

46th Series SPP: Synopsis Submission

| | |
|---|--|
| Project Reference Number | 46S_BE_1651 |
| Title of the Project | Enhanced LSB algorithm in a spatial domain of steganography |
| Name of the College & Department | Rajarajeswari College of Engineering Computer Science & Engineering |
| Name of the students & Guide(s) | Guide:-Dr. Kamal Raj T Students:- Ms. Arshiya Nazneen Mr Avinaasi L J Mr. Chaitanya Mahaprabhu S M Ms. Farheen Taj |
| Keywords | Steganography, LSB, Spatial domain, Block-selection, embedding, detection |
| Introduction/background (with specific reference to the project, work done earlier, etc) - about 20 lines | <p>Most common methods used in steganography to camouflage information in digital photos is the least significant bit algorithm. Poor ability to encrypt sensitive data, lack of robustness against attacks, and obvious deformation of stegoimages are some of its drawbacks. In the spatial domain of steganography, an extended LSB replacement innovation was developed to circumvent these limitations. The proposed algorithm adopts a hybrid strategy that combines the advantages of the algorithm with some additional techniques to increase the embedding capacity, improve flexibility, and reduce visual distortion. The suggested method is to first divide the cover image into non-overlapping blocks and then use the private key to generate a random sequence of pixels in each block. The hidden data is then embedded in the tiny selected pixels, making it difficult for an attacker to detect the embedded data. In addition, the algorithm uses a dynamic threshold to determine the number of bits that need to be replaced. This reduces visual distortion and increases attack strength.</p> |

| | |
|------------------------------|--|
| Objectives(about10lines) | Improved embedding capacity, Increased security, Reduced distortion, Error correction, Flexibility |
| Innovation about the project | Explore the application of steganography within machine learning models. This concept involves embedding secret information directly into the parameters or weights of a neural network without compromising its performance. By leveraging the high-dimensional nature of machine learning models, this technique could offer a novel way to securely transmit sensitive information while avoiding traditional channels of communication that may be monitored or compromised. |

| | |
|--------------------------------|--|
| <p>Methodology</p> | <p>The section outlines a method for concealing information by splitting an image into 8 distinct bit-planes. The approach involves converting pixel values into their corresponding 8-bit binary forms and then taking each <i>i</i>th bit from every pixel byte to produce the corresponding <i>i</i>th bit-plane image. This approach is a popular technique employed in steganography, which involves embedding confidential information within other types of data, such as images or audio files.</p> <p>A 20–25 frame conversion of the video is done first, each having a video-related characteristic. To create 24-bit bitmaps, the frames are transformed. These bitmaps are then divided into 8 bit RGB segments. Considering all of the RGB units in the movie, the Red, Green, Blue units can hold a lot of data. To avoid significant changes to the video, only one bit of the RGB bytes is altered. The 8 bit RGB units are where the adjustments, as already explained, are made. Additionally, the LSB, not the MSB, is the target of the changes. The reason for this is that the MSB adjustments typically result in a significant shift from the prior state. The intended message's confidentiality could be impacted by this. In order to be undetectable to the human sight, steganography's goal is to be. The LSB adjustments assist in achieving the same result. Human perception is unable to perceive the alteration since the effect is so slight, hence the hidden message's secrecy is kept safe and secure. We were able to hide three bits of information in each pixel's colour utilising a 24-bit picture. The 21-bit and 24-bit colours are difficult for people's eyes to separate from one another. Each component consists of one byte, or eight bits, with the first bit typically the most crucial. The last bit of each byte in each component is altered when secret information is kept hidden using the LSB technique.</p> |
| <p>Results and Conclusions</p> | <p>A steganography project for image, audio, or video files, these are the buttons or options to select the type of file the user wants to upload and hide a secret message in. Image: File type: Specify the types of image files that the system can accept, such as JPEG, PNG, or GIF. Audio: File type: Specify the types of audio files that the system can accept, such as MP3, WAV, or AAC. Video: File type: Specify the types of video files that the system can accept, such as MP4, AVI, or MOV.</p> |

| | |
|------------------------------|--|
| | <p>Choose a steganography algorithm: There are different steganography algorithms that can be used to hide a message in an audio file. Some of the most common methods include modifying the LSBs of the audio samples or changing the phase of the audio signal. 2. Determine the maximum message size: Before embedding the message, you need to determine the topmost size of the memorandum that can be concealed in the audio file without causing visible changes. This depends on the steganography algorithm you are using and the size of the audio file. 3. Convert the message: Convert the message you want to hide into binary format</p> |
| <p>Scope for future work</p> | <p>Increased Capacity: Researchers may strive to develop more efficient and effective ways to incorporate data into files, increasing the likelihood of data being hidden within a single file. Better Security: Researchers can work to develop more secure steganography techniques, including new methods of data integration that are more resilient to detection and attack. Applications in blockchain and cryptocurrency: Steganography can be used in blockchain technology to hide confidential information such as private keys. Mobile and cloud-based steganography: With the growth of mobile and cloud computing, steganography can be used to protect sensitive information on mobile devices or in cloud storage.</p> <p>In this study, a revolutionary image steganography technology is offered as a method. The programme creates a stego image that hides private data inside the cover file image. The Several of the most common photographic steganography techniques are covered in this article, highlighting the various ways to hide information within photographs. Every project makes use of the smallest possible bit algorithm to create a quicker and more reliable implementation, and its compression efficiency is reasonable when compared to other techniques.</p> |