Grenze International Journal of Engineering and Technology, June Issue

Securing the Data using Steganography Technique in Images

Dr. Sharath M N[1], Anil Kumar K N[2], Dr. Arjun B C[3] and Harshitha S[4]
[1]Assistant Professor, Department of Computer Science and Engineering, Rajeev Institute of Technology, Hassan, India
Email: sharathmn64@rithassan.ac.in
[2]Assistant Professor, Department of Information Science and Engineering Rajeev Institute of Technology, Hassan, India
Email: akanilgowda@rithassan.ac.in
[3]Professor, Department of Information Science and Engineering, Rajeev Institute of Technology, Hassan, India
Email: bc.arjun@rithassan.ac.in
[4]Assistant Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India
Email: sh@mcehassan.ac.in

***Abstract*—Since ancient times, it has been necessary to conceal secret communications and tranfer information without leaks. In today's technology, all available digital media, such as photographs, sound files, films, and so on, provide a rich environment for hiding information that the human eye cannot detect and exploiting unused or redundant data bits. This information can be used to convey messages to hidden agents, but it can also be used as a pressure technique to deliver additional messages within a single file, minimizing the amount of data that must be transferred. This paper demonstrates two methods for encoding /storing a message within the RGB pixels of a cover image (canvas image) without causing visual distortion. A message is broken up into several chunks, converted to 8-bit binary values, encrypted with a simple symmetric exclusive OR (XOR) encryption key, and then encoded into a canvas image by changing the least significant bit (LSB) of the pixel value in both directions. The first approach saves the secret message sequentially, beginning with the top-left pixel, and then encodes the secret message from top to bottom and left to right. The second method randomly encodes the cover image's pixels with the hidden image's message bits, making the concealment less sensitive to scrutiny.**

***Index Terms*— Steganography, image file, video file.**

I. INTRODUCTION

Steganography is stated as "the art of concealing messages within other media files," or "the act of concealing secret information within files such as audio files, image files, video files, and so on." This allows people to establish a hidden entity that can only be determined by those who understand the encoding means and have the password key. Steganography is comes from the Greek word for "covered writing." The cover picture, the hidden message, and the Stegano-image are the three essential pieces of a steganography system. The diagram below depicts the general structure of steganography.

There are numerous methods for implementing steganography, however the most prevalent is the LSB algorithm (Least Significant Bit) concealment. The least significant bits of distinct bytes of the canvas image are updated with a bit from the secret message that will be buried in it in this procedure. Steganography is an ancient

Grenze ID: 01.GIJET.9.2.417

technique. It has been used from prehistoric times. Prior to the development of computers, individuals used a variety of means to hide a message. One method for concealing or hiding communications was to hide them in other persons.

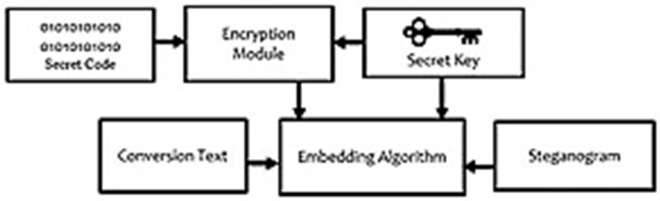

Figure 1: General structure of a steganography

The ancient Greeks used to shave the leader of a delivery guy and tattoo a message on his head, then dismiss him when his hair grew back. Another method used by people was to write a message on silk, encase it in wax, and have a messenger ingest it. The communication would be recovered at a later time. Both of these strategies were effective when the message was not time sensitive. Another method for concealing messages inside regular and random items, such as the bunghole of a beer barrel. When an envoy sent blank folding tablets with a message scrawled under the wax, the Spartans were warned of an impending attack by Xerxes. Because steganography was widely employed during World War II, various steganographic techniques were developed.
The multi-layer perceptron model is regarded as the best model for identifying speech emotions. This is due to the fact that, when compared to other models like SVM, KNN, etc., the MLP classifier is more suitable for datasets with complicated structures [6]. In recent years, Deep Learning has drawn increased interest and is thought to be a developing field of research in ML [4]. On the other hand, speech-based classification techniques like natural language processing (NLP) and SER are greatly enhanced when recurrent structures like recurrent neural networks (RNNs) and long short-term memory (LSTM) [22].

II. Literature Review

Maciej et al. [1] proposes various variations of imperceptibility and talk about their fittingness by building solid instances of Stegano frameworks and spread content conveyances. A tight logical connection between the undertaking of finding the utilization of Stegano frameworks and the assignment of separating between conceivable spread content conveyances is gotten. Arshiya et al. [2] present a similar investigation and execution examination of various picture steganography strategies utilizing different kinds of spread media with the conversation of their record positions. They likewise talk about the inserting areas alongside a conversation on striking specialized properties, applications, confinements, and steganalysis. Rosal Ignatius De Moses Setiadi [3] suggests a method to enhance the payload message by installing messages using the Least Significant Bit (LSB) technique on the expanded edge zones. Messages are not simply placed on the LSB; instead, they are jumbled using XOR operations with the Most Significant Bit (MSB) in order to add security aspects.
The plot is supposed to produce results after encoding and packing the mystery information, according to Mohammed Mahdi Hashim et al. [4]. It is transmitted while arranging the mystery message to follow and direct each component of the Stego picture and coordinating the mystery bits with the LSB during installation to determine 0 (P_Even) and 1 (P_Odd). In order to improve the steganography, the results suggested implanting a mystery message based on P_Even/P_Odd with two control arbitrary parameters. A steganographic scheme based on the RGB shading spread picture is presented by Shiv Prasad et al. in their paper from [5]. The pixel-esteem differencing (PVD) method sequentially inserts the secret message bits into each colour pixel. The mysterious information is then placed on each square independently using the PVD method. To create the three adjusted shading sections, the two covering squares are straightened. The spread picture's installation restriction has been improved by the concept of covering squares. In order to conceal the mystery information in an image, Aditya Kumar et al. [6] suggest a novel n-rightmost-piece substitution picture steganography technique, where 1 B n B 4. The key goals of the suggested approach are: (1) raising the peak signal to noise ratio (PSNR); (2) raising the insertion limit (EC); (3) avoiding the fall of the limit problem (FOBP); and (4) demonstrating fortitude in the face of salt and pepper uproar and RS attack. The mystery information's n bits and the n-rightmost bits for each pixel are first converted to decimal quality.
Another steganographic method called remote cushioning (Wipad) is presented by Krzysztof et al. [7]. It hinges on incorporating secret information into the softening of edges at the physical layer of the distant neighbourhood

(WLANs). The method used to accommodate an exhibition study based on a Markov model recently proposed and accepted by the authors uses gauges from the IEEE 802.11 a/g standard. The results show that the Wipad can transport steganographic data at a maximum rate of 1.1 Mbit/s for information outlines and 0.44 Mbit/s for affirmation outlines. This is the largest known steganographic organisation channel, as far as the designers can tell. Gandharba Swain [8] offers a very high limit steganography method that makes use of differencing and replacement elements. It divides the image into 3-pixel squares that aren't covered. The least significant bit (LSB) replacement is applied to two LSBs for each pixel of a square, and remainder esteem differencing (QVD) is applied to the remaining six bits. There are therefore two levels of installation: (I) LSB substitution at lower bit planes and (ii) QVD at higher piece planes. If a square that has been inserted into this design still has a problem with falling off the edge, it is rectified from the above cross breed installing and a modified 4-piece LSB replacement is used. Sum and Difference Covering Set (SDCS), a versatile steganography method developed by Xue et al. [9], allows for the early evaluation of noisy pixels in accordance with an iterative commotion level assessment concept.

Vipula et al.'s [10] focus was on combining different information security models for safe interactive media correspondence. They did this by combining steganography and encryption techniques. Evidently, the Advanced Encryption Standard (AES) was used by the inventors as a cryptography technique. The particular security challenges for sight and sound correspondence across dispersed computing conditions have been audited by Sharath M. N. et al. [11] in this study. Various approaches, such as cryptography and steganography, have been looked at. Additionally, hybrid security frameworks combining steganography and cryptography have been evaluated for their effectiveness in securing the exchange of sound and visual information through cloud foundations.

III. Motivations

Steganography has evolved to deal with the introduction of digital media in the modern world. With the prevalence of digital cameras and the ease of worldwide access that the internet provides, there are a myriad of media in which we can conceal information. Steganography techniques have grown in popularity during the previous few decades. One reason for this is that many governments prohibit the use of cryptography in digital media; therefore, the covert method of steganography is required to convey a private message. Many people were also afraid that terrorist organisations were transmitting hidden messages via the internet and movies.

IV. Proposed Methodology

We employ the least critical section of each pixel of a picture to hide a message within a digital message. Each pixel is composed of three eight-bit whole integers that save the shading estimation in each image, as seen in the fig 2.

For example, 255 red, 255 green, and 0 blue results in yellow shading. By supplanting the least significant piece in each of these shading esteems, it is possible to conceal a secret message, a little at a time, without affecting the shading esteems excessively, as shown in fig 3. The overall idea behind LSB algorithm is shown in below fig 4.

V. Process of Steganographic Encoding

Encoding concealed messages utilizing steganography follows the essential procedure layout. The message is initially dismembered to see whether it is a book or pictorial communication. The message type and message structure are estimated in an 8-piece Header that is utilised to reconstruct the message during the Decoding Process. The Header is associated with the beginning of the message, and this new united message is encoded using a clear symmetric Exclusive OR (XOR) encryption key that adheres to the bit basis shown in Tables 1 and 2.

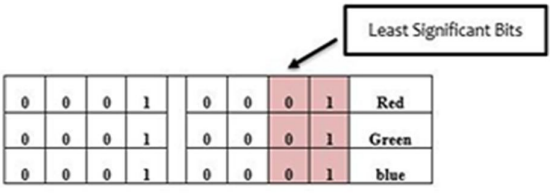

Figure 2: Least significant bit representation

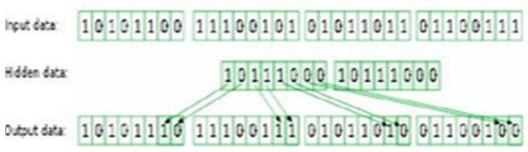

Figure 3: Hiding of bits

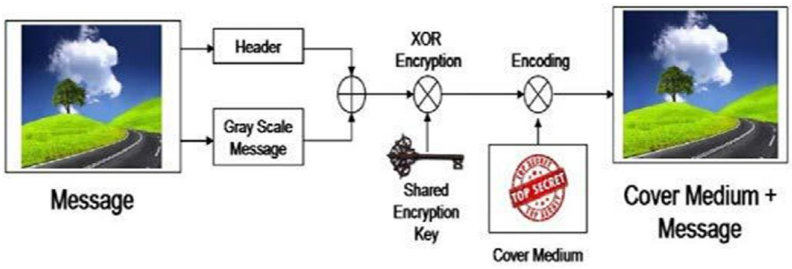

Figure 4: Encodin process outline

XOR is a valuable addition to symmetric encryption since a comparable encryption key may be used to recover the Plaintext from the Cypher text in Table 2. We can clearly see that if we are to successfully retrieve the initial message, we must utilise the same encryption key for the unscrambling procedure. Finally, the scrambled Header and Message are encoded onto the Cover Medium Image's least important bits in one of two methods.

General embedding algorithm

Begin

Burden the spread picture, Convert picture to byte cluster

Convert message data to byte bunch

If

Message can't be contained in spread picture exit with botch message

Else

For each piece in the message byte

Begin

Conceal message bit in the LSB of the relating spread picture byte

End

VI. STEGANOGRAPHIC DECODING PROCESS

The fundamental approach set forth as follows is used to decipher and recover the buried message. With this tactic, the consequences of the encoding technique are turned around, revealing the puzzle's message. Fig 5 shows the decoding process outline.

The Header is always decoded, and then XOR unscrambled and separated to determine the estimations and message type. The message is then encoded and XOR unscrambled before being reassembled using the Header estimate information. The combined Header respects are retrieved from the Cover Medium Image and decoded using the same XOR encryption key that was used during encoding. The Header estimation respect (length for content; width time's stature for picture message) is employed to select the stop and inspiration for the recuperation tally, reducing the diverse nature and reviving the recuperation process.

TABLE I. BIT LOGIC

Message value	Encryption key value	Encrypted value
0	0	0
0	1	1
1	0	1
1	1	0

TABLE II. XOR ENCRYPTION BIT LOGIC

Encoding	Decoding
Plaintext:10101010	Cipher text:10100101
Encryption key:00001111	Encryption key:00001111
Cipher text: 10100101	Recovered Plaintext:10101010

The script then recovers the whole combined Message from the Cover Medium Image by determining when to cease utilising the Header Dimensions. The recovered Message is unscrambled with the same XOR encryption key that was used during the encoding process. Finally, if the message type includes a picture, the programme re-tries the main photo from the unscrambled message contents for display using the recovered Header's stature/width assumptions.

General decoding algorithm

Begin

Burden Stenganographic picture

Convert steganography picture –into byte exhibit
If
Decoding type is LSD
Begin
For the initial 32 byte
Duplicate the LSB into a variety of length 32
Beginning from length 32+1 of the steganographed - picture cluster
Begin

Duplicate the LSB of comparable steganographed exhibit into a variety of length 8
Convert the cluster into a byte worth and spare in the comparing list of the made exhibit
Convert the exhibit an incentive into string or picture
End
End

MATLAB script files are used to implement the Sequential and Pseudo-Random Encoder and Decoder functionalities. Message transposition and XOR encryption are also included for added protection. It is created a simple user-input function that allows a user to encode and decode their own concealed messages in MATLAB without the need for preloading variables.

VII. Result and Discussion

Snapshot of the actual outputs given by the program based on text inputs and image inputs as shown in fig 6, fig 7, fig 8, and fig 9.

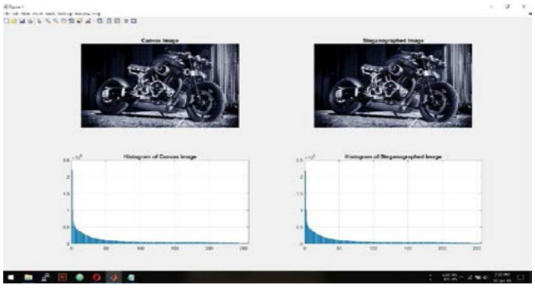

Figure 6: Text encoding steganography out analysis

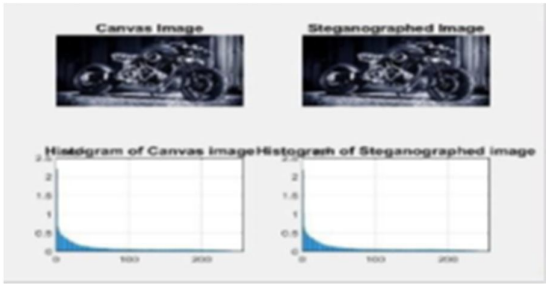

Figure 7: Text encoded steganography output histogram

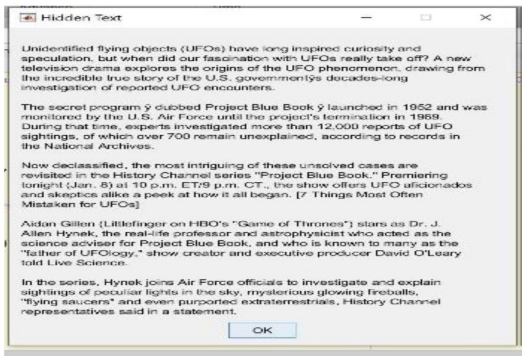

Figure 8: Text decoding steganography output

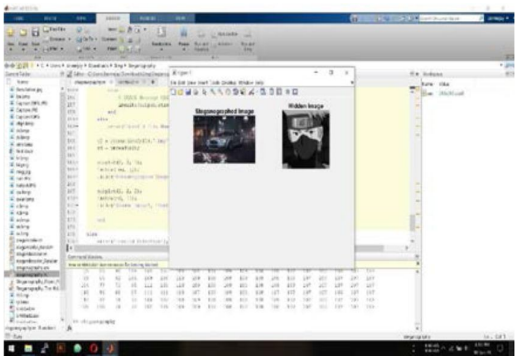

Figure 9: Image encoding steganography inpu

VIII. Conclusion and Future Scope

Hidden messages continue to be an essential and expanding science that allows for the secure transport of information. Steganographic techniques and processes take advantage of detecting limitations in the human visual system to store messages in digital media's underutilized/redundant bits. This work used MATLAB to develop relatively simple sequential and pseudo-random encoding and decoding algorithms. Adapting these abilities into a more proficient and web-friendly organisation is a natural extension of this work and would

provide an intriguing correlation. Although steganography makes it difficult to determine the proximity of a hidden message, steganalysis employs factual evaluation apparatuses and processes to separate and recover message information from a spread picture. Another area for future research would be to assess the effectiveness and relative security of our systems.

REFERENCES

[1] Maciej Liśkiewicz, Rüdiger Reischuk, and Ulrich Wölfel. Security levels in steganography – insecurity does not imply detectability. Electronic Colloquium on Computational Complexity (ECCC), 22(10), 2015.

[2] Ansari, A. et al. (2019). A comparative study of recent steganography techniques for multiple image formats. IJCNIS. 1 (1), p11-25. in press. doi:5815/ijcnis.2019.01.02

[3] D. R. I. M. Setiadi, "Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation," Intl J. Electron. Telecommun., vol. 65, no. 2, pp. 295–300, 2019.

[4] Mahdi, Mohammed Hashim, et al. "Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption." IOP Conference Series: Materials Science and Engineering. Vol. 518. No. 5. IOP

[5] S. Prasad, A.K. Pal.An RGB colour image steganography scheme using overlapping block-based pixel-value differencing,Open Science, 4 (4) (2017), Article 161066

[6] Sahu, A.K.; and Swain, G. (2019). A novel n-rightmost bit replacement image steganography technique. 3D Research, 10(1), Article 211.

[7] Szczypiorski, K. and Mazurczyk, W. Steganography in IEEE 802.11 OFDM symbols. Security and Communication Networks 3 (2011), 1–12.

[8] Swain, G. (2018). Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. Arabian Journal for Science and Engineering2018,1-10.doi: https://doi.org/10.1007/ s13369-018-3372-2.

[9] B.Xue, X. Li and Z. Guo, "A New SDCS-based Content-adaptive Steganography Using Iterative Noise-Level Estimation," 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Adelaide, SA, 2015, pp. 68- 71.

[10] Vipula Madhukar Wajgade, "Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 4, April 2013.

[11] M. N. Sharath, T. M. Rajesh and M. Patil, "Analysis of Secure Multimedia Communication in Cloud Computing," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 2019, pp. 136-144, doi:10.1109/ICICICT46008.2019.8993352.

[12] Sharath M N, Dr. Rajesh T M, Dr. Mallanagouda Patil. "Novel video Steganography approach with the combination of knight tour and 7th bit model of embedding data". EEO. 2021; 20(4): 657-669. doi:10.17051/ilkonline.2021.04.70.

[13] Sharath, M.N., Rajesh, T.M. & Patil, M." Design of optimal metaheuristics based pixel selection with homomorphic encryption technique for video steganography".Int.j.inf.tecnol.14, 2265–2274(2022). https://doi.org/10.1007/s41870-022-01005-9.

[14] Sharath M N, Dr. Rajesh T M, Dr. Mallanagouda Patil. "A Novel Encryption with Bacterial Foraging Optimization Algorithm based Pixel Selection Scheme for Video Steganography". Multimedia Tools and Applications.https://doi.org/10.1007/s11042-023-14420-2