*Grenze International Journal of Engineering and Technology, June Issue*

# Silent Sentinels: Unveiling Hidden Messages in an Image using Steganography and Cryptography

M. Santoshi Kumari[1], Ch. BenerjeeBhuwaneswar Reddy[2], Eitiki Vishwas[3] and Goli Venkata Srihan[4]
[1-4]Gokaraju Rangaraju Institute of Engineering and Technology
Artificial Intelligence and Machine Learning Department, Hyderabad,India
Email: {santoshi1631,ch.benerjeereddy, etikivishwas47, venkatasrihangoli}@gmail.com

***Abstract*—Image Steganography is the process of hiding information in images, the information can be text, image or a video. The person cannot differentiate between a steganographic image and an original image Traditionally, the Least Significant Bit (LSB) method has been the most popular choice for steganography due to its simplicity and effective in hiding the text data in an image. This LSB is a beginner friendly technique and could be understood by a naive user even. Making changes to the least significant bit of every pixel doesn't change the content of an image. Making a strong steganographic image that maintains the data integrity and security and resilience to a cyber-attack is a concern these days. Here first the message that needs to be embedded in an image is first encrypted with a cryptographic algorithm with a secret key. This secret key is only shared between the sender and receiver.Later the message is embedded in the image using the Least Significant Bit (LSB). It is responsibility of the user to distinguish between the a bundle of steganographic image and the original image, further upon discovering the steganographic image he/she should detect the encrypted message from the steganographic image. Upon discovery of the encrypted message he/she should decrypt the secret message using the same encrypting algorithm and the secret key used for encrypting the message. This message, that is, the secret message is now made available to the user to see it.**

***Index Terms*—LSB(Least Significant Bit), ResNet(Residual Network), VGG(Visual Geometry Group), DCT(Discrete Cosine Transform), PR(Pixel Ratio), DES(Data Encryption Standards), ANN(Artificial Neural Network), CNN(Convolution Neural Network), ReLu(Rectified Linear Unit), PCA(Principal Component Analysis), SGD(Stochastic Gradient Descent), ROI(Region Of Interest).**

## I. INTRODUCTION

In this contemporary society that is embedded with technological advancement, the security of the users' communication proves to be paramount. Thus, image steganography, which is a procedure for concealing information within images, becomes an extremely effective means of safeguarding secrets. Interactions that occur in our everyday life are not immune to some threats like masquerading and man in middle attacks that present daunting risk of losing perpetuating information or even sharing sensitive information with third parties who would inappropriately use the same for their own benefits. In the contemporary world, it is very importantto safeguard sensitive data due to the technological developments. Steganography, an approach that encompasses hiding information, has been in existence for centuries since the ancient Greeks'. Methods of the past were steganography through invisible writing and embedding secret messages in the skin of a tattoo scalps in times of

*Grenze ID: 01.GIJET.11.2.565_23*

war. This domain has dramatically transformed in the era of modern computing with an enroll computer environment. Hiding techniques have changed since the end of the twentieth century and are closely related to cryptography, steganography, watermarking, and other forms of encryption.Among these techniques, steganography draws the attention of researchers and is widely used due to the vast presence of digital images, videos, and audio in modern people's lives. As a concept, steganography is different from cryptography where an input plain text is randomly arranged to an unreadable format normally referred as cipher and even if somebody intercepts the message, cannot read it without a decryption key, here the channel itself hides the existence of the message. Thus, steganographic techniques guarantee that sensitive or confidential messages or data are hidden in images, audio files, and video files in a way that will be unnoticed or even unknown to individuals who use those media files.Steganography is the manners in which a file that a person wants to hide is inserted into the carrier file without making any noticeable changes in the latter.

Some of the most realized methods include least significant bit (LSB) method in which the least significant bits of the pixel value are changed to hold the concealed message. This information can only be read by intended recipient by applying certain algorithms and by knowing the keys of the sender. This means it is not easily possible for any other user who is not authorized to either find out the data that is hidden or to gain access to that data.Thus, the image steganography is utilized in multiple scenarios such as secure communication, watermarking, digital rights management, and protection of intellectual property. It is also used in espionage and spying to convey messages which are coded so as not to draw undue attention. Even if steganography is concealing messages effectively, man and technology do not leave it out of control. The challenge emerges when it comes to Steganalysis – a process of identifying the hidden data in the media. Methods including but not limited to statistical analysis, pattern analysis, and artificial neural network are applied to look for steganographic signal. In order to overcome these threats, modern steganographic techniques are actively updated with the aim to increase their security and invulnerability.

All in all, the proposed method of image steganography is indispensable when it comes to safe communication in the modern world. Through concealing data in digital image, it offers an efficient way of promoting the security of information by shielding it from unauthorized and rigorous identification. It is consequently expected that with the advancement of technology and with added development in Eric Jeffries' steganography that it is inevitable that steganography is also bound to take up even a more critical role in ensuring privacy and security in today's complex world.

## II. LITERATURE SURVEY

Harpreet Kaur and Jyoti Rani, with others[1] proposed a paper called "A Survey on different techniques of steganography". This survey paper examines various techniques in LSB (Least Significant Bit) steganography, a method where data is hidden in the least significant bit of every image pixels. It categorizes different LSB embedding strategies and discusses their applications, strengths, and vulnerabilities to attacks. The survey also explores advancements in LSB steganalysis techniques aimed at detecting hidden data, providing a new view of the current state of LSB-based steganography in digital image security analysis.

Hamidreza Rashidykanan and Bahram Nazeri [2] has proposed a paper called "A Novel Image Steganography Scheme Based on LSB Substitution and Genetic Algorithm". This paper presents a new method for image steganography using LSB modification with a new genetic algorithm. It provides an effective way to recognize the embed information into digital images or carrier images while increasing protection against detection. By using genetic algorithms, the concept of dynamically adjusting the (LSB) Least Significant Bits embedding process to improve the security, reliability and ensure robustness against any of the steganalysis techniques, providing a promising first step in covert communication into secured ones.

Kousik Dasgupta, Jyotsna Kumar Mandal with others [3] has proposed a paper called "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain". This work presents a new LSB steganography method combining the old chaos theory and the deep neural networks. Using chaotic maps to generate embedding sites in the carrier image and optimize neural network parameters, this method increases data hiding ability and security. It aims to reduce the error in the traditional LSB method by introducing the distortion layer and change of the neural network model parameters being used, thus improving protection against data loss and advances in secret communication.

Tanmoy Sarkar, Sugata Sanyal [4] has proposed a paper called " Steganalysis: Detecting LSB Steganographic Techniques ". This survey examines and evaluates several unique integration methods designed to verify LSB Least Significant Bit steganography. It works on the theory of statistics, machine learning and deep learning models for hidden data discovery using the LSB techniques. This research paper would discuss the advances in

media technologies like images, audio files, video files, pdf files i. e any of the carrier objects facing challenges in detecting LSB insertions, and future research directions for improving digital image forensics in the context of LSB-based steganography.

Z. Ni, Y. Q. Shi [5] has proposed a paper called "Image Steganalysis of LSB Matching Using Differences Between Nonadjacent Pixels ". This paper discusses the steganalysis method that aims to detect LSB matching steganography by calculating the differences between the non-adjacent pixels in an image. It explores the statistical features and relationships in images to identify the subtle or small changes caused by LSB embedding. By using different pixel values in non-adjacent areas, the proposed method improves the detection accuracy and robustness of LSB matching steganography technology to a great extent, contributing to the advancement of digital image forensics and in the field cyber security.

Shahidrahman, Jamaliuddin Habib, Ullah Khan with others [6] has proposed. This paper introduces a steganalysis method that uses the same traditional level and optimization to find LSB matching steganography. It uses phase matching to identify phase between the edges to find the useful information in images and to improve the detection ability using the pre-processing and the elimination techniques. The proposed method is mainly for improving the accuracy of determining LSB matching patterns and to provide information on effective techniques for identifying confidential information, and increase the security of digital images.

Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul and others [7] have proposed a paper called " A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key". This paper presents a new method to detect (least significant bit) LSB steganography by identifying unique pixel that change during the data embedding process. This method aims to study the changes in image texture, color distribution, and consistency caused by the LSB process. Using statistical methods and machine learning to extract and analyze these features, the method improves the detection accuracy and robustness over LSB steganography methods. Results demonstrate the effectiveness of the detection method in reliably identifying hidden data while minimizing the false positives that have occurred. This research uses image analysis to detect LSB-based hidden information in digital images, which helps to improve steganalysis capabilities.

Zhihong Chen and Wenyao Liu, [8] have proposed a paper called " Improved LSB matching steganography with histogram characters reserved ". This paper presents an improved steganalysis method that focus on detecting the LSB (least significant bit) related steganography, which contains information by comparing LSB values on adjacent pixel sides. This method studies the differences between the histogram peaks to identify subtle/small differences that reveal hidden information. This method improves sensitivity and accuracy over LSB matching techniques by analyzing changes in pixel distribution in an image. Experimental results have shown the effectiveness of the steganalysis method used in detecting confidential data with high confidence and efficiency. This method helps in improving the steganalysis capabilities by introducing histogram peak analysis to secure LSB-based information hidden in digital images.

Wa'el Ibrahim, A. Almazaydeh with others [9] and other have proposed a paper called "A novel approach of image steganography for secret communication using spacing method". This paper presents a new method for testing LSB (least bit) image steganography based on the initial identified features that change during data embedding process. This method aims to analyze the changes in the pixel values using the classification and spatial correlation that results from the LSB process. Using machine learning algorithms to extract and evaluate these changes, the system increases the detection accuracy and reliability of complex LSB steganography techniques. The results tries to depicts the effectiveness of the detection method in correctly identifying the secret information while minimizing the false detections.

U A Md Ehsan Ali with his team [10] have proposed a paper called "A Robust Approach for LSB Image Steganography Detection Using First Bit Plane Analysis". The goal is to identify the specific changes in the binary representation of pixel intensity values that occur during the LSB process. By analyzing and comparing original flight patterns using statistical analysis and machine learning techniques, this method increases the detection accuracy and precision of the LSB steganography method.

M. Harith Noor Azam, Farida Ridzuan with others [11] have proposed a paper called “A new method to Estimate Peak Signal to Noise Ratio for Least Significant Bit Modification Audio Steganography”. This method aims to increase the depth of the embedding level from fourth to sixth and eighth LSB level to improve its robustness feature. A method to estimate PSNR, known as PSNR estimator (PE), is introduced to enable early evaluation of imperceptibility feature for each stego-file produced by the audio steganography. The proposed PE can be used as a reference for embedding and further reducing the calculation complexity in finding the feasible value to minimize the trade-off between robustness and imperceptibility.

M. Tariq Barakat, Ziad A. A AI Qadi [12] have proposed a paper called “Highly Secure Method for Secret Data Transmission”. A method for protecting confidential and private data, which combines the two processes of data

cryptography and data steganography. In this methodology a colored digital image is used to generate the private key and this method carries the encryption and decryption process. This will increase the efficiency of the method compared to LSB method and it improves the value of the quality parameters MSE and PSNR.

## III. PROBLEM STATEMENT AND OBJECTIVES

- Propose steganalysis techniques based on deep learning algorithms to extract concealed messages from steganographic covers. Create an easy to navigate front-end for the encryption and decryption process of the messages. Develop a secure method of storing the keys that are used by the encryption and steganographic embedding algorithms. And also ensure the keys are stored and transmitted in a safe manner. Fine tune deep learning models that are capable of identifying concealed information hidden in the images within the dataset. To protect the private data it is necessary to use the abilities of user authentication, access control and data encryption for its transmission and storage. Carry out extensive testing to ascertain the stability and correctness of the application.
- To enhance the encryption of user message using a Hybrid Substitution Cipher
- To embed the Encrypted message in Random Pixels of an Image using LSB Steganography
- Enabling the integrity and security of the system by monitoring the users behaviour

### *A.Proposed Method*

This proposed work on image steganography is to improve the security communication by using the cryptographic algorithm along with proper steganography methods. When it comes to the process of encrypting the messages posted by the users, the Hybrid Substitution Cipher is employed, whereas the messages are hidden in the least significant bits of the digital images. To enhance the recovery of concealed messages, new steganalysis approaches will be built based on deep learning that refines the models for the discovery of hidden data. The processes of encryption and decryption will also be presented on the site's front-end, and a secure way to store and transfer the key will be developed. Moreover, user identification and its enforcement, as well as data encryption, will impact the protection of the private data before and after the transmission process is launched. Integration testing will be done to prove that the application is right and that there are no major organizational issues, thus securing the channel of communication.

### *B.Architecture diagram*

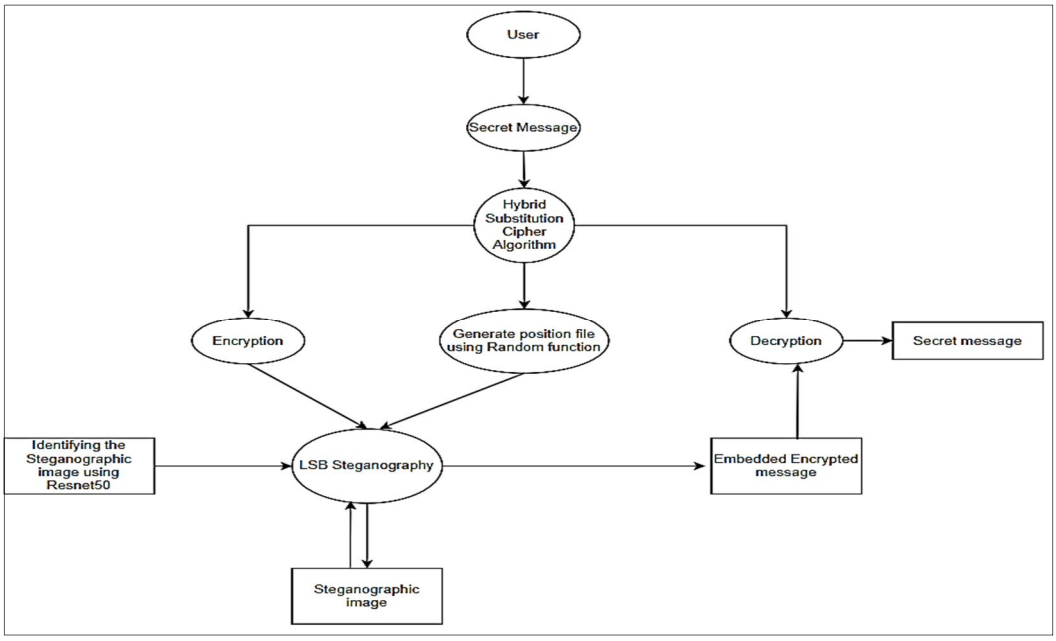


Figure 1 Architecture diagram

Figure 1 explains to take the input from the user using a Graphical user interface (GUI) then use an encryption algorithm like caesar's cipher, substitution cipher or a hybrid encryption algorithm to encrypt the message provide by the user. Here use a symmetric key to encrypt the data which can be used to decrypt the cipher using

the same key. It is done using Least Significant Bit(LSB) steganography. Every pixel in a image is represented in the form of RGB format which is defined as red, green, blue. The values of these RGB varies from 0 to 255 i. e (0, 0, 0) to (255, 255, 255) which represent the intensity of the colour in that pixel. Now imagine an image having a shape of length 128 and breadth 128. It would have 128*128*3 number of values that can be modified. LSB changes the least significant bit of each pixel. By changing the least significant bit of each pixel the information doesn't vary much. For example the number 5 is expressed as 00000101.
It is the binary representation of the digit 5, now by changing the least significant bit of number 5 turns 00000101 into the binary format 00000100 which doesn't change much information. For example the word 'hello' cannot be directly embedded into the image, rather it is first converted into the binary i. e 01101000 01100101 01101100 01101100 01101111. These individual bits are then placed in the image at random positions. To recognize where we have embedded these pixels, we maintain a pixel position file which has entries of the pixels that being altered. The pixels that are selected to alter in the image are generated completely in a random manner. Should make a note that the no of pixels that are going to be altered should be less than the total pixel capacity of an image being used.
So sending 100's of original image with 1 original image will surely confuse the user even though he/she knows the presence of the secret information in 1 of the images. This is done by duplicating the original image 100 of times and sending 100 original images and 1 steganographic image to the receiver. To overcome this situation we have to perform clustering on the images. Normal cluster will unable to segregate the images into different classes. To handle this situation, we use Resnet50 a deep learning algorithm which is available in tensor flow module used to extract the features of the images. First take the image and then normalize it i. e convert the pixel values from (0-255, 0-255, 0-255) to (0-1, 0-1, 0-1) after normalizing the image convert the image into a numpy array, there exist a built-in method called feature extraction which extracts the features of the images like, edges, textures, patterns, shapes, parts of objects, object compositions, contextual relationships, abstract representations. These features will slightly differ from the steganographic image and the original image.
These features are then classified using the clustering method as there are no labels to classify them we use the array of features extracted to cluster them into 2 classes. cluster 1 for the group of original image and cluster 2 for the steganographic image. After identifying the steganographic image he/she has to retrieve the information from the image, as the pixel that we embedded are generated in a random manner, the traditional LSB technique fails to decode the message. To properly decode the message we need the pixel position file from the sender. we have to use the only the pixels that are specified in the pixel position files. Use this file and decode the encrypted message.
i. Modules Description: First comes the encryption module in which the user input is encrypted using an encrypting algorithm i. e a substitution cipher with a symmetric key then the generated text is now sent to pixel position function which generate random pixels based in the length of the input provided. This encrypted message and the pixel position file is now given as input to the LSB steganography function which embeds the input in the image provided. The steganographic image is then identified using a deep-learning algorithm called 'Resnet50', later this is image is given as input to the LSB steganographic algorithm along with the positon file for decoding the message. The message decoded from the image is in the encrypted format, later this message is passed through the decrypting algorithm which uses the same symmetric key used while encryption to generate the original secret image

## IV. RESULTS AND DISCUSSIONS

### *A. Description about Dataset*

There is no need for an image dataset for data entry in this work. Instead of that images are taken from chrome or any other website based on user input or selected from the user's computer. This approach eliminates the need for prerecorded data and provides flexibility in the images used for steganography as you can provide arbitrary images as input. Using random web images ensures that every steganographic operation we perform is unique, which increases the security of the text during the process. The address where the text is stored, used in the decoding process.

### *B. Significance of the Proposed Method with its Advantages*

The method proposed is a unique attempt to hide the message of the user in an image which cannot be seen by the human eye unless he/she is looking for it. Traditional LSB steganography modifies the LSB of every pixel in a sequential ways sometimes a computer experts or a cyber attacker may get to know that there is a confidential

Detailed Explanation about the Experimental Results

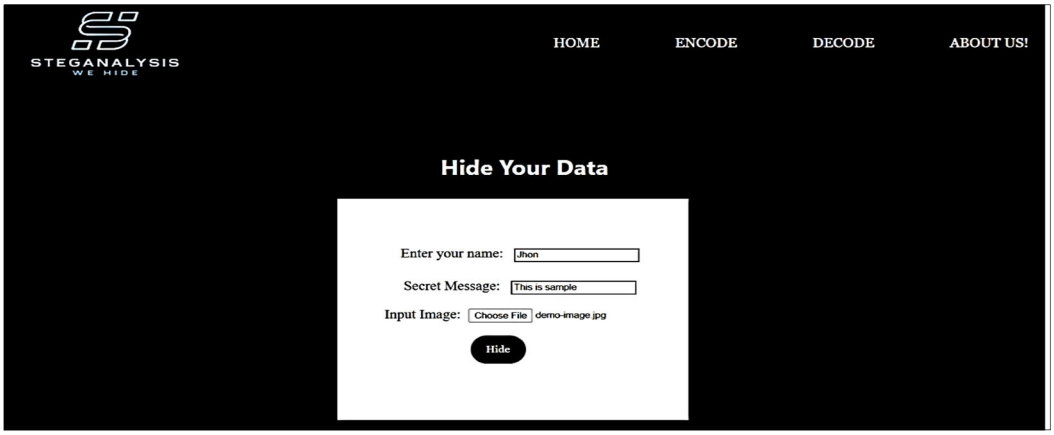


Figure 2a. Encode page

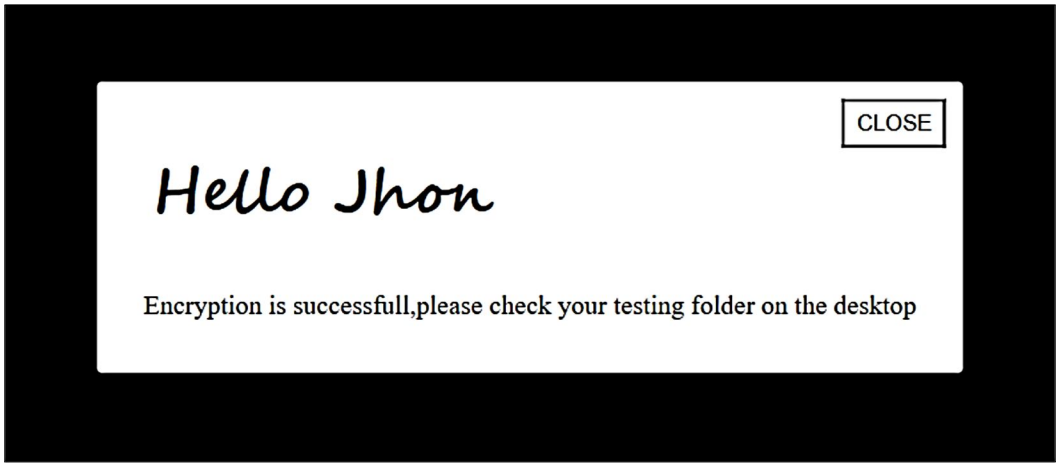


Figure 2b. Output in encode page

RESULTS SUMMARY

| Test Image | Message Size | PSNR (dB) | MSE | Encryption Time (ms) | Embedding Time (ms) | Extraction Accuracy (%) | BER (%) |
|---|---|---|---|---|---|---|---|
| airplane | 168 | 81.03 | 0 | 0.03 | 3891 | 100 | 0.0 |
| dinosaur | 13376 | 66.07 | 0.02 | 0.59 | 8712.43 | 100 | 0.01 |
| tree | 1640 | 75.22 | 0 | 0.09 | 9535.10 | 100 | 0.0 |
| mountains | 2848 | 71.85 | 0 | 0.12 | 7871.59 | 100 | 0.0 |
| books | 3400 | 71.55 | 0 | 0.12 | 5132.08 | 100 | 0.0 |
| streets | 5432 | 74.15 | 0 | 0.21 | 5181.93 | 99.98 | 0.02 |
| lion | 1280 | 79.63 | 0 | 0.06 | 8698.18 | 100 | 0.0 |
| table | 4000 | 69.59 | 0.01 | 0.12 | 7855.70 | 99.97 | 0.02 |

data in the image he or she is viewing then he uses the traditional LSB steganography and finds your secret message. This becomes a threat to the confidentiality to the data being sent. To avoid this attack we try to change the LSB of random pixels in the image which changes every time the operation being performed. This position are generated in a random way based on the length of the input provided by the user, to keep track of the pixels being altered we maintain a pixel-position file which is generally a text file in which the data i. e positions/coordinates of the pixels altered are stored.

During the decrypting process the traditional LSB steganography technique fails a the pixels altered during the encoding process is not in a sequential manner so the pixel position file is necessary to identify the pixels altered. Now using this pixel position we try to decode the message which was previously been encoded, although we get the message it will be in an encrypted format. To decrypt this we have to again pass this encrypted text into the

decryption function with the secret key which was used during the encryption process. Now the decryption process will be successful and we get the actual message. Any file either it is position file or the steganographic image or the secret key goes wrong the entire process collapse and the user will unable to read the secret message. By sending only a single image there is always a risk of grabbing the attention of the cyber attackers, so instead of sending a single image send a bundle of 100 original images and 1 steganographic image. Now even though someone know there is a steganographic image in it but fails to detect which image it was. He/she tries the brute-force attack method where he checks for every image whether it is stenographic or not, but what if we send 1000 original images and 1 steganographic images even though he tries brute-force attack the system cpu resources will be in a tremendous manner.

Even though he/she was able to detect the steganographic images the text decoded will be in the encrypted manner so he/she have to know the encrypting algorithm used and the secret key used which was only shared between the end-users. This does not prevent from the attack but doesn't harm your file during the attack. The technique used to detect the steganographic image out of 100's of original images is not brute-force method rather it is done using the deep neural network method called 'Resnet'. Residual Networks (Resnet) is a deep neural network which was a built-in method that can classify the images. It was already trained of a huge dataset and performs well on new training samples. First all the images I. e 100 original images and 1 steganographic image is sent to the Resnet50 model which has 50 hidden layers to process the input.

The images are flattened and normalized to a particular range now the features are extracted from the images provided and saved for the upcoming process. We use clustering algorithm which is a unsupervised machine learning algorithm which handle non labelled data based on finding the Euclidean distance between the inputs. Specify the number of clusters as 2 and pass the features started to the clustering algorithm, we generally know that all the original images will have one feature vector whereas the steganographic image in which the pixels are altered will have another feature vector. Based on these differences the images are classified into 2 categories.

## V. Conclusion and Future Enhancements

This steganography method offers a safe and secured way for hiding the customers information with the usage of encryption after which embedding the generated text in the pictures the use of Least substantial Bit (LSB) steganography technique. With a hybrid substitution cipher, the gadget makes positive that the text is securely and error-free encryption earlier than embedding it into a provider photograph, boosting the general safety of the hidden/personal message. The random insertion of the encrypted textual content in an photo's pixels and the recording of pixel positions will further contribute to the system's reliability and safety. The objective of image steganography is to enhance the secret and secured communication between the end-users. By embedding secret messages or sensitive information within digital images, audio files, video files, steganography allows individual users or organizations to communicate in a peer-to-peer manner without drawing the attention that there exists hidden information in that media.

This hiding nature plays a crucial role in the scenarios where confidentiality and integrity is given the prior importance. This position are generated in a random way based on the length of the input provided by the user, to keep track of the pixels being altered we maintain a pixel-position file which is generally a text file in which the data i. e positions/coordinates of the pixels altered are stored. During the decrypting process the traditional LSB steganography technique fails a the pixels altered during the encoding process is not in a sequential manner so the pixel position file is necessary to identify the pixels altered. Now using this pixel position we try to decode the message which was previously been encoded, although we get the message it will be in an encrypted format. To decrypt this we have to again pass this encrypted text into the decryption function with the secret key which was used during the encryption process. Now the decryption process will be successful and we get the actual message. Implementing adaptive embedding techniques that dynamically select the most suitable pixels for embedding based on the content of the cover image, further minimizing the visual impact and enhancing security.

Random generation of secret key which has a tenure of 5 minutes.

Develop real-time steganalysis detection systems using advanced machine learning and deep learning models to identify steganographic images more efficiently and accurately. Reporting them to the cyber security organizations.

Improve the user interface by building a mobile app which provide better visualization tools and more intuitive controls, making the system even more accessible to users with varying levels of technical expertise.

REFERENCES


[1] Harpreet Kaur and Jyoti Rani, “A Survey on different techniques of steganography”, In Proceedings of the 4th International Conference on Advancements in Engineering & Technology (ICAET-2016), vol. 57, pp. 1-6, 11 May 2016, DOI:10. 1051/matecconf/20165702003

[2] Hamidreza Rashidy Kanan and Bahram Nazeri, ”A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm”, In proceeding of ScienceDirect, vol. 41, no. 14, pp. 6123-6130, DOI: https://doi.org/10.1016/j.eswa.2014.04.022

[3] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, “A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain”, In proceedings of International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 3, pp. 11-21, February 2014, DOI:10.5121/ijsptm.2014.3102

[4] Tanmoy Sarkar and Sugata Sanyal, “Steganalysis: Detecting LSB Steganographic

[5] Techniques”, In proceedings of arXiv, 20 May 2014, DOI: arXiv:1405.5119

[6] Zhihua Xia, Xinhui Wang, “Steganalysis of LSB matching using differences between nonadjacent pixels”, In proceedings to Multimedia Tools and Applications, vol. 75, no. 4, pp. 1947-1962, 21 November 2014, DOI:10. 1007/s11042-014-2381-8

[7] Shahidrahman, Jamaliuddin Habib, “A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method”, In proceedings of IEEE Confrence, pp. 124053-124075, 2022, DOI:10.1109/ACCESS.2022.3224745

[8] Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul Islam, “A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key”, In proceedings of American Journal of Engineering Research (AJER), vol. 02, no. 9, pp. 118-126, 2022.

[9] Zhihong Chen and Wenyao Liu, “Improved LSB matching steganography with histogram characters reserved”, In Proceedings of SPIE - The International Society for Optica, vol. 6837, pp. 224-231, 4 January 2008, DOI:10.1117/12.755324

[10] Wa’el Ibrahim, A. Almazaydeh, H. S. Sheshadri and S. K. Padma, “A Novel Approach of Image Steganography for Secret Communication Using Spacing Method”, International Journal of Network Security & Its Applications (IJNSA), vol. 10, 2018, DOI: 10. 5121/ijnsa.2018.10304

[11] U A Md Ehsan Ali, Md Sohrawordi and others , “A Robust and Secured Image Steganography using LSB and Random Bit Substitution“, In proceeding to American Journal of Engineering Research (AJER), volume: 8, Page no: 39-44,Available: https://www.researchgate.net/publication/331544868_A_Robust_and_Secured_Image_Steganography_using_LSB_and_Random_Bit_Substitution

[12] Muhammad Harith Noor Azam, Farida Ridzuan and others “A New Method to Estimate Peak Signal to Noise Ratio for Least Significant Bit Modification Audio Steganography”, In proceedings to Pertanika Journal of Science and Technology 30(1):497-511, Volume: 30,2022, DOI: 10. 47836/pjst. 30. 1. 27

[13] Mohamad Tariq Barakat, A Ziad and Ziad A. A Al Qadi, ”Highly Secure Method for Secret Data Transmission”, In proceedings to International Journal of Scientific Engineering and Science, Volume 6, Issue 1, Page no: 49-55, 2022