International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.8May - June – 2024
DOI:10.46647/ijetms.2024.v08i03.032 ISSN: 2581-4621

Text Hiding by Image using LSB

T. Raghavendra Gupta[1], Prakash Saw[2], Nithul K.C[3], Nehal Kumar Singh[4], S. Srikar Reddy[5]

[1]Associate Professor, Department of CSE, HITAM, T.S
[2]B. Tech Student, Department of CSE, HITAM, T.S
[3]B. Tech Student, Department of CSE, HITAM, T.S
[4]B. Tech Student, Department of CSE, HITAM, T.S
[5]B. Tech Student, Department of CSE, HITAM, T.S

***Abstract*—**In most defence and research organization, they need to send and receive important textual information related to weapon designs, maps, and satellite details. If this textual information is sent normally, hackers can intercept it, and the imported information can be leaked. To prevent this, data can be hidden under an image. This process involves a plain text and an image file. We will use a cover image file and the message, and then taken into consideration the cover image pixels. In that image, we will embed each bit of secret text until the last bit of secret text is hidden under the image. Then we can send this image file to the client, who can use reverse process to retrieve the original text from the image. There are many techniques and algorithms in cyber security to hide data, and each technique has its own importance. The technique used in this study is Least Significant Bit (LSB).

***Keywords*—Textual Information, satellite-details, LSB, hidden under image**

INTRODUCTION

Secure Image Communication is the art and science of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden message. By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. Today, the term Secure Image Communication includes the concealment of digital information within computer files. For example, the sender might start with an ordinary looking image file, then adjust the color of every 100th pixel to correspond to a letter in the alphabet a change so subtle that someone who isn't actively looking for it is unlikely to notice it. It is also called Digital Water Marking. because it also holds digital information within computer file. Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Image hiding refers to the process of hiding data within an image file. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. It is argued that the encryption Software implementations of ciphers are usually too slow to process image and video data in commercial systems. Hardware implementations, on the other hand, add more cost to service providers and consumer electronics device manufacturers.

LITERATURE REVIEW

Existing System

The responses to various research articles are documented below by the order of the number that have been used to specify them in the references in the end. In the year of 2011 Brazil, A.L. Sanchez, A. Conci, A. Behlilovic.et The study of Internet connects more people, increasing the need

DOI:10.46647/ijetms.2024.v08i03.032 ISSN: 2581-4621

for transmitting secure information. One way to protect the data sent over the web is to conceal the relevant information inside a typical image, hiding the data from intruders. They proposed a hybrid heuristic, combining a genetic algorithm and the path re-linking meta heuristic to efficiently solve this problem. In this way, the inclusion of a path re-linking procedure can significantly improve the performance of a genetic algorithm for the problem considered. In the year of 2011 Bhowal, K. Sarkar, D. Biswas, S. Sarkar.et al presented the Audio hiding that is a method that ensures secured data transfer between parties normally in internet community. In this present a novel, principled approach to resolve the remained problems of substitution technique of Audio hiding. In the first level, here authors first extract image data from an image file. In the second level, authors use a powerful GA (Genetic Algorithm) based LSB (Least Significant Bit) Algorithm to embed the image data into audio data. Here image data bits are embedded into random and higher LSB layers. consequential in increased robustness against noise addition. On the other hand, GA operators are used to reduce the distortion. Outcomes show that, if we provide a relatively good initial GA can fine-tune the output, and produce more security in order to protect the data not to be read by the third party or it cannot get into unauthorized access. In the year of 2012 Qiangfu Zhao, Akatsuka, M. Cheng Hsiung Hsieh.et al proposed the study of an image morphing based method for information hiding. The basic idea is to hide a secret image into a morphed image which is obtained from the secrete image and another reference image. To make this method useful, it is necessary to produce natural morphed images. To produce natural mor 7 phed images, we should choose a proper feature point set (FPS) for morphing. This work if we do it manually, because the number of possible FPSs is very large. They adopted interactive genetic algorithm (IGA) in this study and conducted experiments for generating facial images. In the year of 2012 Khosravi, M. Soleymanpour Moghaddam, S. Mahyabadi.et al investigated a method is proposed which is based on the spatial domain: Least Significant Bit (LSB) with Genetic Operators. The LSB matching method proposed by Mielikainen utilizes a binary function to reduce the number of changed pixel values. While in this a bipolar evaluating system is proposed to assess the performance of different orders for LSB matching with Genetic Algorithm. Afterward a genetic algorithm strategy is employed to search for an optimal solution among all the permutation orders. The experimental outcomes show that by employing the proposed bipolar evaluating system, the distortion of the image is reduced while the probability of detection is decreased. In the year of 2012 Sanchez, A. Conci, A. Zeljkovic, E. Behlilovic, N. Karahodzic.et at pre sented the study on increasing range of data types which are exchanged over this network (video, audio, text messages) emphasize the security problem that this way of communication has. The flood of multimedia contents in the structure of transmitted data has made the appearance of images in this network quite normal. This revived the use of hiding data within images in order to hide information to avoid unauthorized access. A much used technique for this purpose, the LSB (Least Significant Bits) technique. Which was chosen to be the message carrier. These differences make quite a path for a crypt analyst to doubt the authenticity (independence) of the picture itself.A. Zeljkovic.et at Palette based images, such as GIF images, are popular image file format commonly used on the Internet. GIF images are indexed images where the colors used in the image are stored in a palette or a color lookup table. GIF images can also be used for Text Hiding, although extra care should be taken. The main issue with the palette based approach is that if one changes the least significant bit of a pixel, it could result in an entirely different colour since the index to the colour paletle gets modified. One possible solution to this problem is to sort the palette so that the colour differences between consecutive colors are minimized. The strong and weak points regarding embedding information in GIF images using LSB is that since GIF images only had a bit depth of 8, the total amount of information that could be embedded will be less.

A. Limitations of Existing System

While hiding data under an image using steganography techniques like LSB can provide a level of security, there are some limitations to consider.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.8May - June – 2024
DOI:10.46647/ijetms.2024.v08i03.032 ISSN: 2581-4621

• The size of the cover image needs to be larger than the size of the message being hidden. This means that if the message is too large, it may not be able to be hidden under a cover image without being noticeable. Additionally, if the cover image is compressed or re sized, it may distort or lose the hidden message, making it difficult to retrieve the original data.
• Steganography techniques like LSB are vulnerable to attacks from advanced algorithms and techniques used by attackers to detect the presence of hidden data. As a result, it is important to use additional security measures to protect the data, such as encryption and authentication.
• Steganography can be used to hide data, it does not provide protection against interception or unauthorized access to the communication channel. Therefore, it is essential to use secure communication channels and protocols to ensure that the data is protected during transmission. There is a lack of security in existing system. There was manual processing of data which resulted in a time-consuming process.

METHODOLOGY

A. Steganography

Steganography in image data hiding is the practice of hiding secret information within an image file in a way that it is not visible or detectable to the human eye. The goal of steganography is to conceal the presence of the hidden data in the image, while minimizing any perceptible changes to the image itself. Steganography, an ancient practice with modern implications, involves concealing secret information within digital media to avoid detection. Its historical roots trace back to methods like invisible ink and hidden messages within wax tablets, evolving alongside advancements in digital technology. In the contemporary digital landscape, steganography finds applications across various domains, including covert communication, cybersecurity, privacy protection, and digital forensics. Least Significant Bit (LSB) insertion: This is one of the most commonly used techniques in steganography. It involves replacing the least significant bit of each pixel in the image with a bit from the secret message. This technique is simple and effective, but it can result in a loss of quality in the image if too much data is hidden.

Encoding: In the encoding the text message will be embedded into the image file. The embedding will be done based on the principle of ”Least Significant Bit” (LSB) algorithm. The LSB algorithm uses the least significant bits of each pixel and replace with the significant bits of the text document, such that the message will be encrypted into the image. This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security. Encoding involves the use of a code to change original data into a form that can be used by an external process. The type of code used for converting characters is known as American Standard Code for Information Interchange (ASCII), the most commonly used encoding scheme for files that contain text. ASCII contains printable and nonprintable characters that represent uppercase and lowercase letters, symbols, punctuation marks and numbers. A unique number is assigned to some characters. The standard ASCII scheme has only zero to 127 character positions; 128 through 255 are undefined.

The problem of undefined characters is solved by Unicode encoding, which assigns a number to every character used worldwide. Other types of codes include BinHex, Uuencode (UNIX to UNIX encoding) and Multipurpose Internet Mail Extensions (MIME). Encoding is also used to reduce the size of audio and video files. Each audio and video file format has a corresponding coder-decoder (codec) program that is used to code it into the appropriate format and then decodes for playback. Encoding should not be confused with encryption, which hides content. Both techniques are used extensively in the networking, software programming, wireless communication and storage fields.

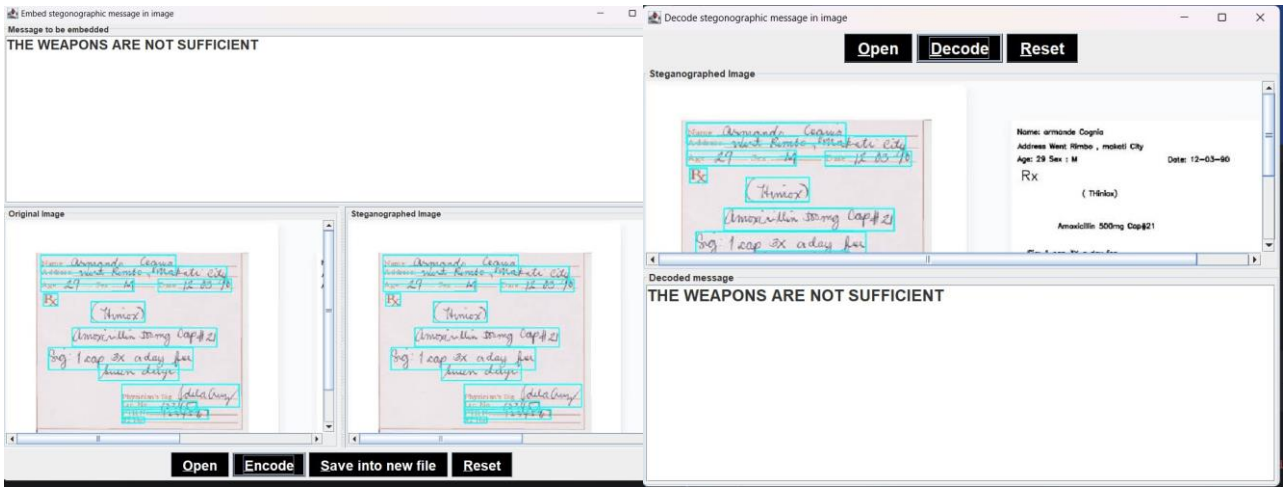
Decoding: In the decoding module, the receiver receives the carrier image from sender through the transmission medium. The receiver then sends the carrier image to the decryption phase. In the decryption phase, the same Least Significant Algorithm is implemented for decrypting the least significant bits from the image and merge in an order to frame the original message bits. After successful arrangement, the file is decrypt-ed from the carrier file and accessed as an original text

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.8May - June – 2024
DOI:10.46647/ijetms.2024.v08i03.032 ISSN: 2581-4621

document. Most computers use an encoding methodology to transfer, save or use data. Data to be encoded are transformed via an encoding mechanism (for example, the American Standard Code for Information Interchange (ASCII) or BinHex) and transmitted via a communication medium. As an example, when sending an email, all data, including certain attachments and images, are encoded using a format such as Multipurpose Internet Mail Extensions (MIME). When data arrives, decoding converts the email message content to its original form.

Least Significant Bit prediction: LSB stands for Least Significant Bit. It is a term commonly used in computing and digital signal processing, particularly in the context of binary numbers and binary representation of data. In binary representation, each digit is called a bit, and these bits can represent the presence or absence of certain features, signals, or values. In a binary number, each bit holds a place value, with the rightmost bit having the smallest place value (1), and the leftmost bit having the largest place value 2n. The least significant bit (LSB) is the bit in a binary number with the smallest place value. It represents the smallest unit of change in the value of a binary number. For example, in the binary number 10110, the LSB is 0, as it is the rightmost bit. LSB (Least Significant Bit) prediction is a technique used in digital signal processing and data compression to predict the value of the least significant bit of a signal or data point based on the values of its more significant bits. The basic idea behind LSB prediction is that the least significant bit of a data point is often the most random and unpredictable, while the more significant bits contain more useful information. LSB prediction can be used in various applications, such as audio and image compression, where the least significant bits can be removed or quantize to reduce the amount of data without significantly affecting the quality of the signal or image. By predicting the value of the LSB based on the more significant bits, the compression algorithm can achieve better compression ratios with minimal loss of quality. LSB manipulation finds applications in encryption, where its alteration may compromise cryptographic security, and in digital watermarking and steganography, enabling covert data embedding within media files without perceptible degradation. Understanding the LSB is crucial for tasks ranging from data encoding and manipulation to security and multimedia processing, underscoring its pivotal role in digital systems. Its significance spans across various domains: in binary arithmetic, it dictates the smallest unit of change during addition or subtraction operations. In digital audio and video, the LSB corresponds to the smallest amplitude or colour variation, impacting signal quality, particularly in compression algorithms.

Input and Output Images



DOI:10.46647/ijetms.2024.v08i03.032 ISSN: 2581-4621

References

[1] Fonteneau C., Motsch J., Babel M., and D'eforges O.,"a hicrarchical selective acryption technique in a scalable image codes*, Iniemational Conference in Communications, Bucharest, Romania 2008.

[2] M. M. Fisch, H. Signer, and A. Uhl, "Layered Encryption Techniques for DCT- Coded Visual Data," in European Signal Processing Conference (EUSIPCO) 2010, Vienna, Austria, sep., 2010.

[3] Han Shuihua and Yang Shuangyuan, Non-members,"An Asymmetric Image Encryption Based on Matrix Transformation', ecti transactions on computer and information technology vol. 1, no.2 November 2011.

[4] M. Van Droogenbroeck and R. Benedett, Techniques for a Selective Encryption of Uncom pressed and Compressed Images, in Proccodinas of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2012, Ghent, Belgium, Sept. 2012.

[5] Xiliang Liu, Selective encryption of multimedia content in distribution networks; daliages and new directions". Proceedings of Communications, Internet, and lufirmation Technology (CIT 2003), Scottidale, AZ, USA, Nov. 2016.