|  |
| --- |
| MINI PROJECT  ON  “LSB BASED IMAGE STEGANOGRAPHY”    **NAME : MANAV BAKSH**  **CFID : 104609** |
| **CONTENT**  **S.NO TOPICS : PAGE**  **1. TITLE OF THE PROJECT 3**  **2. PROJECT DESCRIPTION 4-5**  **3. PROJECT REQUIREMENTS**  **3.1. FUNCTIONAL REQUIREMENTS 6**  **3.2 NON-FUNCTIONAL REQUIREMENTS 6-7**  **3.3 SOFTWARE REQUIREMENTS 7**  **3.4 HARDWARE REQUIREMENTS 7**  **4. PROJECT RESEARCH**  **4.1 HISTORY 8**  **4.2 IMAGE STEGANOGRAPHY:OVERVIEW 9-10**  **4.3 WORKING 11**  **4.4 USE CASE DIAGRAM 12**  **4.5 ADVANTAGES 13**  **4.6 DISADVANTAGES 13**  **4.7 APPLICATION 14**  **4.8 FUTURE SCOPE 14-15**  **5. TESTING**  **5.1 TEST PLAN 16**  **5.2 TEST CASES 17-18**  **6. RESULT 19**  **7. CONCLUSION 20** |
| **TITLE OF THE PROJECT:**    **PROBLEM STATEMENT:**  The aim of the project is to hide the data or information over an image using the least significant bit steganographic algorithm at receiver side and to send the stego or encrypted file to the destination where the retrieval or decryption of the secret data is done. |
| **PROJECT DESCRIPTION:**  Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and literally means covered writing. A Steganography system consists of three elements: cover image (which hides the secret message),the secret message and the stegano-image(which is the cover object with a message embedded inside it). A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as the RGB model. The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.  The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore,an altered |
| image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique. |
| **PROJECT REQUIREMENTS:**   1. **FUNCTIONAL REQUIREMENTS:**  * Secret Text Message File: In this file you will have to write a secret message to hide or you can select any text file of secret message. * Cover Image: Cover Image is the image to be selected in which a secret text message can be hidden. * Stego Encryption LSB implementation is performed on cover image to hide secret text messages by replacing bits of cover image by the bits of message. * Sender: In this Sender sends this stego image to the intended recipient to which he does want to communicate. * Receiver : In this receiver receives the stego image and opens the decryption option for getting hidden text messages inside that image.   **2. NON-FUNCTIONAL REQUIREMENTS:**   * Safety Requirements:Sender and Receiver should make sure that only they are having the same software to encrypt and decrypt data inside the image. Both should take care of eavesdropping. * Security Requirements:Develop a software in which embedding secret text data in image.Only sender and receiver should be aware of encrypted le. Users should not |
| unfold the message regarding sent images receiver info.   * Software Quality Attributes: The Quality of the software is maintained in such a way that only sender and receiver   can communicate through image.There is no probability of knowing a secret image.  **3. SOFTWARE REQUIREMENTS:**   * Operating System : Windows 10, Windows Subsystem for Linux * Front End : C * Tool : CodeBlocks, Ubuntu Terminal * Windows Image Viewer   **4. HARDWARE REQUIREMENTS:**   * Intel i3 * Processor: 2.48 GHz, 4 GB RAM * Minimum Hardware Requirement:   Pentium 3 166 MHZ Or Higher 128 mb RAM |
| **PROJECT RESEARCH**  **HISTORY:**  The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples in his Histories.Histiaeus sent a message to his vassal, Aristagoras,by shaving the head of his most trusted servant, "marking" the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Additionally, Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand. Steganography has been widely used for centuries. Here are some examples Hidden messages within a wax tablet: in ancient Greece, people wrote messages on wood and covered it with wax that bore an innocent covering message. Hidden messages on messenger's body were also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head. The message allegedly carried a warning to Greece about Persian invasion plans. The method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow and restrictions on the number and the size of messages that can be encoded on one person's scalp. |
| **IMAGE STEGANOGRAPHY : OVERVIEW**  Steganography aims to hide information in a cover data in such a way that non-participating persons are not able to detect the presence of this information by analyzing the information detection. Unlike watermarking, steganography does not intend to prevent the hidden information by opponents of removing or changing the hidden message, which is embedded in the cover data but it emphasizes on remaining undetectable. Steganography is particularly interesting for applications in which the encryption can not be used to protect the communication of confidential info.  Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited.Image Steganography is the technique of hiding the data within the image in such a way that prevents the unintended user from the detection of the hidden messages or data. |
| To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, ltering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files. The project deals with learning about the various types of steganography available. Image steganography is performed for images and the concerning data is also decrypted to retrieve the message image. Since this can be done in several ways, image steganography is studied and one of the methods is used to demonstrate it. Image steganography refers to hiding information i.e. text, images or audio files in another image or video files. The current project aims to use steganography for an image with another image using spatial domain technique. This hidden information can be retrieved only through proper decoding technique. This encryption and decryption of the images is done using C codes.    **WORKING :**  The Encoding Process :  The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process. For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text file.  The Decoding Process :  The offset of the image is retrieved from its header. Create the user space using the same process as in the Encoding. Using the functions the data of the image is taken into a byte array. Using the above byte array, the bit stream of the original text file is retrieved into another byte array. And the above byte array is  FIG : LSB ALGORITHM  written into the decoded text file, giving the original message.    **USE CASE DIAGRAM :**      **SENDER**  **RECEIVER**      **ADVANTAGES :**   * The main advantage of this system is that it provides security to your messages without the third party. * Number of bits have been replaced according to user or sender, therefore third parties can not guess passwords. * Normal network users can't guess the image. * In steganography anyone cant jump on a suspect by looking at images. * It is Reliable. * Easy to use. * Easy Maintenance. * Systems have been secured by password authentication.   **DISADVANTAGES :**   * Images can have attacks like diluting, nosing, contrast changes and so on. * Number bits of pixel should be replaced by equal bits of message. * If someone is eavesdropping then there is a probability of the message to unfold. * If more than two people have the same steganography software then hidden messages can be acquired. * Intruders may penetrate suspecting images to get hidden data.     **APPLICATIONS :**   * Condential Communication and Secret Data Storing. * Protection of Data Alteration. * Access Control System for Digital Content Distribution. * E-Commerce. * Media. * Database Systems. * Digital Watermarking.   **FUTURE SCOPE :**  Steganography, though, is still a fairly new idea. There are constant advancements in the computer eld, suggesting advancements in the eld of steganography as well. It is likely that there will soon be more efficient and more advanced techniques for Steganalysis. A hopeful advancement is the improved sensitivity to small messages. Knowing how difficult it is to detect the presence of a fairly large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image! It is like finding a microscopic needle in the ultimate haystack. What is scary is that such a small le of only one or two sentences may be all that is needed to commence a terrorist attack. In the future, it is hoped that the technique of Steganalysis will advance such that it will become much easier to detect even small messages within an image. In this work it explores only a small part of the science of steganography. As a new discipline, there is a great deal more    research and development to do. The following section describes areas for research which were of shoots of, or tangential to,our main objectives.  1. Detecting Steganography in Image Files:  Can steganography be detected in images files? This is a difficult question. It may be possible to detect a simple Steganographic technique by simply analyzing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image in a random way or encrypts the data before embedding, it may be nearly impossible to detect.  2.Steganography on the World Wide Web:  The world wide web(www) makes extensive use of inline images.There are literally millions of images on various web pages worldwide. It may be possible to develop  3.Steganography in printed media:  If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded data be recovered?  This would require a special form of steganography to which could allow for inaccuracies in the printing and scanning equipment.    **TESTING**  **TEST PLAN :**  Testing define s the status of the working functionalities of any particular system. Through testing particular software one can’t identify the defects in it but can analyse the performance of s software and its working behaviour . By testing the software we can find the limitations that become the conditions which the performance is measured on that particular level. In order to start the testing process the primary thing is requirements of the software development cycle. Using this phase the testing phase will be easier for testers.The capacity of the software can be calculated by executing the code and inspecting the code in different conditions such as testing the software by subjecting it to different sources as input and examining the results with respect to the inputs.  There are two types of testing . The functional testing, which defines the specified function of a particular code in the program. This type of testing gives us a brief description about the program’s performance and security in the various functional areas.  The other type of testing is non-functional testing. Non-functional testing defines the capabilities of particular software like its log data etc. It is opposite to functional testing and so will not describe the specifications like security  and performance.    **TEST CASES :**  START UP - SCREEN DISPLAY   |  |  |  | | --- | --- | --- | | **TEST DESCRIPTION** | **EXPECTED OUTCOME** | **AS EXPECTED** | | Open Software | Software was opened without glitches and anamolies. | Yes | | Action > Encrypt image | Encryption option will appear and the option to select an image appears. | Yes | | Action >  Decrypt Image | Decryption option will appear and the  option to select an image appears. | Yes | | Action>Browse | A dialogue box will appear to select the image from the system. | Yes | | Action>close | The software will be closed. | Yes | | Action>Encrypt  (If no image is  loaded first) | A dialogue box will appear showing error,encryption  information is  incomplete. | No | | Action>Decrypt  (If no image is  loaded first) | A dialogue box will appear showing error,text boxes must not be empty. | No |     ENCRYPTION :   |  |  |  | | --- | --- | --- | | **TEST DESCRIPTION** | **EXPECTED OUTCOME** | **AS EXPECTED** | | Select image from hard drive. | Image will be selected if there  are no errors while selecting. In case of any error an  appropriate pop up will be displayed. | Yes | | Perform the  Steganography | Operations will be performed. | Yes | | View the Image | The image will be displayed if steganography has been successfully  performed on it. | Yes |   DECRYPTION :   |  |  |  | | --- | --- | --- | | **TEST DESCRIPTION** | **EXPECTED OUTCOME** | **AS EXPECTED** | | Select an Image  File for Decryption | Image will be selected if there are no errors while selecting. In case  of any error a window will be  displayed. | Yes | | Action>Decrypt | The decrypted image occurs. | Yes |     **RESULT :**  Steganography was performed and the image was encrypted with the secret message and then the decryption was performed to ensure  the working of the project.  FIG: ARCHITECTURE    FIG: ENCRYPTION FIG: DECRYPTION |
| **CONCLUSION**  It is observed that through LSB Substitution Steganographic method, the results obtained in data hiding are pretty impressive as it utilizes the simple fact that any image could be broken up to individual bit-planes each consisting of different levels of information. It is to be noted that as discussed earlier, this method is only effective for bitmap images as these involve lossless compression techniques.But this process can also be extended to be used for color images where, bit plane slicing is to be done individually for the top four bit-planes for each of R, G, B of the message image.  It is also important to discuss that though steganography was once undetected, with the various methods currently used, it is not only easy to detect the presence but also retrieving them is easier. For instance, without having to use a software or complex tools for detection, simple methods to observe if an image has been manipulated are: 1. Size of the image: A Steganographic image has a huge storage size when compared to a regular image of the same dimensions. I.e. if the original image storage size would be few KBs, the Steganographic image could be several MBs in size. This again varies with the resolution and type of image used. 2. Noise in image: A Steganographic image has noise when compared to a regular image.This is the reason why initially little noise is added to the cover image, so that the Steganographic image doesn't appear very noisy when compared to the original cover image. |