CONVEYANCE OF DATA USING IMAGE STEGANOGRAPHY

Mrs. S. Naga Sindhu[11]Assistant professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P, India.
AkunuriKeerthi Sri[2,]Student,[6]Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P, India.
Divvela Harshitha[3], ,[5]Student,[6]Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P, India.
Kakumani Akash[4], Student,[6]Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P, India.
Mettapalli Raghu Vamsi,[5]Student,[6]Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P, India.
Dr.T. Balamuralikrishna[6] Student,[6]Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering and Technology, A.P, India.

ABSTRACT :
The art of data hiding involves concealing information for a variety of reasons, including maintaining privacy, protecting secret information, and more. Data exchange via the internet network must be done securely. Thus, there are several methods, including steganography and cryptography, to safely convey data to the target. Image Data concealing within an image is referred to as steganography. The image chosen for data concealment is referred to as the cover image, while the image produced through steganography is referred to as the stego image. In this project, we provide a pixel-based method for hiding the data by employing the blind hide algorithm for embedding the data into the photos, together with a discrete wavelet transform steganographic method. The presented plan is an easy and effective technique to conceal sensitive information. It reduces image degradation and maintains the image's qualities. In comparison to Exploiting Modification Direction, it enhances payload capacity. It is extremely safe from attacks, at least in a substantial way. The restored image is of excellent quality. Key Words: Data Hiding, Image Steganography Methods, Data Embedding and Extracting, Image Steganography.

1. INTRODUCTION

Conveyance of data using image steganography are essential algorithm must be used in today's fast-paced world. Proper use of steganography algorithms can increase data security and confidentiality. In this project we will discuss about steganography techniques used for data hiding. By implementing a "steganography" approach to conceal data in a cover image, it has already been possible to find a solution to this issue. The quantity of data that can be concealed, the message's clarity, and robustness all affect how the cover image is composed. The proposed plan in this document makes use of the pixel matching method. This method is used to keep the image quality high while it is being transmitted through communication networks. Data concealment method and data recovery procedure are the two ways to obtain it.We will look at the best practices, tools, and methods that can be used to increase the data security by using steganography algorithms and workflow efficiently and effectively. Furthermore, we will discuss how to apply these strategies in different work environments and how to measure their effectiveness.

2. METHODOLOGY

The methodology utilized in this study's research has as its goal creating the best model's categorization rules.Spatial Domain Methods: spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of cover image in such a way that the effect of message is not visible on the cover imageSpatial Domain Methods: spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of cover mage in such a way that the effect of message is not visible on the cover imageSpatial Domain Methods: spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of coverimage in such a way that the effect of message is

 DOI10.36893.JK.2023.V13I04N16.00157-00162

notvisible on the cover domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of coverimage in such a way that the effect of message is notvisible on the cover mageSpatial Domain Methods: spatial domain Steganography technique refers to methods in which data hidinis performed directly on the pixel value of cover image in such a way that the effect of message is not visible on the cover image

1.SPATIAL DOMAIN METHODS:

The term "steganography technique" describes procedures where data concealing is carried out directly on the pixel value of the cover image in order to make the message invisible on the cover image. Least-significant bit, Pixel Value Differencing, and Binary Pattern Complexity are the spatial domain approaches.

TRANSFORM DOMAIN STEGANOGRAPHY:

Data is hidden inside the image using sophisticated techniques. Information is concealed in the photos using various algorithms and processing techniques. When a signal is embedded in frequency domain, it does so considerably more effectively than when it is embedded in time domain. Techniques in the transform domain conceal information in images that are less subject to compression, image processing, and cropping than are techniques in the spatial domain. Certain transform domain approaches do both lossless and lossy format conversions without regard to the image format. Transform domain techniques are classified into a number of groups, including Discrete Fourier transformation (DFT), discrete cosine transformation (DCT), Discrete Wavelet transformation (DWT).

Spread spectrum:

This method makes advantage of the spread spectrum. The secret data is dispersed over a large frequency spectrum in this manner. Every frequency band's signal-to-noise ratio must be so low that it is challenging to detect the presence of data. There would still be enough information available in other bands to recover the data, even if portions of the data were removed from a few bands. As a result, it is challenging to totally delete the data without also completely ruining the cover. It is a very effective strategy for military communication.

3. PROCEDURE

Process of implementation involves of roles:

1. **CO (Cover Object)**
2. **SD (Secret Data)**
3. **SO (Stego Object)**
4. **SK (Stego Key)**

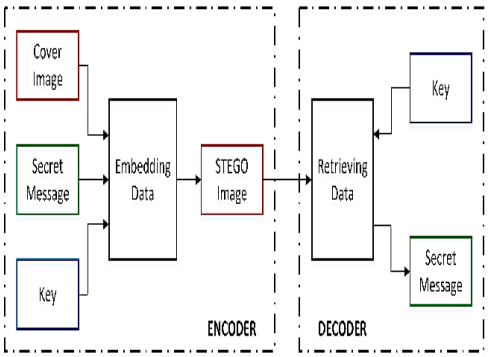

Fig 1. Fundamental steganography architecture

1.CO (Cover Object):

Data hiding is performed in this CO.In this process random image is selected form the internet which is called cover image. Cover image selection is the first step in image steganography where data is hiden into the cover image according to the sender choice. And sender sends the cover object from sender to receiver after all the encryption process by using pixel based methods and blind hide algorithms.

2.SD (Secret Data)

Secret data is hidden into the cover image. Embedding the data inside the cover image is done by user according to the sender choice where embedding data inside the cover object can be done in any format like picture form, number format, file format, video format or text format. Embedding data inside the cover image is done by using blind hide algorithm

2.1 Blind Hide Algorithm The best technique to conceal information in an image is in this way. Because it just begins at the top left corner of the image and moves across it pixel by pixel, it blindly hides the data. Moreover, it modifies the message's least important bits in the pixel colours. The least significant bits are read off to begin the decoding process, starting at the top left. Also, it isn't very clever because only the top portion of the image is altered while the bottom portion of the image remains the same, making it obvious what has been modified.

ALGORITHM FOR PIXEL SWAP:

- choose the cover image's two pixels x1 and x2 using a pseudo-random sequence.
- Create another group of pixels if the two pixels are not within a predetermined distance (often 2 or 3), in which case they can be used for encryption.
- Message bit should be selected. Check to see if x1 > x2 if the message bit is zero or one. If not, switch x1 and x2. Reverse the operation for message bit one (zero).
- Similarly, choose the pixels for decoding by employing the same pseudo-random sequence. Verify that the 2 pixels fall inside the pre-defined range. The message bit is zero (one) if x1>x2, else it is one (zero).

3.SO (Stego Object)

After the data is buried inside, the CO is in the Stego Object state. After the embedding procedure, the Stego image is obtained. The stego image is obtained after the secret data has been encrypted into the cover image using the least significant bit technique and pixel matching from left to right. Next, using the hide-and-seek process, the secret data is distributed at random once the image's data has been encrypted. The message is dispersed throughout the image by the hide-seek algorithm at random. It takes its name from the Windows 95 steganography utility "Hide and Seek," which employs a related method. It creates a random seed using a password and chooses the first position to hide in using this seed. It keeps generating positions at random until the message has been fully concealed.

3.1 **FILTER FIRST:**

The image is filtered using one of the built-in filters via the filter first algorithm. The highest filter values are then covered up first. Moreover, retrieving the message with filter first doesn't require a password. The most significant bits are filtered by the filter first method, followed by the least significant bits.

3.2. **BATTLE STEG:**

The best algorithm for doing battleship steganography is called the battle steg algorithm. The highest filter values are used as ships after the image has first undergone filtering. The algorithm then fires at the image at random, and when it spots a ship, it clusters its shots around it in an attempt to sink it, before moving on to look for more ships. Combat steg obscures the message at random. And since a password is required to access the communication, it is safe.

3.3 Transform domain techniques

- Discrete Fourier Transform (DFT): Using different Fourier coefficient values, this technique conceals secret data.
- Discrete Cosine Transform (DCT): With this technique, the secret message is concealed by changing the magnitude of the converted coefficients. The image's concealed information is evenly dispersed throughout. This results in a stronger technique.
- Discrete Wavelet Transform (DWT): It embeds data using the wavelets approach. It primarily serves to boost the image's capacity and robustness. Also, for data embedding, the wavelet coefficients are modified.

4.SK (Stego Key)

Stego keyHide function is used for the hidden data within the CO. Stego key generated both the sender and receiver side by using blind hide algorithm.In the above figure.1, the cover image, secret

ISSN: 2278-4632
Vol-13, Issue-04, No.06, April : 2023

message and key is used for embedding the data to attain the stego image. This is done is the encryption phase. In contrast, the secret message is retrieved by using the key in the decryption phase.

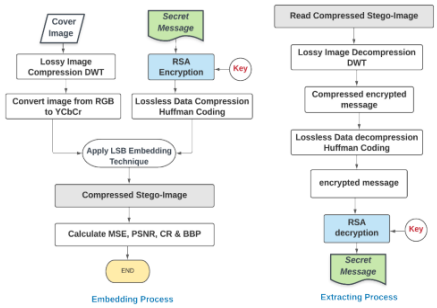

Fig 2. Process of embedding and extracting the secret message

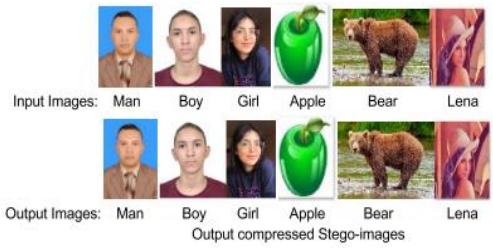

Fig 3. Input/output of images

4.RESULTS The parameters that were determined by comparing the stego image produced by our suggested method to the stego image produced by the blind hide steganography algorithm are listed below.

A. Accuracy:

By comparing the original image pixels to the stego image pixels produced by our proposed algorithm and the BLIND HIDE algorithm, accuracy is determined.

Images	Proposed Method	BLIND HIDE
Image1	0.99990563	0.99989138
Image2	0.99995917	0.99994583
Image3	0.99995917	0.99995417

Table 1. Comparison of stego image for Accuracy.

B. Precision:

By comparing the original image pixels with the stego image pixels produced by our suggested technique and the blind hide algorithm, precision is calculated.

Images	Proposed Method	BLIND HIDE
Image1	0.99990579	0.99989143
Image2	0.99995918	0.99994585
Image3	0.99995918	0.99995418

Table 2. Comparison of stego image for precision.

C. Recall: By comparing the original picture pixels with the stego image pixels produced by our suggested method and the blind hide algorithm, recall is computed.

 DOI10.36893.JK.2023.V13I04N16.00157-00162

ISSN: 2278-4632
Vol-13, Issue-04, No.06, April : 2023

Images	Proposed Method	BLIND HIDE
Image1	0.99990563	0.99989138
Image2	0.99995917	0.99994583
Image3	0.99995917	0.99995417

Table 3. Comparison of stego image for recall.

Features of image steganography:

- Secure data transfer
- Military communities.
- Digital watermarking.
- Networking sectors.
- It is also used for confidential communication and secret data
- storing.Protection from data alteration.
- Used for access control the system for digital content
- distribution.Used in media database systems
- Intelligence agencies use them for communication.
- Used inMedical sector.

5.CONCLUSION

The technique of conveying secret information by concealing it in plain sight under a cover image is known as image steganography. Deep learning techniques are employed often across many disciplines and have been used in the study of steganography. The suggested plan is an easy and effective technique to conceal sensitive information. It reduces image degradation and maintains the image's qualities. When compared to exploiting modification direction, it enhances payload capacity. Compared to least significant bit, it is far more secure against attackers. The recovered image is of excellent quality, and the edited image closely resembles the original. not vulnerable to rotational and translational attacks. We come at the following conclusions by comparing the outcomes of our suggested method to blind hide: It is obvious that our proposed method produces more accuracy, precision, recall, and f1-score. The output image produced by our suggested method is almost the same size as the original image. Because PNG (Portable Network Graphics) is compressed and lossless rather than BMP (Bitmap), which is uncompressed and lossy, our suggested method produces steganograted images in PNG, which is superior to BMP (Bitmap).

6. ACKNOWLEDGMENT

For allowing the authors to perform this project CONVEYANCE OF DATA USING IMAGE STEGANOGRAPHY by Dhanekula Institute of Engineering & Technology, Ganguru, Bachelor of Technology, Faculty of Computer Science and Engineering Technology Department, and our beloved guide Assistant Professor Mrs. S. NAGA SINDHUthrough the provision of computational resources and a conductive working environment.

7. REFERENCES

[1] R. Singh, G. Chawla, “A Review on Image Steganography,” Internationl Journal of Advanced Research inComputer Science and Software Engineering , vol. 4, pp. 686-689, May. 2014.
[2] Rakhi,S.Gawande, “A Review on Steganography Methods,”Internationl Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , vol. 2, no. 6,pp. 4635-4638, Oct. 2013.
[3] C. Gayathri, V. Kalpana, “A Study on Image Steganography Technical, Techniques,”Internationl Journal of Engineering and Technology(IJET) , vol. 5, no. 2, pp. 572-577, Apr-May.2013.
[4] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, “A new Steganography Method for Gray Level Images using Parity Checker,” International Journal of Computer Applications, vol. 11, no. 11, Dec. 2010.

 DOI10.36893.JK.2023.V13I04N16.00157-00162

[5] R. Patel, V. Kumar, V. Tyagi, and V. Asthana, ‘‘A fast and improved image compression technique using Huffman
coding,’’ in Proc. Int. Conf. Wireless Commun,Signal Process. Netw. (WiSPNET), Mar. 2016, pp. 2283–2286.
[6] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, ‘‘An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding,’’ Opt. Lasers Eng., vol. 124, Jan. 2020, Art. no. 105837
[7] EfeÇiftci; EmreSümer A Novel Steganography Method for Halftone Images DOI: 10.1109/SIU55565.2022.9864763
[8] ShivamIlasariya;ParthPatel;VatsalPatel;SwapnilGharat Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)
[9] A Novel Method of high-Capacity Steganography Technique in Double Precision Images -2021 International Conference on Computational Performance Evaluation (ComPE) .

