Image Watermarking with Capacity Analysis

P SOWJANYA[1], REVATHI CHILLAPALLI[2]
[1] *Associate Professor, CSE Department, PSCMRCET, Vijayawada, A.P, India*
[2] *Graduate Student, CSE Department, PSCMRCET, Vijayawada, A.P, India*

Abstract*— In the present world, communicating online without worrying about outside interference is getting harder. especially those industries that share sensitive data, such as the military, governmental agencies, and private businesses. They spend a lot of money and energy trying to get the development of secure communication methods. Security over communication channels is promoted by image processing encryption approaches that use a variety of algorithms and distinct analysis methods. techniques that set our tool apart in terms of information security. Various steganographic techniques exist nowadays that transform our confidential message into a stego medium and transmit it across a variety of communication channels. We increase the security of our message by employing algorithms like BlindHide in conjunction with a variety of analytical techniques that will enhance our tool's ability to reveal information about the encoded accuracy and size of our secret message. Our goal is to create a tool that will provide a benchmark value indicating the exact location of our message within our cover file. We can determine the information on the stego medium's presence in our message by using bulk analysis and Stego. Our tool is improved and made more secure by all of these analysis techniques.

Index Terms- Steganography, Stego-Image, Encryption, Digital Image Processing, and Cryptography

I. INTRODUCTION

Third parties cannot access our data because of cryptography. It covers the technique of employing symmetric and asymmetric cryptography algorithms to encode our message as ciphertext. This mechanism's risk factor is that it gives hostile users the ability to "know" that a secret message is being sent between users. When using steganography, we hide our message in a different medium (sometimes referred to as a "stego medium") that enhances security and eliminates any possibility of a message being transferred to an unauthorized party. By utilizing diverse steganography-based analysis processes, it is possible to attain secure communication.

Using steganography, private communications can be shielded from prying eyes. This is not the same as cryptography, which is a technology for encrypting and decrypting data and protecting our information. Steganography is a trickery and concealment technique. This is a way to protect messages while keeping confidential information hidden. It isn't a form of cryptography because no data is altered or a key is required. Rather, it is a very subtle concealing of knowledge that can be carried out in ways that are misleading. Steganography may be a technique that safeguards confidentiality, whereas cryptography may be a science that primarily protects privacy.

DIP's objective is to manipulate photos in order to change or remove pertinent information. Pixels are individual image elements that are referred to as digital images. The Digital Number (DN) assigned to these pixels can be used to identify them. Digital image processing is the technique of processing graphical images using a computer. It is essential to realize that a digital image consists of a finite set of components, each of which has unique characteristics. These consist of pixels, pels, picture constituents, and image elements.

II. RELATED WORK

[1] Taha and associates When we discuss steganography, we are discussing covert communication. In order to ensure that confidential information is transmitted in a way that cannot be guessed at, this paper explains the significance of steganography. Together with the application of cryptography, our hidden image is better encrypted. Achieving confidentiality and integrity is the primary objective of cryptography and steganography. Our goal is to stop illegal users from accessing our data. These two strategies will encourage more security, which will lead to improved communication. It offers

security by preventing anyone from accessing the confidential data.

[2] Al-Khodaidi and others Important multi-media exists for security-related purposes. A crucial and efficient intermediary method for enhancing the security of sensitive data is counting-based secret sharing. This essay focuses on improving the image. reorganized employing the LSB bits. Our ultimate stego image should have less distortion and be of higher quality. The least significant bits are used by the LSB method, which stores data in them. This is the most widely used method since it can produce relatively little distortion in comparison to conventional methods. The data can be in more than simply text; it can also be in bitmap, audio, video, and other formats. Both 1-bit and 2-bit methods are employed; the 1-bit approach selects one zero to generate a key; a decreasing number of zeros will result in fewer shares; the 2-bit method uses the target key to create shares for users. Steganography is useful for protecting our data and encrypts messages using a variety of multimedia formats.

Table 2.1: Comparative study on steganographic techniques

S.No	Author Name	Algorithm	Advantages	Disadvantages
1.	Taha	algorithms for asymmetric encryption (AES). code for secret encryption (SEA). security algorithms that rely on keys.	robust encryption that is quicker.	difficult to put into practice. high upkeep.
2.	Al Khodaidi	Bit that is least significant (LSB).	Simple to put into practice	not secure and susceptible to steganography.

III. PROPOSED SYSTEM

The steganographic algorithm and analytical techniques can be combined to create a highly encrypted message when we need stronger protection. This has shown to be a highly useful tool for communication encryption. This method's straightforward yet intricate task is to transform plain text into encrypted text, which is subsequently transformed into a stego picture. For the target communicator, we can get the original data back using conventional decryption techniques. The fundamental concept is employing steganographic techniques to encrypt a cover carrier and a secret message. The greatest instrument for enabling strong information security is this double encryption method. The simplest method for concealing information in an image is called BlindHide. The top left corner of the portion in the image is where the hiding technique begins. The method involves traversing over the image's bits and matching each secret message bit character to its corresponding image bit character, pixel by pixel. It follows the pixel color's significant bit shift to correspond with the message that has to be put.

Using a loss-less picture format and replacing the x least significant bits of each pixel in scan lines throughout the image with the binary data is a simple way to secure binary data on an image. This is not safe since an attacker can easily get the secret data by just repeating the method. This strategy is called "BlindHide" since it conceals the information in an indiscernible manner and is not very good at it. The image's initial portion is distorted, while the remaining portion remains the same.

3.1 ALGORITHMS RELATED TO STEGANOGRAPHY

The information is secured by the four algorithms that are present. While some include data without filtering

the image, others do. What unites them all is that they are all using the Least Significant Bit (LSB) algorithm to repair the data that has to be hidden in the cover image's pixelation.

3.1.1 BlindHide Algorithm

Initially, This technique hides the data pixel per pixel using a bitmap picture. The data is used to replace the least important bits. This procedure offers a simple means of data security. Although it is a line-by-line procedure, it is not always secure. Our information is vulnerable to attack by outside parties. The attacker can obtain information by repeating the procedure. It is done in a mindless manner. This method isn't always organized.

Choose a private message.

1) Change the hidden message to a numeric value.
2) Convert the value in decimal to a binary number in eight bits.
3) Select a 24-bit picture (PNG, JPEG, or BMP).
4) Find the decimal value of the image matrix.
5) Go back to binary numbers with 8 bits.
6) Picture manipulation.
7) Start reading the image from the upper left corner of the image.
8) Starting with the message bit on the left, insert message bits into the picture bits.
9) In a fresh picture, replicate the insertion value (stego).

3.1.2 Stego Analysis

Steganalysis adheres to a conventional procedure whereby features are first extracted from the provided medium and then utilized for steganography feature detection. There are two categories of features: deep features and handcrafted features. Popular elements in the Handcrafted include statistical Features are taken out by hand. Although the second category isn't stated clearly, deep autoencoders or neural networks can automatically extract it. Classification is used to distinguish between the cover image and the stego image after feature extraction. Three methods are used in this process. The initial phase in this classification is statistical strategy. This involves using an empirical threshold to ascertain whether confidential information is present. In order to learn the process cover medium, machine learning is applied. It may now split the stego picture and cover. The neural network serves as the last resort and is employed for both feature extraction and classification.

Multi-media files, including audio, video, and image files, are employed in stego analysis. The primary purpose of these files is to conceal the secret message, and stego analysis is used for this procedure.

3.1.3 BenchMark Analysis

In addition to comparing original and stego photos, this analysis will assess stego images independently. The constructor's choices determine which tests are executed. Benchmarks can also be output as plain text by it. This makes the following possible: generating a random message, merging two folders for the stego output, and producing a CSV file to graph the laplace values of an image. Our tool uses photos to conduct a number of benchmarks. In addition to comparing original and stego photographs, it will assess stego images on their own.

The constructor's choices determine which tests are executed. Our goal is to construct our output benchmarks in plain language so that the user can assess them. Largely, ego analysis tools are conventional. The technological community is more focused on perfecting for notable reasons. universal concepts, steganography, rather than refining steganographic techniques. However, the creation of a sophisticated steganalysis tool necessitates the existence of steganography applications.

3.1.4 Bulk Analysis

Bulk steganalysis is limited to uniformly merging a folder containing messages with another folder containing photos using a single algorithm. After a steg analysis, the data are output to the appropriate folder and the original folder.There is no deletion of the concatenated files from the temporary folder. The only file types that will be mixed with.jpg,.png, and.bmp picture files are.txt message files.All other types of files within the specified folders will be disregarded.

3.2 ARCHITECTURE OF THE SYSTEM

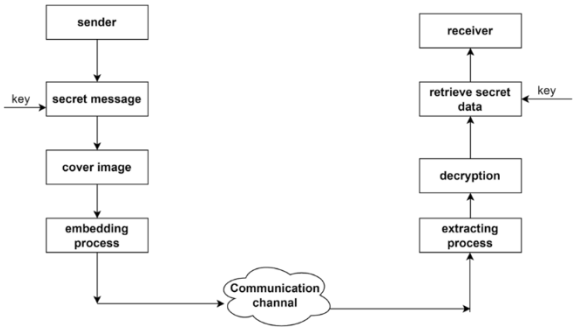

Fig 3.1: System Architectur

[a] Problem Definition: Encoding and decoding our message in a stego_image
Input: stego_image and bitmap_image
Output: embeddedstegoimage

The following are the steps in the algorithm:

1. The encryption key and the inputs for both stego_image and bitmap_image are supplied by the sender.
2. The embedded stego_image is now prepared to be sent over a communication channel to the recipient after being password-encrypted.
3. Lastly, the receiver will obtain the finished image following receipt of the stego_medium and key entry.

IV. EXECUTABLE RESULTS

These procedures enable us to obtain the result that our secret message is embedded in an image. Steganographic techniques are used for the encryption process, and the same algorithm is then used for the extraction process, yielding the embedded stego image with the secret message.

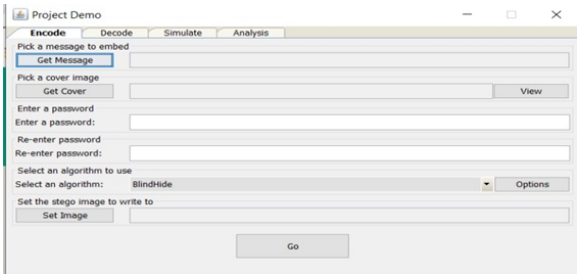

Fig 4.1: Built Tool

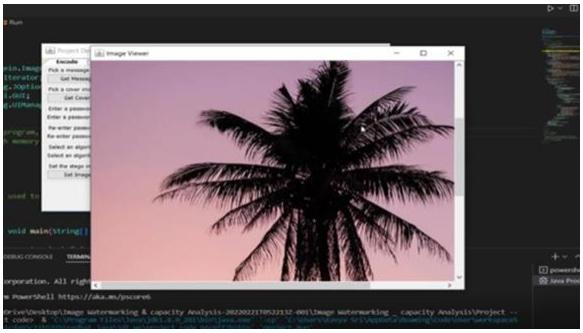

Fig 4.2: Stego_image

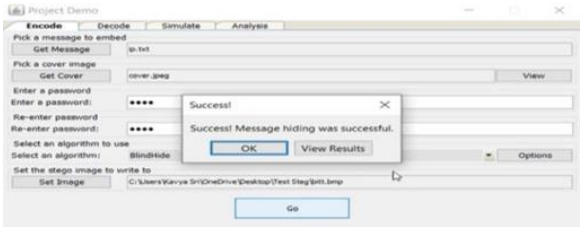

Fig 4.3: Embedded confirmation

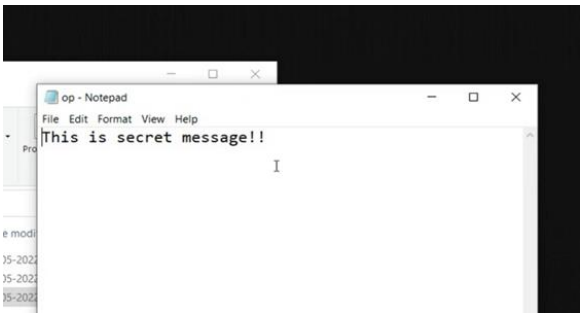

Fig 4.4: Output file of out embedded message

CONCLUSION

In this study, we argued that, given today's environment of well-equipped attackers with hostile hacking techniques, protecting sensitive data is a critical task.Our suggested method offers a means of concealing our data inside a stego image, which can only be accessed with a password that is shared by the sender and recipient. We guarantee that the best method of securely communicating is through the use of cryptography and steganography in our proposed system. Mechanisms for capacity analysis, such as bulk, benchmark, and steg analysis, will improve the tool's usefulness by revealing information that is buried therein.

REFERENCES

[1] Alzuabidi, H. M., Hashim, M. M., Taha, M. S., Mohd Rahim, M. S., and Lafta, S. A. (2019). Combination of Steganography and Cryptography: A Short Survey. Materials Science and Engineering IOP Conference Series, 518, 052003. doi:10.1757-899x/518/5/052003;1788

[2] AlKhodari, T., Gutub, A. Improving the propagation of picture steganography for multimedia counting-based secret-sharing with improved security. Appl 80 Multimed Tools, 1143–1173 (2021). There is a 10.1007/s11042-020-09720-w available.