Journal of Information Hiding and Privacy Protection
DOI:10.32604/jihpp.2021.026760
Article

Tech Science Press

Pixel Based Steganography for Secure Information Hiding

N. Shyla* **and K. Kalimuthu**

SRMIST, Kattankulathur, Chennai
*Corresponding Author: N. Shyla. Email: sn3657@srmist.edu.in

Received: 04 January 2022; Accepted: 13 January 2022

Abstract: The term “steganography” is derived from the Greek words steganos, which means “verified, concealed, or guaranteed”, and graphein, which means “writing”. The primary motivation for considering steganography is to prevent unapproved individuals from obtaining disguised data. With the ultimate goal of comprehending the fundamental inspiration driving the steganography procedures, there should be no significant change in the example report. The Least Significant Bit (LSB) system, which is one of the methodologies for concealing propelled picture data, is examined in this assessment. In this evaluation, another procedure for data stowing indefinitely is proposed with the ultimate goal of limiting the progressions occurring in the spread record while hiding the data with the LSB technique and making the best cover to make it difficult to get concealed data. The RGB (Red, Green, and Blue) pixel esteem based stegnography technique is proposed in this proposition. The claim to fame of this calculation is that, unlike other stegnography calculations, we do not change the pixels unless absolutely necessary.

Keywords: LSB; RGB; pixel based steganography

1 Introduction

The speed with which communication has advanced around us has recently been astounding. Nowadays, everyone relies on rapid Personal Computer systems such as the internet for information/data trade, which is quite unsecure and data can be exposed. For a variety of reasons, a large amount of personal data is often obtained, used, and transferred to third-party organizations. As a result, information security is becoming a major concern in information exchange via the internet or other information platforms. To protect sensitive information, we can use Stegnography or Cryptography. Because the proposed mystery message does not stand out for scrutiny, stegnography is generally seen as preferable to cryptography.

Stegnography is the act of placing data in a certain showcase known as covering media without making any discernible changes to it. The goal is to shroud an implanted document inside the disseminated medium to the point where the presence of the installed record is obscured. Based on a photograph The covering media for stegnography is photographs. For picture-based stegnography, a few techniques have been proposed, with LSB being the simplest. Stegnography takes on the primary role of secretly transmitting messages. Sound/video recordings, advanced pictures, and other media have all been used to build and implement unique message concealing tactics in the past.

Consider a Digital Colour Image, each pixel is made up of a blend of RGB colours (Red, Green, and Blue). At each pixel in a 24-piece bitmap, there will be 8 bits addressing all three concealing regards (Red, Green, and Blue). It creates a diverse range of colours. Because the data is so large, even a little increase in pixel power has no discernible effect. Furthermore, the human visual system is incapable of perceiving minute changes in the pixel. In RGB Intensity Based Variable-Bits Image stegnography portray’s new count for RGB picture-based steganography. This figuring presents consideration of a reasonable number of bits for each pixel's channel (R, G, or B) in light of the pixel's genuine concealing estimates.

1.1 Issue Statement

Wherever on the planet, documents containing numerous information, for example, pictures, video, sound, content are shared in seconds. This system, which makes our life simpler, accompanies intense security gaps. To stay away from this security openings, we are utilizing cryptography and steganography idea.

1.2 Existing System

In existing, the clearest method is LSB (Least Significant Bit) Stegnography. In this assignment, for trade we have considered LSB Steganography and RGB Stegnography. There exist two sorts of LSB Stegnography procedures–LSB1 Stegnography and LSB2 Stegnography.

1.3 Disadvantages

The drawback of the present strategies is that it adds uproar to the image which makes the image look dull or grainy making it suspicious for a person about nearness of a covered message inside the image.

1.4 Proposed System

The proposed methodology in this endeavor is RGB pixel look on based steganography technique. The distinguishing strength of this computation is that we do not change the pixels like other steganography figuring's except for if it is totally required.

During the encryption method the Stegano program will look at the image and will incorporate the specific RGB pixel, separate it from other pixel and find the mod value of that RGB pixel. If mod value matches the character, that region in the image could be used to address the character.

The issue arises on to what extent we will have the choice to store the region of a pixel which can recognize a character. We can either store it in an alternate book report or make it as a part of the image metadata itself. We are proposing to make it part of the image metadata itself.

1.5 Advantages

In this strategy, the information cannot be effectively unraveled regardless of regardless of how it is obtained, because it is wrapped in both outlines and encryption.

2 Related Work

Triple-A disguise system is acquainted as another strategy with conceal advanced information inside picture based medium. The calculation includes more randomization by utilizing two unique seeds created from a client picked key so as to choose the component(s) used to conceal the mystery bits just as the quantity of the bits utilized inside the RGB picture part. This randomization includes greater security particularly if a functioning encryption system is utilized. The limit proportion is expanded above SCC and pixel pointer plot. Triple-A has a limit proportion of 14% and can be expanded if increasingly number of bits is utilized inside the component(s) [1].

Another steganography strategy exhibited, examined and actualized. This strategy conceals the mystery message dependent on contrasting and looking through the least noteworthy bits of RGB picture in a request of (3 bits to R-segment 3 bits to Gcomponent-2 bits to B-component) by which we can shroud a solitary character in one pixel picture, so just proper number of pixel pictures are required to conceal the mystery message. While we are choosing a pixel picture haphazardly, picture will not get influenced in the issues of goals and clearness. The proposed technique was contrasted and the LSB and progressed LSB strategies which shroud the information in least huge bits and indistinguishable bits [2].

This examination paper proposes a verified, strong methodology of data security utilizing steganography. It presents two segment-based L-S-B (Least Significant Bit) stegano-graphy strategies for installing mystery information at all noteworthy bits of blue segments and fractional green segments of arbitrary pixel areas in the edges of pictures. A versatile L-S-B based stegano-graphy is proposed for implanting information dependent on the information accessible in MSB's (Most Significant Bits) of red, green, and blue segments of arbitrarily chosen pixels across smooth zones [3].

A half and half element identification channel is additionally recommended that performs better to anticipate edge territories even in uproarious conditions. AES (Advanced Encryption Standard) and arbitrary pixel inserting is consolidated to give two-level security. The trial aftereffects of the proposed approach are better as far as PSNR and limit. The examination investigation of yield results with other existing strategies is giving the proposed approach an edge over others. It has been altogether tried for different steganalysis assaults like visual investigation, histogram examination, chi-square, and RS investigation and could continue every one of these assaults quite well [4].

The point of this examination is to structure a steganography calculation which shroud the message behind the picture as well as give more secure than other concepts. With the end goal of security, encryption method is utilized with a client characterized key. In the calculation structured by creator a message is stow away into a picture as a picture that is utilizing picture age technique message is changed over into the picture of predefined arrangement and afterward by utilizing planned calculation that picture will stow away into the spread picture. RGB picture design is utilized to improve the nature of the stego picture. Finally, that R-G-B picture will spare as B-M-P picture record with the goal that no lossy pressure can happen and the first message do not wreck and can be separate for what it's worth [5].

Information stowing away is the craft of concealing information for different purposes, for example, to keep up private information, secure classified information, etc. There are heaps of systems utilized for information stowing away and the outstanding procedure is the Steganography. In contemporary terms, Steganography has advanced into a computerized technique of concealing a record in some type of sight and sound, for example, a picture, a sound document or even a video document. This paper displays another Steganography technique dependent on the spatial area for encoding additional data in a picture by making little changes to its pixels. The proposed strategy centers around one specific famous system, Least Significant Bit (L-S-B) Embedding. Rather than utilizing the L-S-B-1 of the spread for inserting the message, L-S-B-2 has been utilized to expand the heartiness. L-S-B-1 might be altered by the bit of the message, to limit the distinction between the spread and the Stego-spread. For more security to the message bits a Stego-Key has been utilized to permute the message bits before inserting it [6].

3 Methodology

The fundamental wordings utilized in the Steganography frameworks are:

- Spread message
- Secret message
- Secret key
- Embedding calculation

The spread message is the transporter of the message, for example, picture, video, sound, content, or some other advanced media. The mystery message is the data which is should have been covered up in the reasonable media. The mystery key is normally used to implant the message contingent upon the concealing calculation. The installing calculation is the way or the possibility that generally used to implant the mystery data into the spread message. This investigation incorporate picture inside the other picture so above all else need to think about a picture.

The previously mentioned framework engineering has the accompanying two modules:

1. Encoding
2. Decoding

3.1 Encoding

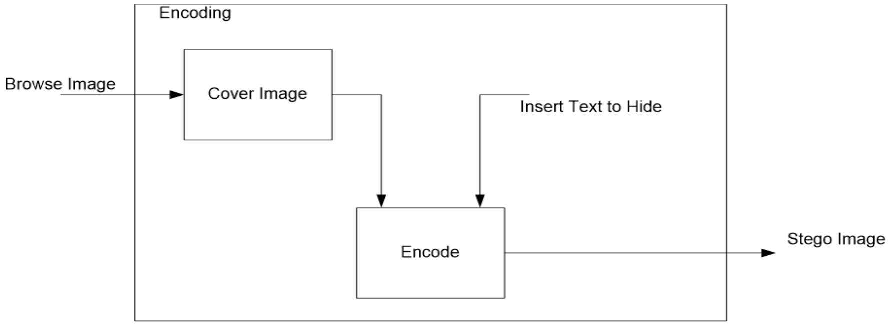


Figure 1: Data hiding into Cover Image

As shown in Fig. 1:

Stage 1: The application prompts for the substance and picture from the sender who needs to cover the message.

Stage 2: Steganographic program scrambles the substance using DES or RSA or some other encryption estimation.

Stage 3: Steganographic program assessments the image to find the pixel estimation of the significant number of pixels inside the image.

Stage 4: Steganographic program uses the novel R-G-B modbit methodology to check whether each letter of the message can be addressed in the image and records the circumstance to a field in the image metadata itself. For tally of modbit the program incorporates the R-G-B estimations of each pixel and segments it to get the mod. In case the mod worth matches with that addressed for the character inside, the circumstance for that character is recorded.

Stage 5: If the image does not have pixel regards to address a particular character, the steganographic program finds and changes a pixel that almost organizes with the image pixel and which can address the character of substance.

Stage 6: Finally, when all of the pixels which can be perceived on the image and its position is recorded close by the image metadata, the customer is instructed that the encryption part is done.

3.2 Decoding

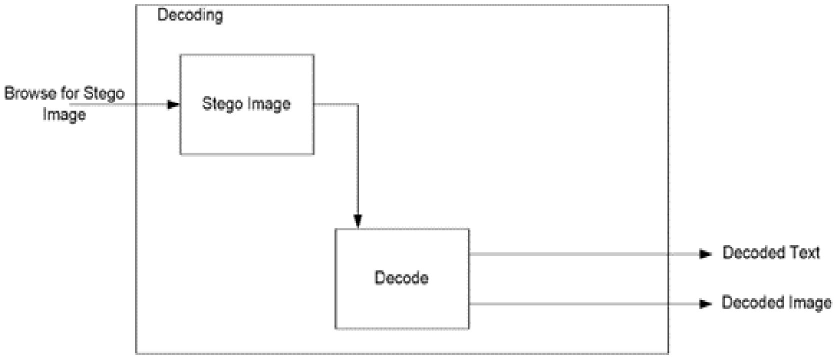


Figure 2: Data unhiding from Stegno Image

As shown in Fig. 2:

Stage 1: The beneficiary opens the image.

Stage 2: The stegano-graphic programming demands key to unravel the image report.

Stage 3: Stegano-graphic programming unscrambles the metadata first and finds the pixel positions.

Stage 4: Using the pixel positions, get the R-G-B regards and disentangles by pivot modbit and finds the looking at mixed substance.

Stage 5: Decrypt this substance and give back the message to the customer.

4 Algorithms

This is minimal complex of the steganography systems arranged in the use of LSB, and thusly the most helpless. Introducing process contains the progressive substitution of each Least Basic Bit (LSB) of the image pixel for the bit message. For its ease, this method can cover an unfathomable volume of information.

The standards are given underneath:

Stage 1: Convert the data from decimal to combined.

Stage 2: Read spread picture.

Stage 3: Convert the spread Image from decimal to combined.

Stage 4: Break the byte to be concealed into bits.

Stage 5: Take starting 8 byte of remarkable data from the spread Image.

Stage 6: Replace the least basic piece by one bit of the data to be concealed.

First byte of interesting information from the Cover picture:

E.g.: - 1 0 1 0 First piece of the information to be covered up: 1

Supplant the least huge piece

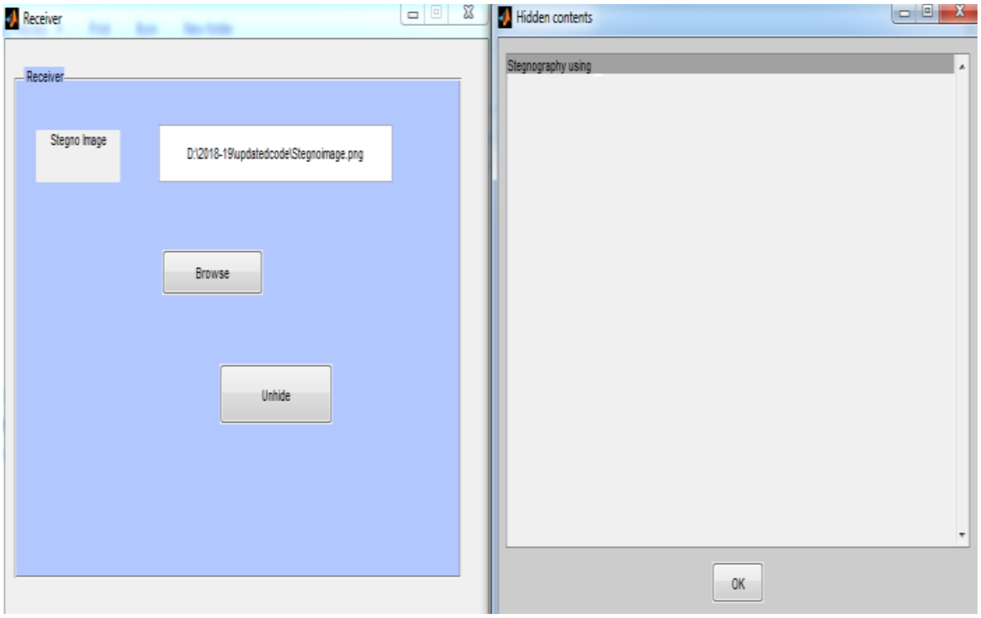
1	1	0	1	1	0	0	0
							□
1	1	0	1	1	0	0	1

This procedure will be proceeded for initial 8 bytes of information and disguise the primary byte of information.

Stage 7: Continue the Stage 6 for all pixels. Pictures in the wake of inserting information utilizing LSB Steganography.

5 Results

Below figures explains the Snapshots for hiding the data into the image. Fig. 3 explains the Sender has to choose a Cover Image and choose text file to gide into the Cover Image. It also displays the time taken in seconds for Hiding the data and PSNR values.



Stegno Image: D:\2018-19\updatedcode\Stegnoimage.png

Stegnography using

Figure 3: Process of hiding the data

Fig. 4 shows the Steganographic image after hiding the data into the Cover Image.

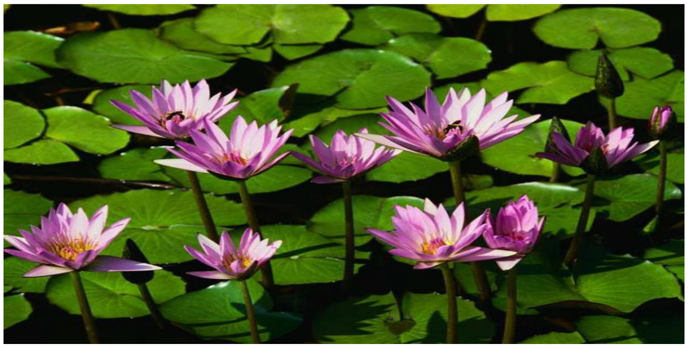
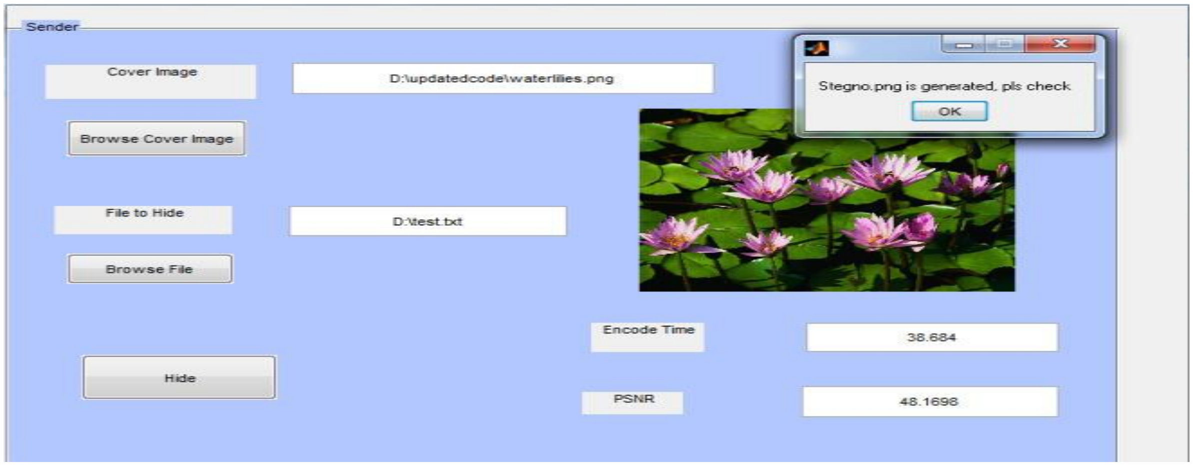


Figure 4: Stegno Image after hiding the data

Fig. 5 explains the unhide or decoding the Stegno Image. And it also displays the data contains in the text after unhiding process.



Cover Image: D:\updatedcode\waterlilies.png

File to Hide: D:\test.txt

Stegno.png is generated, pls check

Encode Time: 38.684

PSNR: 48.1698

Figure 5: Process of unhiding data from the Stegno Image

6 Conclusion

This Paper proposed another procedure for picture based steganography. It exhibits an improved steganography strategy for installing mystery message bit in picture meta- data fields dependent on the R-G-B esteems and the situation of the pixels. The picture pixels will be changed distinctly for values where the calculation cannot discover a pixel which can speak to it.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Refrences

[1] T. Namita and S. Madhu, "Secure RGB image steganography from pixel indicator to triple algorithm–An incremental growth", *International Journal of Security and its Applications*, vol. 4, no. 4, pp. 53–62, 2010.

[2] K. Lakshmi Prasad and T. C. Malleswara Rao, "A novel secured RGB LSB Steganography with enhanced stego-image quality" *International Journal of Engineering and Applications*, vol. 3, no. 6, pp. 1299–1303, 2013.

[3] J. Mamta and S. Parvinder "An improved LSB based steganography technique for RGB color images", *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, pp. 513–517, 2013

[4] Babita and M. Ayushi, "Secure image steganography algorithm using RGB image format and encryption technique", *International Journal of Computer Science and Engineering Technology*, vol. 4, no. 6, pp. 758–762, 2013.

[5] A. E. Mustafa, A. M. F. ElGamal, M. E. ElAlmi and B. D. Ahmed, "A proposed algorithm for steganography in digital image based on least significant bit", *Research Journal Specific Education Faculty of Specific Education (Mansoura University)*, vol. 3, no. 21, pp. 751–766, 2011.

[6] A. Joseph, D. R. Raphael, V. Sundaram, "Cryptography and Steganography–A survey", *International Journal of Computer Technology and Applications*, vol. 2, no. 3, pp. 626–630, 2005.