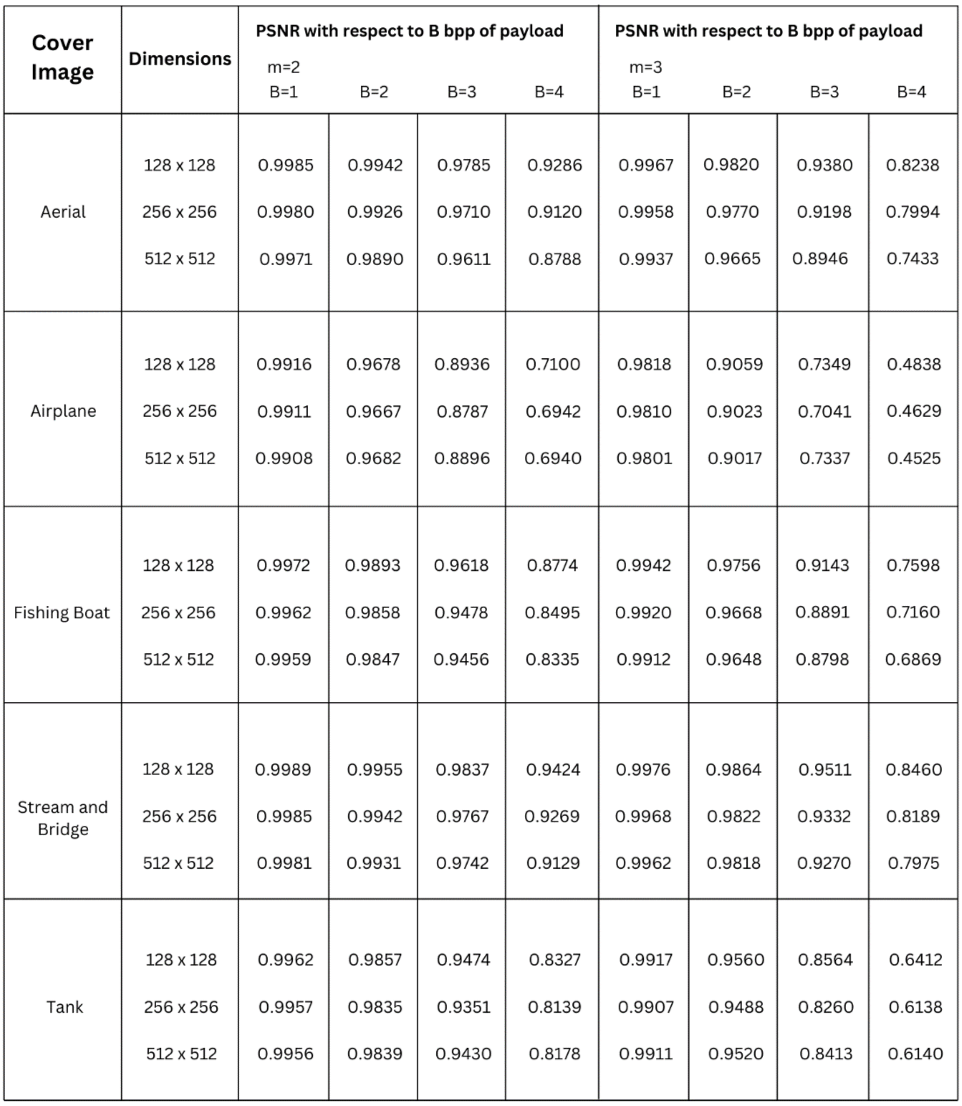
Figure 4.1 Test Images

The Steganographic image was evaluated based on two parameters PSNR and SSIM



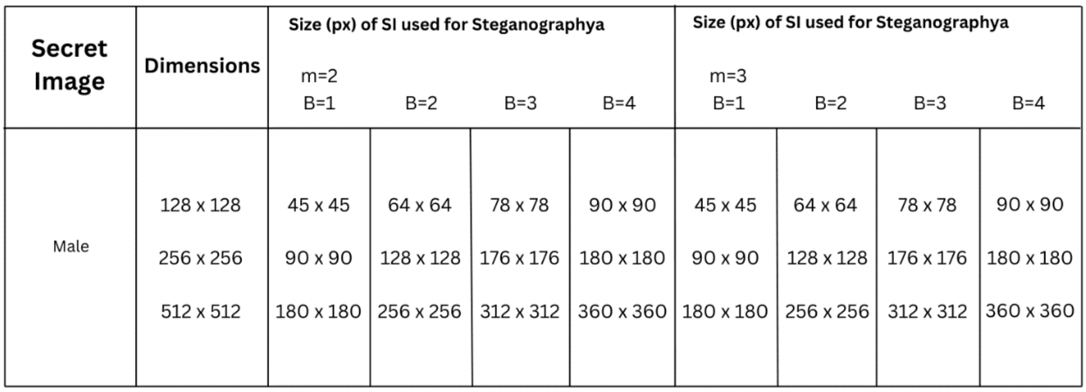
Cover Image	Dimensions	PSNR with respect to B bpp of payload m=2 B=1	B=2	B=3	B=4	PSNR with respect to B bpp of payload m=3 B=1	B=2	B=3	B=4
Aerial	128 x 128	49.7484	43.7324	37.9880	32.0130	46.3174	38.7134	32.7396	26.9317
	256 x 256	49.7049	43.7884	37.5832	31.9980	46.2991	38.6223	32.4393	26.9156
	512 x 512	49.6943	43.7701	37.9421	32.0510	46.2402	38.5830	32.7718	26.9649
Airplane	128 x 128	49.7778	43.7570	38.0161	32.1703	46.3065	38.5546	32.6952	27.5983
	256 x 256	49.6881	43.7705	37.6692	32.1275	46.2636	38.5944	32.4515	26.8688
	512 x 512	49.4782	43.8931	37.9665	32.1003	45.9664	38.4839	32.9600	26.8470
Fishing Boat	128 x 128	49.7346	43.7733	37.9179	31.9354	46.3522	39.8418	33.7248	27.5909
	256 x 256	49.6472	43.7860	37.6477	32.0534	46.2755	39.7789	33.7149	27.6977
	512 x 512	49.6264	43.7829	37.9464	32.0871	46.2013	39.8485	33.8148	27.8334
Stream and Bridge	128 x 128	49.7565	43.8166	38.0161	31.9459	46.3977	38.6815	32.7552	26.8552
	256 x 256	49.7070	43.7452	37.5983	32.0072	46.2622	38.6261	32.5293	26.9562
	512 x 512	49.3384	43.8081	37.9967	32.0362	46.3005	39.4898	32.7628	27.0299
Tank	128 x 128	49.7067	43.8863	37.9624	32.0429	46.2726	38.6632	32.8160	26.9036
	256 x 256	49.7281	43.7644	37.5620	32.0131	46.2657	38.5546	32.4167	26.8993
	512 x 512	49.4682	43.7902	38.0071	32.0694	46.3807	38.7795	32.7764	26.9440

Table 4.2 PSNR results of 5 Test Images



Cover Image	Dimensions	PSNR with respect to B bpp of payload m=2 B=1	B=2	B=3	B=4	PSNR with respect to B bpp of payload m=3 B=1	B=2	B=3	B=4
Aerial	128 x 128	0.9985	0.9942	0.9785	0.9286	0.9967	0.9820	0.9380	0.8238
	256 x 256	0.9980	0.9926	0.9710	0.9120	0.9958	0.9770	0.9198	0.7994
	512 x 512	0.9971	0.9890	0.9611	0.8788	0.9937	0.9665	0.8946	0.7433
Airplane	128 x 128	0.9916	0.9678	0.8936	0.7100	0.9818	0.9059	0.7349	0.4838
	256 x 256	0.9911	0.9667	0.8787	0.6942	0.9810	0.9023	0.7041	0.4629
	512 x 512	0.9908	0.9682	0.8896	0.6940	0.9801	0.9017	0.7337	0.4525
Fishing Boat	128 x 128	0.9972	0.9893	0.9618	0.8774	0.9942	0.9756	0.9143	0.7598
	256 x 256	0.9962	0.9858	0.9478	0.8495	0.9920	0.9668	0.8891	0.7160
	512 x 512	0.9959	0.9847	0.9456	0.8335	0.9912	0.9648	0.8798	0.6869
Stream and Bridge	128 x 128	0.9989	0.9955	0.9837	0.9424	0.9976	0.9864	0.9511	0.8460
	256 x 256	0.9985	0.9942	0.9767	0.9269	0.9968	0.9822	0.9332	0.8189
	512 x 512	0.9981	0.9931	0.9742	0.9129	0.9962	0.9818	0.9270	0.7975
Tank	128 x 128	0.9962	0.9857	0.9474	0.8327	0.9917	0.9560	0.8564	0.6412
	256 x 256	0.9957	0.9835	0.9351	0.8139	0.9907	0.9488	0.8260	0.6138
	512 x 512	0.9956	0.9839	0.9430	0.8178	0.9911	0.9520	0.8413	0.6140

Table 4.3 SSIM results of 5 Test Images



Secret Image	Dimensions	Size (px) of SI used for Steganographya m=2 B=1	B=2	B=3	B=4	Size (px) of SI used for Steganographya m=3 B=1	B=2	B=3	B=4
Male	128 x 128	45 x 45	64 x 64	78 x 78	90 x 90	45 x 45	64 x 64	78 x 78	90 x 90
	256 x 256	90 x 90	128 x 128	176 x 176	180 x 180	90 x 90	128 x 128	176 x 176	180 x 180
	512 x 512	180 x 180	256 x 256	312 x 312	360 x 360	180 x 180	256 x 256	312 x 312	360 x 360

Table 4.4 Resolution of Hidden Image used for Steganography

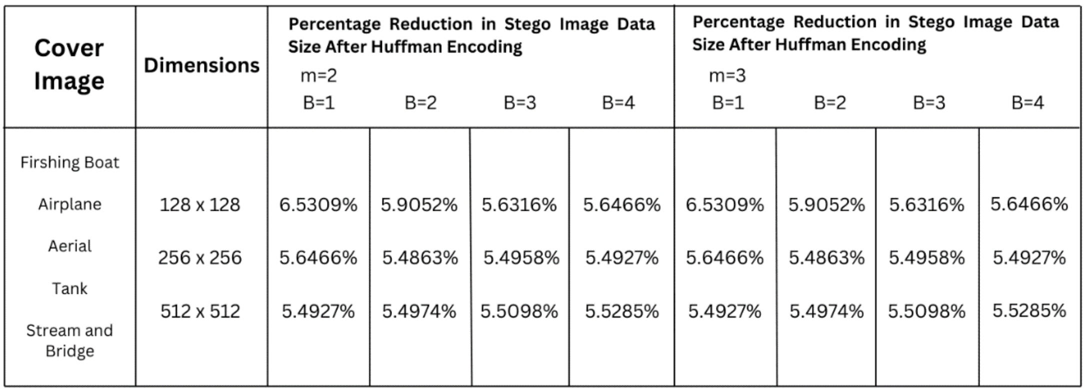
4.2 Conclusion

In conclusion, this work explored a variety of image steganography techniques intending to fully comprehend their unique characteristics and applications. The literature review emphasized the need to use a variety of approaches, each with pros and cons of its own while implementing image steganography. Through this investigation, we learned more about the wide spectrum of uses for image steganography, including covert operations, digital watermarking, and secure communication. Moreover, this work demonstrated the intrinsic trade-off between perceived invisibility and payload capacity. This inverse relationship—in which a higher chance of detectability was often associated with an increase in payload capacity—was noticed when we investigated various steganographic techniques. This result emphasises the necessity of striking a precise balance between the ability to conceal data and preserving the cover image's visual integrity. In summary, our study offered a thorough analysis of image steganography, stressing its importance, uses, and the trade-offs associated with using different methods. In conclusion, the proposed method demonstrates superior stego image quality, assessed through PSNR and SSIM metrics, along with an increased payload capacity.

CHAPTER 5

OBSERVATIONS AND ANALYSIS

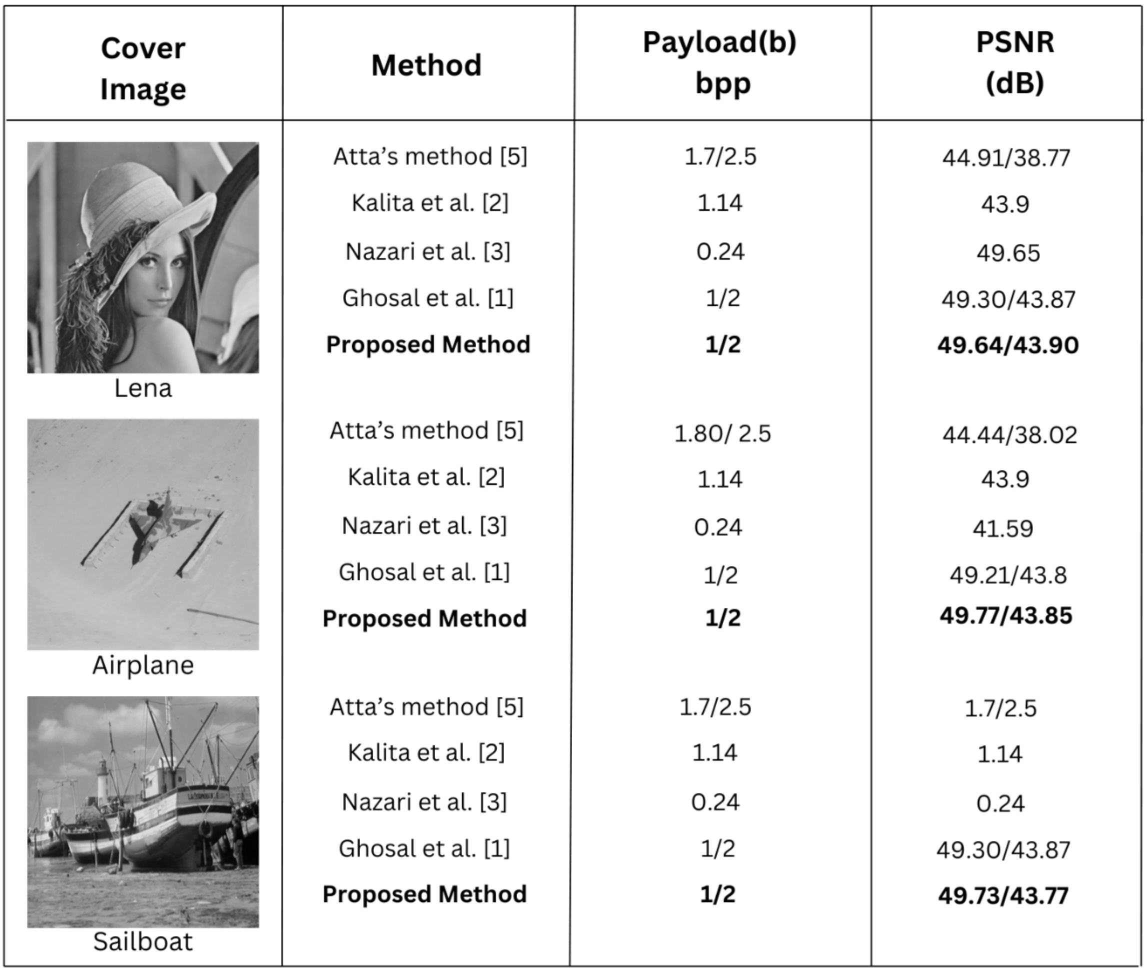
Table 4.1 demonstrates that, for three different resolutions, a 2-pixel group, and a 3-pixel group with bits per pixel ranging from 1-4, we have utilised the Male.bmp picture as HI and the Lena.bmp image as CI. When the payload was inserted using one bit per pixel, the 2-pixel group's highest PSNR value was 49.64; when the payload was embedded using four bits per pixel, the group's minimum PSNR value was 32.02. The SSIM value for the 2-pixel group showed a similar pattern, with 0.9938 being the most ideal value and 0.7662 being the least optimal value. Understandably, the trend that PSNR and SSIM followed was similar to that of the 2-pixel group, where the values considerably reduced with an increase in bits per pixel from 1 to 4. For the 3-pixel group, there was some degradation in PSNR and SSIM values as compared to the 2-pixel group. While the lowest PSNR was 26.81 and the least optimum SSIM value was 0.5534, the maximum PSNR for the 3-pixel group was 46.21 and the most optimal SSIM value was 0.9867. Compared to the Ghosal et al. [1] method, we could observe a slight increase in both parameters overall. Additionally, compared to the binary representation of the hidden image, the encoded data occupies 5.5% less space on average, boosting the embedding capacity when compared to the Ghosal et al. [1] technique. Additionally, the pattern indicates that critical metrics like PSNR and SSIM have an inverse relationship with payload capacity.



Cover Image	Dimensions	Percentage Reduction in Stego Image Data Size After Huffman Encoding m=2				Percentage Reduction in Stego Image Data Size After Huffman Encoding m=3			
		B=1	B=2	B=3	B=4	B=1	B=2	B=3	B=4
Firshing Boat Airplane Aerial Tank Stream and Bridge	128 x 128	6.5309%	5.9052%	5.6316%	5.6466%	6.5309%	5.9052%	5.6316%	5.6466%
	256 x 256	5.6466%	5.4863%	5.4958%	5.4927%	5.6466%	5.4863%	5.4958%	5.4927%
	512 x 512	5.4927%	5.4974%	5.5098%	5.5285%	5.4927%	5.4974%	5.5098%	5.5285%

Table 5.1: Compression Percentage Using Huffman Encoding

Making reference to on to Tables 4.2 and 4.3, we examined a collection of 5 images (128 x 128, 256 x 256, and 512 x 512 pixels) that were selected as CI from the USC-SIPI database. To ensure that the complete HI is contained within the CI, the HI is resized throughout the analysis process in accordance with the dimensions listed in Table 4.4, depending on bits per pixel ranging from 1-4. We would like to mention how data compression was achieved through the use of Huffman encoding before discussing PSNR and SSIM.



Cover Image	Method	Payload(b) bpp	PSNR (dB)
Lena	Atta's method [5]	1.7/2.5	44.91/38.77
	Kalita et al. [2]	1.14	43.9
	Nazari et al. [3]	0.24	49.65
	Ghosal et al. [1]	1/2	49.30/43.87
	Proposed Method	**1/2**	**49.64/43.90**
Airplane	Atta's method [5]	1.80/ 2.5	44.44/38.02
	Kalita et al. [2]	1.14	43.9
	Nazari et al. [3]	0.24	41.59
	Ghosal et al. [1]	1/2	49.21/43.8
	Proposed Method	**1/2**	**49.77/43.85**
Sailboat	Atta's method [5]	1.7/2.5	1.7/2.5
	Kalita et al. [2]	1.14	1.14
	Nazari et al. [3]	0.24	0.24
	Ghosal et al. [1]	1/2	49.30/43.87
	Proposed Method	**1/2**	**49.73/43.77**

Table 5.2: Results of different Steganographic methods

Table 5.1 shows us that the HI was compressed using Huffman encoding up to 6.5% with an average compression of 5.7% for the collection of 5 photos stated in the table. It can have anything from 10,000 and 60,000 bits in terms of number. Because of Huffman encoding, our technique improves embedding capacity and security while offering much higher PSNR and SSIM values than methods offered by other review methods [1] [5] [2] [3], as shown in Table 5.2. In comparison to the embedding capacity of the Ghosal et al. [1] technique, this compression enhances the embedding capacity of the CI. From PSNR and SSIM assessment metrics, we can deduce that, in most situations, there was an improvement in parameters (including an increase in embedding capacity) when compared to the Ghosal et al. [1] technique. When bits per pixel are increased, a similar pattern of parameter deterioration is shown, since this increases the amount of distortion. The characteristics of the 2-pixel group were substantially better than those of the 3-pixel group because the combination of pixel values and coefficient multiplication causes the 3-pixel group to lead to substantially more distortion.

CHAPTER 6

Future Scope

6.1. Future Scope

Despite the considerable advancements made in picture steganography and the diverse array of techniques employed, including the innovative method proposed in this study, there remains ample opportunity for further exploration and enhancement. It is imperative to direct attention towards augmenting the payload capacity while concurrently refining performance metrics. Although Huffman encoding demonstrated notable improvements in embedding capacity and security, there exists potential for further enhancements in achieving higher levels of lossless compression percentage through continued research and development efforts. Additionally, there is scope for refinement in the quality of the resulting stego image, ensuring that the concealed data remains imperceptible while preserving the integrity of the cover image.

Upon contemplation of the project's results, it is clear that the quest for image steganography perfection is a never-ending process characterised by constant innovation and improvement. Subsequent research endeavours need to expand upon current methodologies, investigating creative ways to maximise payload capacity, fortify security protocols, and elevate the visual integrity of stego images.

REFERENCES

[1] S. K. Ghosal, S. Mukhopadhyay , S. Hossain and R. Sarkar, “Exploiting Laguerre transform in image steganography,” in *Computers & Electrical Engineering*, 2021.

[2] M. Kalita, T. Tuithung and S. Majumdar, “A new steganography method using integer wavelet transform and least significant bit substitution,” *The Computer Journal,* vol. 62, no. 11, p. 1639–1655, 2019.

[3] M. Nazari and I. D. Ahmadi, “A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity,” *A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity,* vol. 79, p. 13693–13724, 2020.

[4] S. K. Ghosal, S. Mukhopadhyay, S. Hossain and R. Sarkar, “Application of Lah transform for security and privacy of data through information hiding in telecommunication,” *Transactions on Emerging Telecommunications Technologies,* 2021.

[5] R. Atta and M. Ghanbari, “A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set,” *Journal of visual communication and image representation ,* vol. 53, pp. 42-54, 2018.

[6] R. Das and T. Tuithung, “A novel steganography method for image based on Huffman Encoding,” *2012 3rd National Conference on Emerging Trends and Applications in Computer Science,* pp. 14-18, 2012.

[7] N. Kanzariya, A. Nimavat and H. Patel, “Security of digital images using steganography techniques based on LSB, DCT and Huffman encoding,” *Proceeding of international conference on advances in signal processing and communication-elsevier,* 2013.

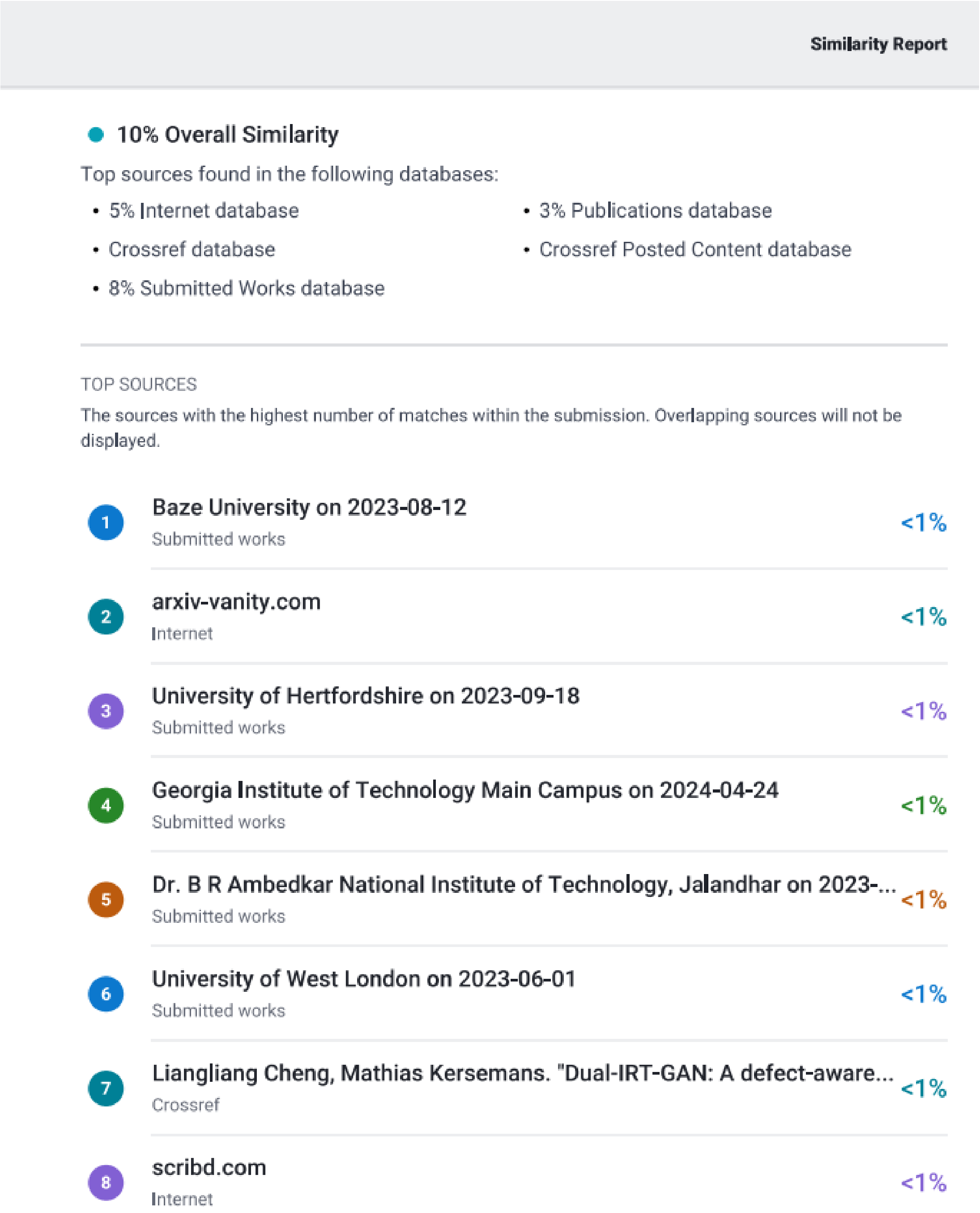
[8] A. Nag, S. Bishwas and P. Sarkar, “A novel technique for image steganography based on Block-DCT and Huffman Encoding,” arXiv, 2010.

[9] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, “Digital Image Steganography: Survey and Analysis of Current Methods,” *Signal Processing,* vol. 90, no. 3, pp. 727-752, 2010.

[10] V. Kumar and D. Kumar, “Performance evaluation of DWT based image steganography,” in *2010 IEEE 2nd International Advance Computing Conference (IACC)*, 2010.

[11] H. Alkhraisat, and . M. Habes, “4-Least Significant Bits Information Hiding Implementation and Analysis,” in *Proceedings of Graphics, Vision and Image Processing Conference*, 2005.

[12] R. Chu, X. You, X. Kong and X. Ba, “A DCT-based image steganographic method resisting statistical attacks,” in *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2004.



Similarity Report

● 10% Overall Similarity

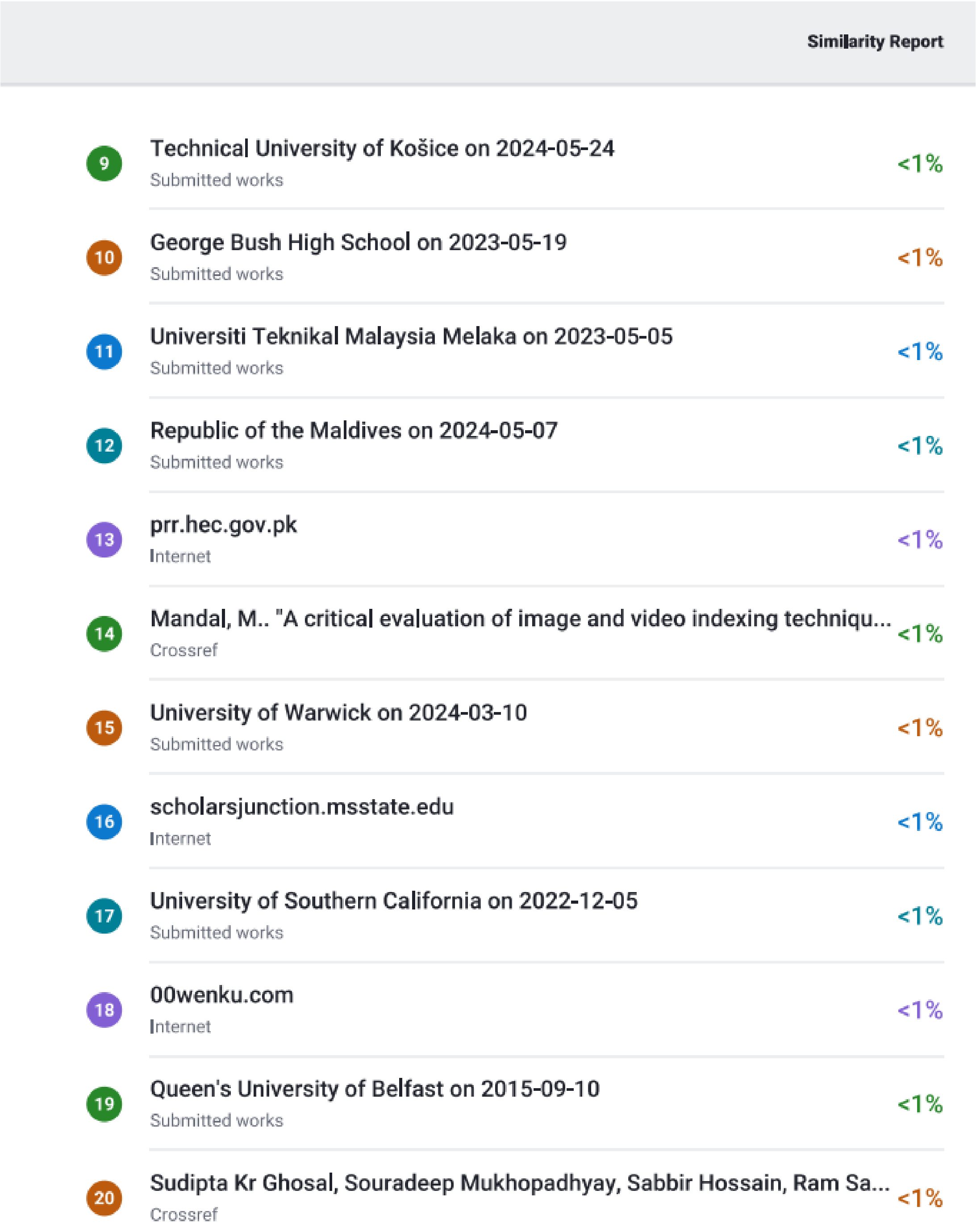
Top sources found in the following databases:

- 5% Internet database
- 3% Publications database
- Crossref database
- Crossref Posted Content database
- 8% Submitted Works database

TOP SOURCES

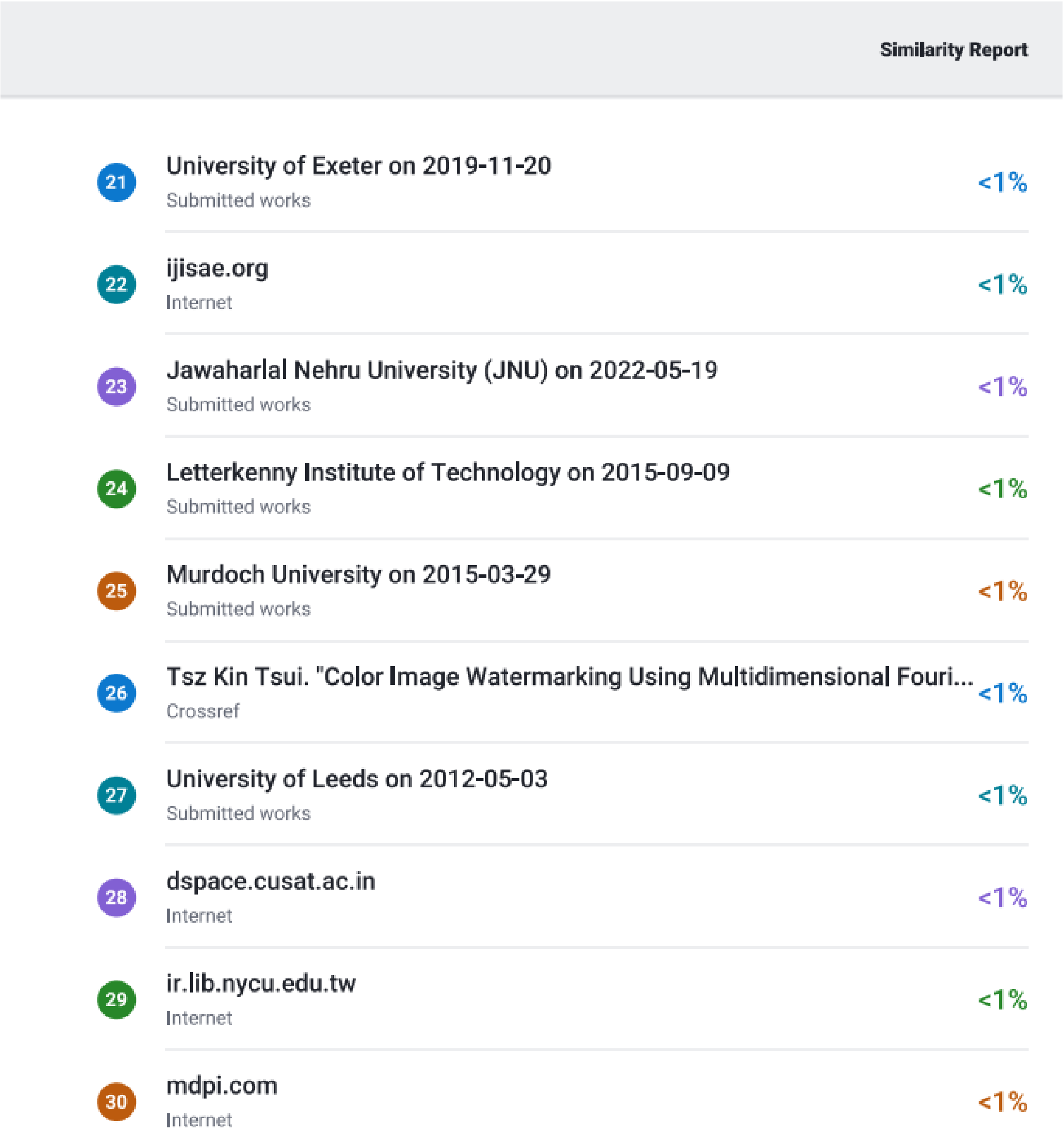
The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Baze University on 2023-08-12 Submitted works	<1%
2	arxiv-vanity.com Internet	<1%
3	University of Hertfordshire on 2023-09-18 Submitted works	<1%
4	Georgia Institute of Technology Main Campus on 2024-04-24 Submitted works	<1%
5	Dr. B R Ambedkar National Institute of Technology, Jalandhar on 2023-... Submitted works	<1%
6	University of West London on 2023-06-01 Submitted works	<1%
7	Liangliang Cheng, Mathias Kersemans. "Dual-IRT-GAN: A defect-aware... Crossref	<1%
8	scribd.com Internet	<1%



Similarity Report

9	Technical University of Košice on 2024-05-24 Submitted works	<1%
10	George Bush High School on 2023-05-19 Submitted works	<1%
11	Universiti Teknikal Malaysia Melaka on 2023-05-05 Submitted works	<1%
12	Republic of the Maldives on 2024-05-07 Submitted works	<1%
13	prr.hec.gov.pk Internet	<1%
14	Mandal, M.. "A critical evaluation of image and video indexing techniqu... Crossref	<1%
15	University of Warwick on 2024-03-10 Submitted works	<1%
16	scholarsjunction.msstate.edu Internet	<1%
17	University of Southern California on 2022-12-05 Submitted works	<1%
18	00wenku.com Internet	<1%
19	Queen's University of Belfast on 2015-09-10 Submitted works	<1%
20	Sudipta Kr Ghosal, Souradeep Mukhopadhyay, Sabbir Hossain, Ram Sa... Crossref	<1%



Similarity Report

21	University of Exeter on 2019-11-20 Submitted works	<1%
22	ijisae.org Internet	<1%
23	Jawaharlal Nehru University (JNU) on 2022-05-19 Submitted works	<1%
24	Letterkenny Institute of Technology on 2015-09-09 Submitted works	<1%
25	Murdoch University on 2015-03-29 Submitted works	<1%
26	Tsz Kin Tsui. "Color Image Watermarking Using Multidimensional Fouri... Crossref	<1%
27	University of Leeds on 2012-05-03 Submitted works	<1%
28	dspace.cusat.ac.in Internet	<1%
29	ir.lib.nycu.edu.tw Internet	<1%
30	mdpi.com Internet	<1%