DELHI TECHNOLOGICAL UNIVERSITY

Image Steganography

Major Project - II Presentation

YASH GUPTA 2K20/EC/241

What is an Image ?

An image is a two-dimensional signal defined by the mathematical function f(x,y), with the pixel value at any point determined by its x and y coordinates.

The figure is a digital image on a computer screen, but it's actually a three-dimensional RGB array of numbers between 0 and 255.

128	230	123
232	123	321
80	255	255

Fig.1 Typical RGB Image

At any point in time, each number represents the value of the function f(x,y). In this case, each of the values 128, 230, and 123 represents a single pixel value. The picture's dimensions are the dimensions of this two-dimensional array.

What is Steganography ?

Steganography Overview

- Art and science of writing hidden messages.
- Ensures only sender and recipient know the message's existence.
- Useful when open or encrypted messages aren't possible.
- Ensures secrecy, unlike cryptography.
- Aims to conceal secret messages and transfer data.
- Only authorized sender and receiver know the existence of the secret data.

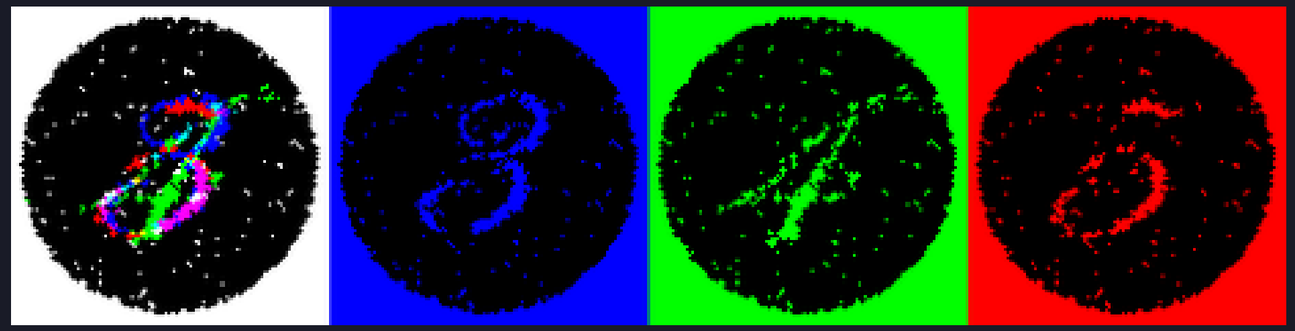


Fig.2 The same image revealed different hidden numbers when viewed through white, blue, green, and red lights.

Steganography is a technique that can be divided into four types: text steganography, image steganography, audio steganography, and video steganography, depending on the medium used.

Contrasting Steganography and Cryptography

- Steganography hides the message itself within innocuous data.
- Cryptography secures the message content by transforming it into an unreadable format.

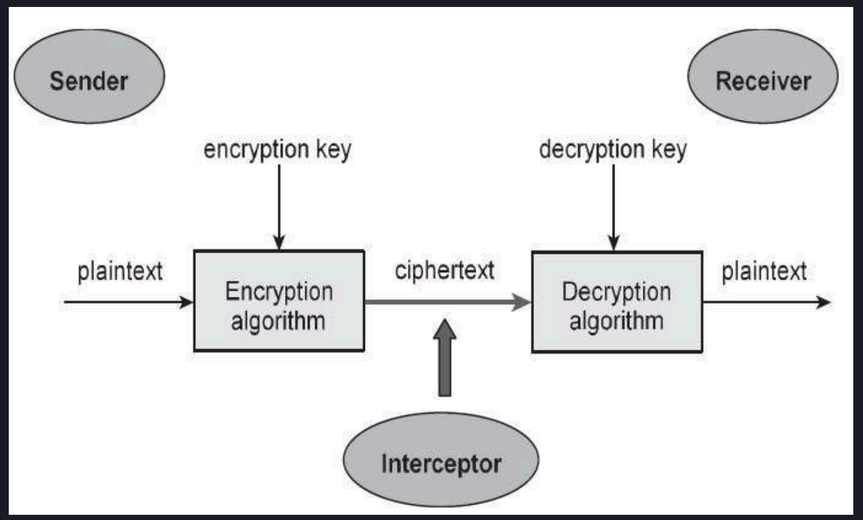


Fig. 3 Cryptography Diagram

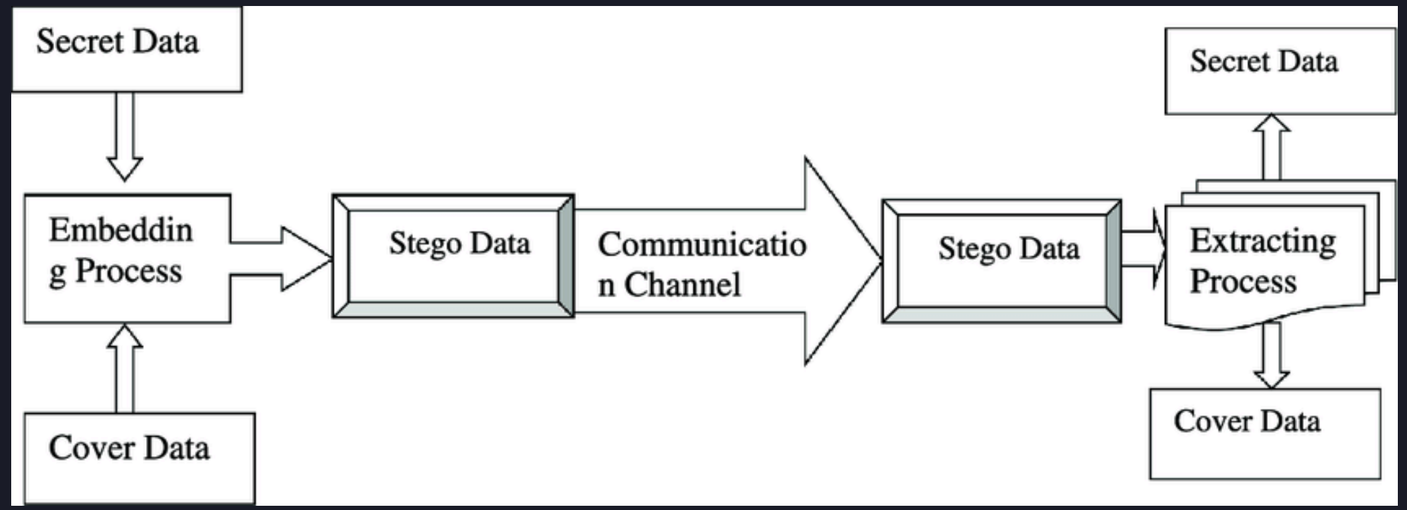


Fig. 4 Steganography Diagram

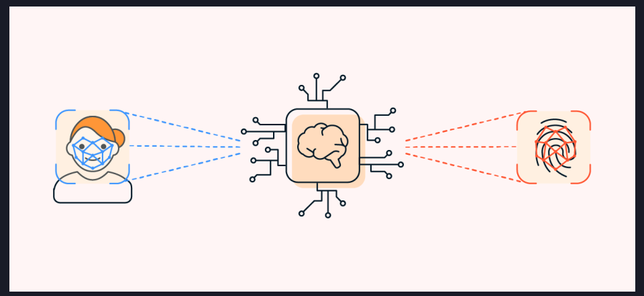
Applications of Steganography

- **Secure Communication:** Steganography ensures covert communication, providing an added layer of security by hiding messages within seemingly innocuous data.

- **Digital Watermarking:** Protecting intellectual property through the embedding of information in digital media, allowing for verification of authenticity and ownership.

- **Covert Channel Establishment:** Creating covert channels for secret communication within seemingly normal data, offering a discreet means of information exchange.

- **Biometric Data Protection:** Enhancing the security of biometric systems by concealing or encrypting biometric data within images.



Types of Steganography

The steganographic algorithms can be broadly classified into two categories:-

1. Spatial Domain Techniques
2. Transform Domain Techniques

1.) **Spatial Domain:-** These techniques use the pixel gray levels and their intensity values directly for encoding the message bits

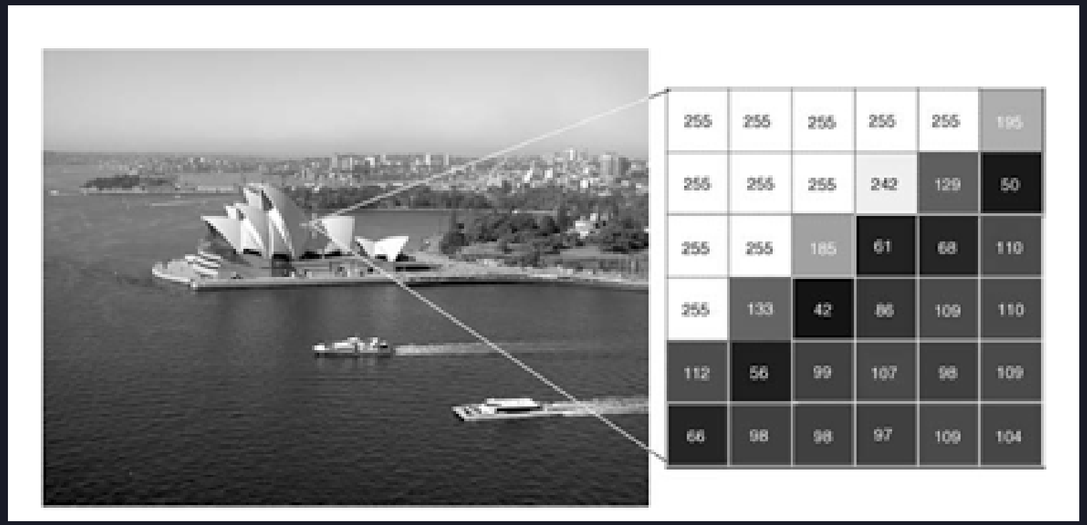
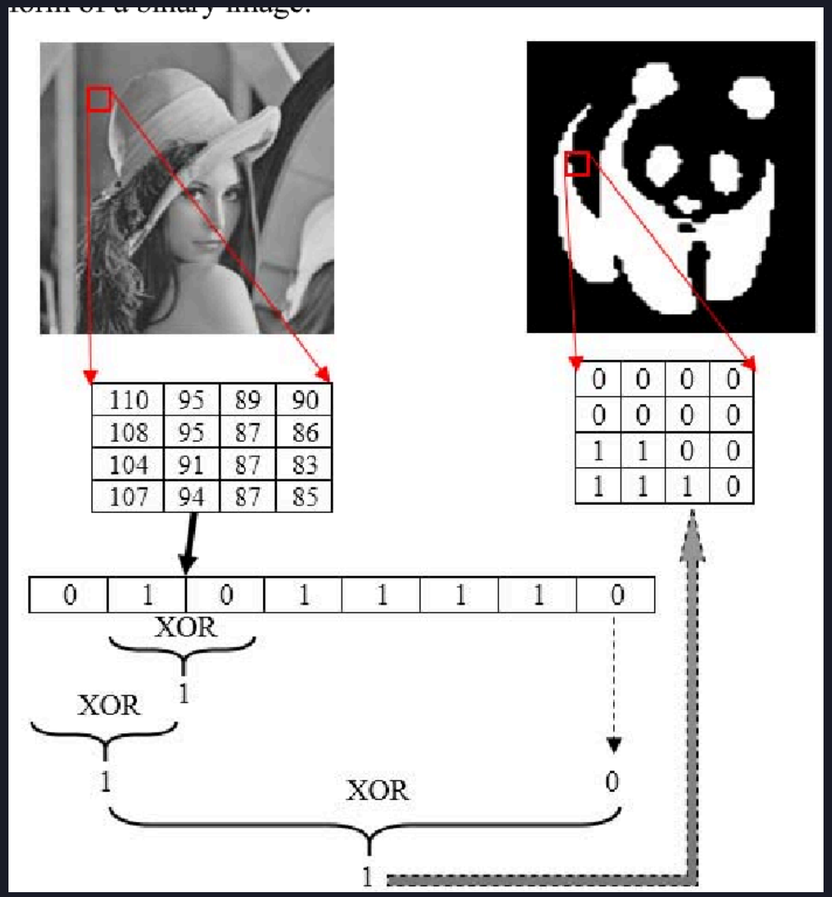


Fig 5. Pixel Representation of a Greyscale Image

- **Process**:
  - Choose a cover image.
  - Encode the secret information.
  - Embed it into the cover image using methods like LSB substitution, random pixel manipulation, or matrix encoding.

- **Transmission/Storage**: The modified image (stego-image) can be shared or stored like any regular image file.

- **Extraction**: Recipients utilize extraction algorithms to retrieve the hidden data while maintaining the cover image's integrity. This process reverses the embedding procedure.



2.) **Transform Domain Steganography:** These techniques try to encode message bits in the transform domain coefficients of the image. Some of the spatial domain techniques are -

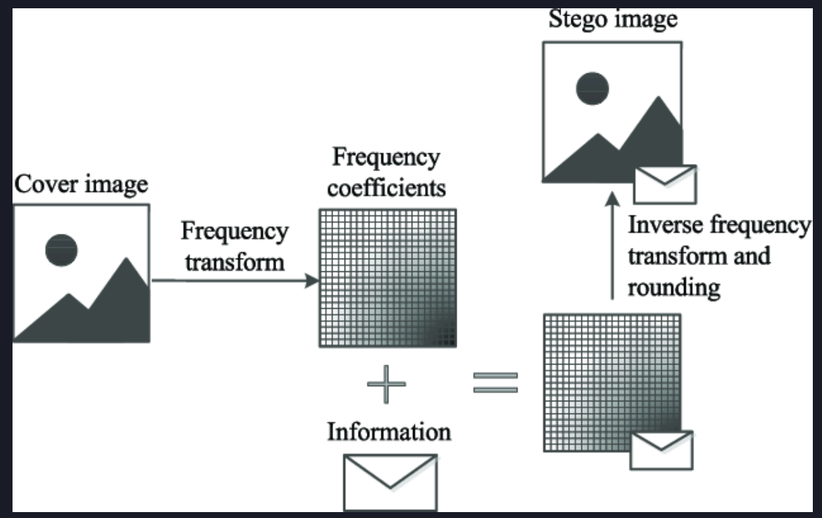


Fig 6. Transform Domain Steganography process

(i) **Discrete Cosine Transform (DCT):** Hides information in the frequency domain by modifying the coefficients obtained through the DCT of an image.

(ii) **Discrete Fourier Transform (DFT):** Conceals data in the frequency components obtained through the DFT, often used in audio steganography.

(iii) **Wavelet-based Steganography:** Utilizes the wavelet transform to embed information, providing high capacity and robustness.

Implemented Algorithm

Steganography and Its Application

• Steganography aims to communicate securely without revealing the true message.

• It involves a cover image and a stego-image, both with no secret message.

• The stego-image should not significantly diverge from the original cover image.

• Steganography is commonly used on computers, with digital data as carriers and networks as high-speed delivery channels.

• Implemented a steganographic algorithm that combines Least Significant Bit substitution, Laguerre Transform, and Huffman coding.

Key Features and it’s significance

Robustness, Capacity, and Security layering in steganalysis

- LSB, Laguerre Transform, and Huffman coding enhance the algorithm's robustness against common steganalysis techniques.
- Laguerre Transform and Huffman coding balance capacity and imperceptibility, enabling significant data hiding.
- Huffman coding optimizes hidden information compression, reducing redundancy and improving efficiency.
- Integrating LSB, LT, and Huffman adds security layers by distributing hidden information across spatial and frequency domains.
- LSB and Frequency adjustment minimize visual impact.
- LT and Huffman coding provide high payload capacity.
- Balances simplicity and effectiveness.
- Adaptable to different image types.
- Resists common steganalysis methods.

Least Significant Bit

LSB Embedding in Image Steganography

- Fundamental technique in image steganography.
- Modifies least significant bit of pixel values without significant visual alteration.
- Pixel values are represented in binary, with the least significant bit being the rightmost bit.
- LSB substitution replaces the least significant bit with hidden message bits, making it imperceptible to the human eye.
- Suitable for hiding text or binary data within images.
- Trade-off between hiding capacity and imperceptibility. Higher capacity may result in noticeable changes, lower capacity ensures subtler concealment.

- Here is an example of working of the Least Significant bit

Fig 7. Pixel modification of a Greyscale Image

Image Analysis: MSB vs LSB Impact

- MSB changes significantly impact the final value.
- LSB changes have minimal impact.
- Least significant bit of steganography used.

Huffman Encoding

Huffman Coding Overview

- An entropy coding technique assigning variable-length codes to symbols based on frequency.
- Applied after LSB substitution and DCT transformation phases for compression and storage optimization.
- Uses shorter codes for frequent symbols and longer codes for less frequent ones.
- A lossless compression technique, ensuring no data loss during encoding and decoding.
- Reduces embedded data size, maximizing payload capacity within the steganographic image.
- Adaptable to different types of embedded data, enhancing algorithm robustness.

Working of Huffman Coding

Huffman Encoding:

- Frequency Analysis: Analyze symbol frequencies in the input data.
- Building the Tree: Construct a Huffman tree based on frequencies.
- Generating Codes: Assign variable-length codes to symbols.
- Creating Bitstream: Replace symbols with codes for compression.

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

Fig.8 Huffman Table

Huffman Decoding:

- Reconstructing Tree: Share Huffman tree knowledge.
- Decoding Bitstream: Traverse tree to decode bits into symbols.
- Mapping Symbols: Assign symbols to reconstruct the original data.
- Result: Efficiently compress and decompress data.

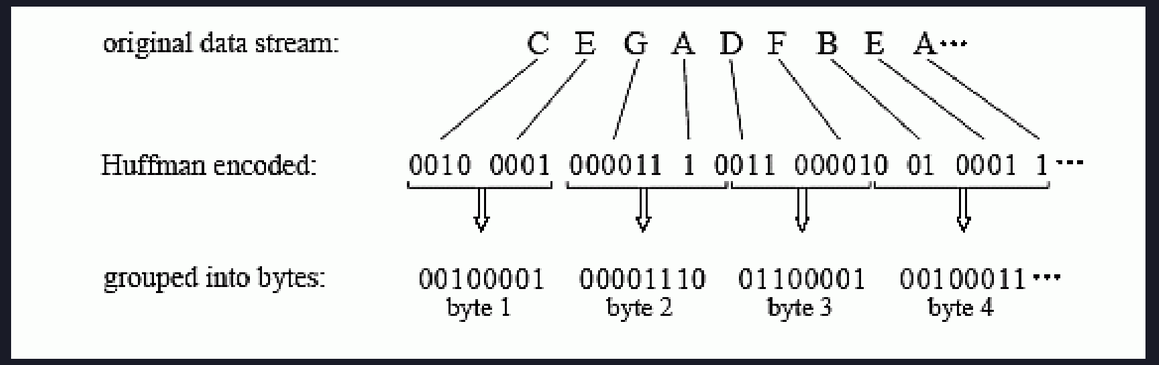


Fig. 9 Huffman Encoding

Laguerre Transform

Laguerre Transform: A New Method for Embedding Hidden Information in Digital Images

- Highlighted for its integer-based calculation, enabling faster operations without data loss.
- Applied in the transform domain to process image data for embedding hidden information.
- Transformed coefficients calculated based on pixel values of image blocks.
- Both forward and inverse transforms are equivalent, ensuring data integrity.
- Supports a wide range of image formats, expanding its applicability beyond JPEG files.

Laguerre Transform

The equation of general term of LT is :

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

The transformed pixel of the pixel group is represented as:

$$t_n = \sum_{k=0}^{n} \frac{n!}{k!} \binom{n}{k} p_n$$

To retrieve the pixel of the pixel group we use ILT:

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

Implementation Algorithm

- Flow Chart Diagram of the Embedding process

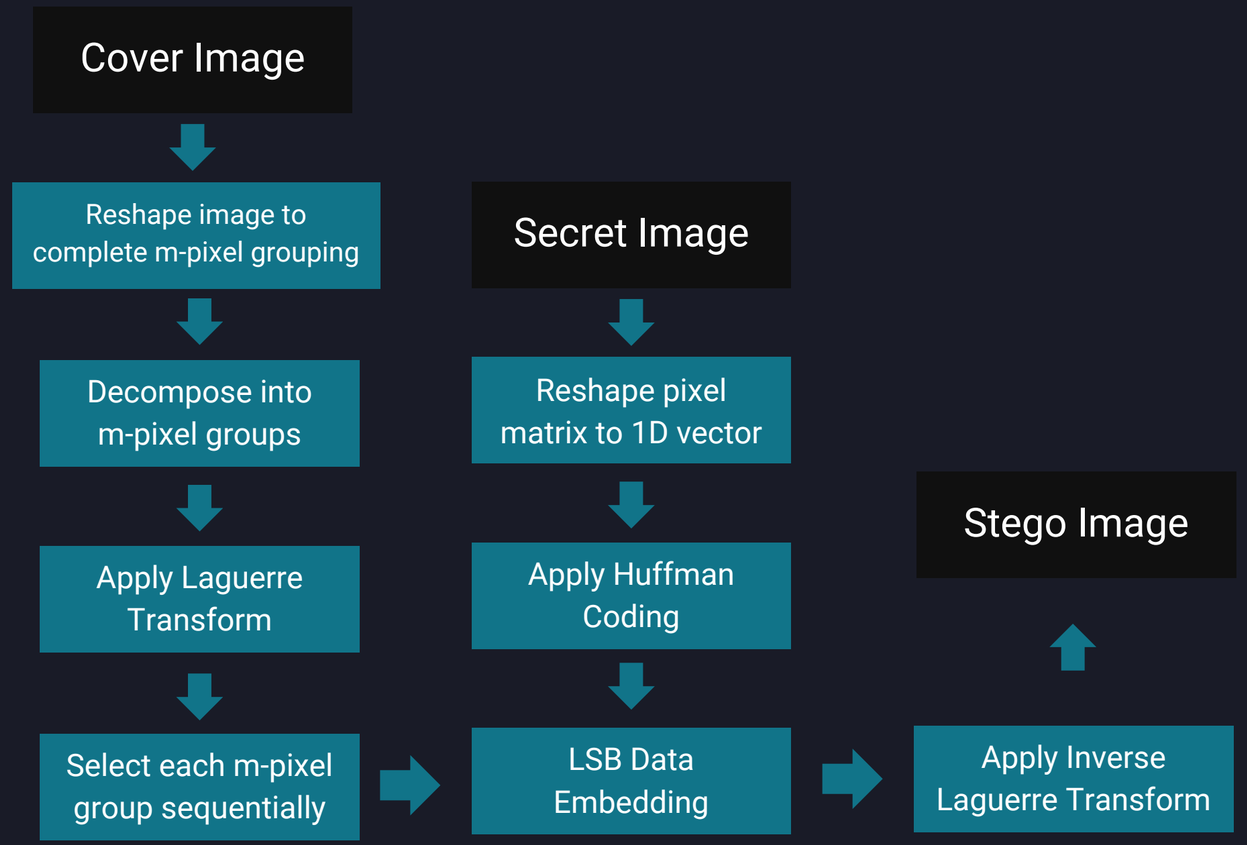


Fig. 10 Flow Chart for data embedding algorithm

- Flow Chart Diagram of the Extraction process

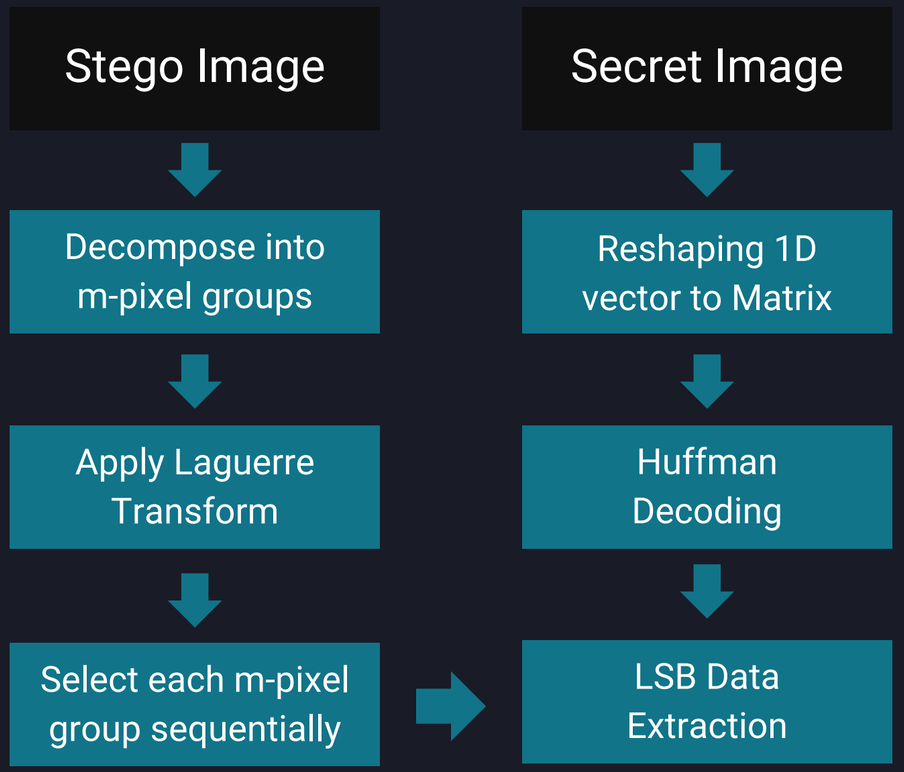


Fig. 11 Flow Chart for data extraction algorithm

Methodology for Embedding

Input: An image acting as a carrier and a secret message/picture.
The result is a stego-image.

1. Reshape the cover image so that it can be divided into non-overlapping m-pixel groups

2. Get the Huffman table of the secret picture.

3. Determine the Huffman encoded binary bit stream of the secret image using the Huffman table acquired in step 1.

4. Determine the size of the encoded bit stream in bits.

5. Divide the carrier picture into non-overlapping m-pixel groups for each of the cover image's blocks.

6. Apply Laguerre Transform to the m-pixel group

7. Insert the bits into the cover image m-pixel group sequentially using the LSB method.

8. Repeat for each m-pixel group acquired in step 4.

9. Use the inverted Laguerre Transform for m-pixel groups sequentially to get spatial domain representation.

Methodology for Extraction

A Stego-image was used as input.
Secret image as output.

1. Divide the stego-image into non-overlapping m-pixel stego-image blocks.

2. Apply Laguerre Transform to each m-pixel group sequentially

3. Extract the Least Significant Bits from the m-pixel group.

4. Repeat step 3 until the 1-D array's size equals the size extracted.

5. Decode the extracted data using the Huffman dictionary.

6. Reshape the 1D vector into a 2D Matrix of the appropriate size to retrieve the Secret Image.

Result

- Input Images

Fig. 12 Image to be hidden

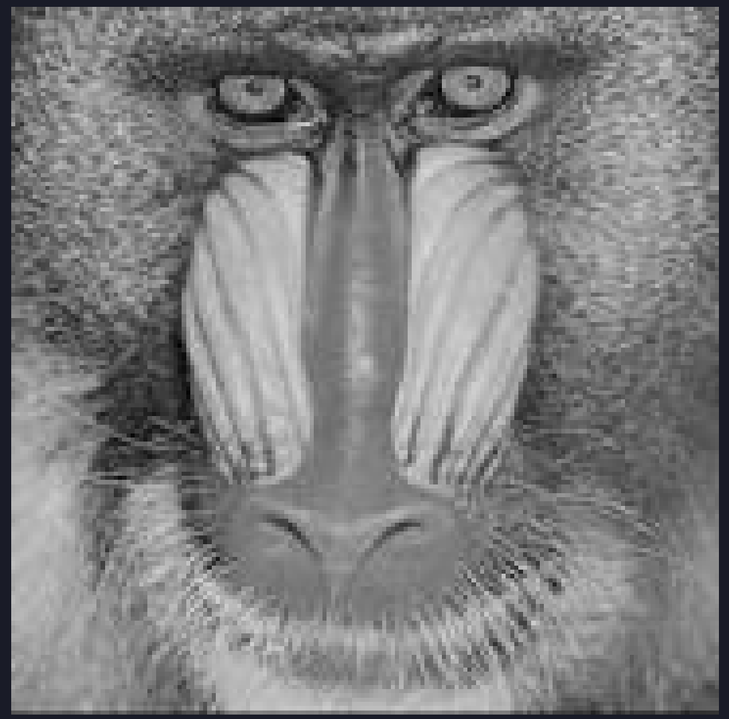


Fig. 13 Cover Image

Result

- Output Images

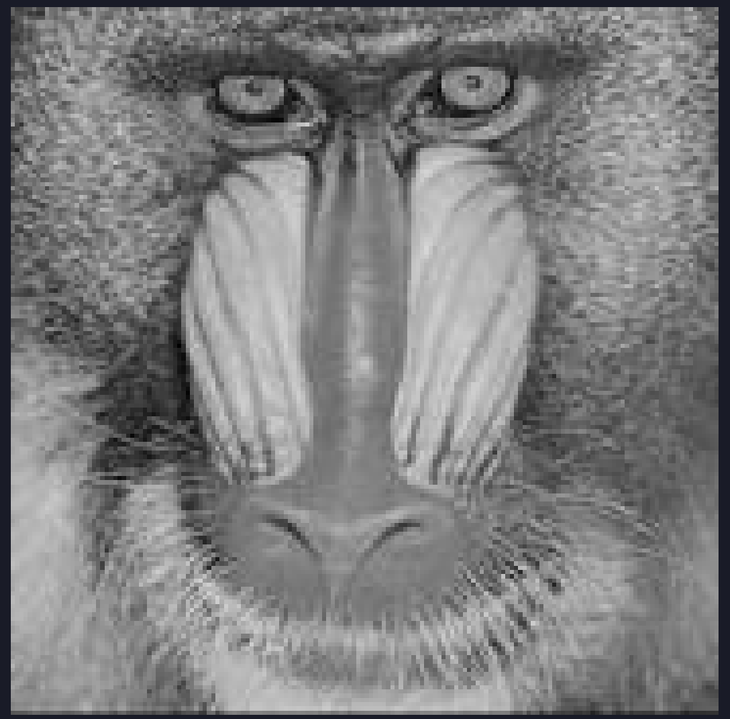


Fig. 14 Final Greyscale Stego Image

Fig. 15 Extracted Image

Result

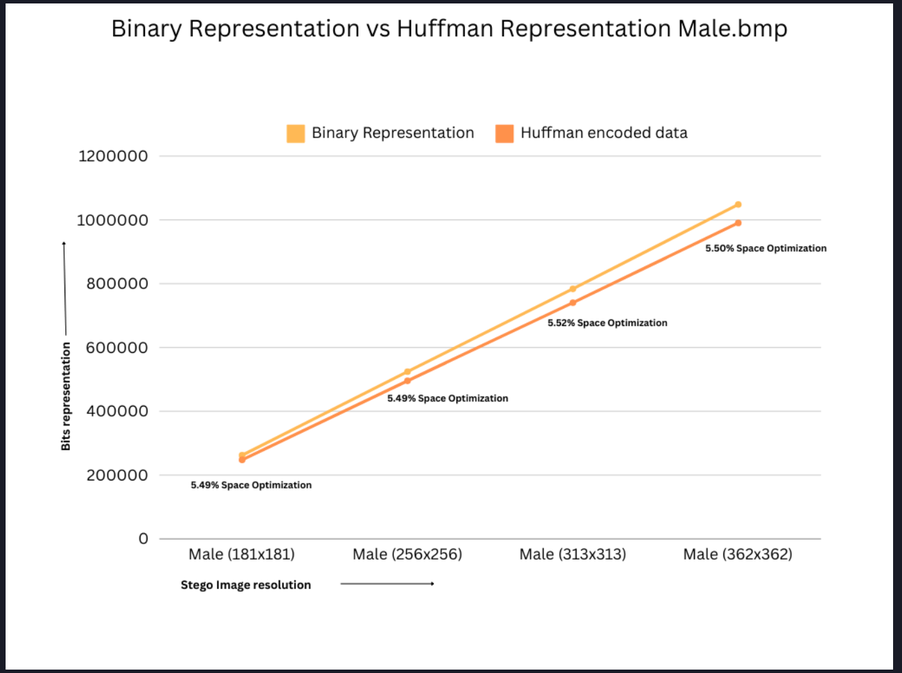
- By integrating LSB, Laguerre Transform, and Huffman coding, our implemented algorithm exemplifies a holistic approach to image steganography, highlighting a deliberate equilibrium among capacity, security, and imperceptibility factors.
- The Laguerre transform conducts calculations based on integers, resulting in faster operations.
- The algorithm under discussion exhibits robust security measures and boasts significant payload capacity and increased, attributed to using Huffman coding.
- The computational complexity of this transform is $O(n \times \log(n))$ where n is the number of pixels in the cover image, offering superior performance compared to existing image steganography algorithms.

Result

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)

Result

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



Result

Cover Image	Method	Payload(b) bpp	PSNR (dB)
 Lena	Atta's method [2]	1.7/2.5	44.91/38.77
	Kalita et al. [3]	1.14	43.9
	Nazari et al. [4]	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 [2]	1.80/ 2.5	44.44/38.02
	Kalita et al. [3]	1.14	43.9
	Nazari et al. [4]	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 [2]	1.7/2.5	1.7/2.5
	Kalita et al. [3]	1.14	1.14
	Nazari et al. [4]	0.24	0.24
	Ghosal et al. [1]	1/2	49.30/43.87
	Proposed Method	**1/2**	**49.73/43.77**

Conclusion

Study on Image Steganography Techniques

- Explored unique characteristics and applications of Image Steganography.
- Literature review highlighted the need for diverse approaches.
- Investigated the use of Image Steganography in covert operations, digital watermarking, and secure communication.
- Demonstrated trade-off between perceived invisibility and payload capacity.
- Identified inverse relationship: higher detectability often leads to increased payload capacity.