Secure Information Hiding Over Encrypted Image

N Shyla and K Kalimuthu

March 19, 2020

Secure Information Hiding Over Encrypted Image

Author Shyla N, Dr. Kalimuthu K
School of Engineering and Technology, Jain University, Bangalore.
SRMIST, SRM University, Chennai.
(E-mail: shylaashok@gmail.com)

Abstract— The steganography word is gotten from the blend of the steganos ,which means "verified, concealed or guaranteed", and the graphein, which implies "composing". The essential inspiration driving steganography mulls over is to prevent the disguised data from being to procured by unapproved individuals. With the ultimate objective to comprehend the basic inspiration driving the steganography procedures, there should be unimportant change in the example report. In this assessment, LSB system which is one of the methodologies for concealing propelled picture data is analyzed. In this assessment, another procedure for data stowing endlessly is proposed with the ultimate objective limit the progressions happening in the spread record while hiding the data with LSB technique and to make the most appropriate cover to make it difficult to get concealed data. The proposed strategy in this proposition is RGB pixel esteem based stegno-graphy technique. The claim to fame of this calculation is that we don't change the pixels like other stegno-graphy calculations aside from on the off chance that it is completely required.

Keywords; LSB, RGBB, Pixel Based Steganography, .

I. INTRODUCTION

The correspondence advances around us have developed at an extraordinary pace lately. For trading of information/data nowadays everybody is depending of fast PC systems like web which is very unprotected and data can get uncovered. Huge measure of individual information is frequently gathered, utilized and moved to outsider associations for an assortment of reasons. Subsequently information security is turning into a significant issue in information correspondence by means of web or some other information platform. We can utilize Stegno-graphy or Cryptography to ensure touchy information. Stegno-graphy is frequently viewed as superior to cryptography in light of the fact that the proposed mystery message doesn't stand out to itself for examination.

Stegno-graphy is the demonstration of installing data in a given showcase called covering media without rolling out any unmistakable improvements in it. The objective is to shroud an implanted document inside the spread media to such an extent that the installed record's presence is covered. Picture based Stegno-graphy utilizes pictures as the covering media. A few strategies have been proposed for picture based Stegno-graphy, LSB being the least complex one. Stegno-graphy assumes the focal job stealthily message correspondence. Distinctive message concealing strategies have been created and executed in the past utilizing sound/video records, advanced pictures, and different medias.

Each pixel is a mix of RGB for instance is (Red, Green, and Blue). A 24-piece bitmap will have 8 bits addressing all of the three concealing regards (red, green, and blue) at each pixel. It makes a wide collection of shades. Since the data is colossal, any little change in the pixel power doesn't reveal any noticeable improvement. Furthermore human visual structure can't perceive the little changes in the pixel. In RGB Intensity Based Variable-Bits Image stegno-graphy delineates new count for RGB picture based steganography. This figuring presents taking care of consider number of bits each channel (R, G or B) of pixel subject to the genuine concealing estimations of that pixel.

Issue Statement

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

Existing System

In existing, the most clear method is LSB (Least Significant Bit) Stegno-graphy. In this assignment, for trade we have considered LSB steganography and RGB Stegno-graphy. There exists two sorts of LSB Stegno-graphy procedures – LSB1 Stegno-graphy and LSB2 Stegno-graphy.

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.

Proposed System

The proposed methodology in this endeavor is RGB pixel regard based stegano-graphy technique. The distinguishing strength of this computation is that we don't change the pixels like other steganography figurings except for if it is totally required.

During the encryption method the Stegano program will look at the image and will incorporate the RGB regards, seclude it and find the mod worth. If mod matches the character, that region in the image could be used to address the character.

The issue develops on in what limit 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.

Advantages:

In this strategy, the information can't be effectively unraveled regardless of whether the information is acquired on the grounds that it is shrouded both in outlines and without encryption.

II. RELATED WORK

Namita Tiwari et al., "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth".[1]

Stegano-graphy is the craft of concealing the way that correspondence is occurring, by concealing data in other data. In this paper we have examine two strategies for RGB picture stegano-graphy one is pixel pointer system and other is triple-An algorithem. They utilizes a similar rule of LSB, where the mystery is covered up at all noteworthy bits of the pixels, with more randomization in choice of the quantity of bits utilized and the shading channels that are utilized. This randomization is relied upon to expand the security of the framework and furthermore increment the limit. These procedures can be applied to R-G-B pictures where every pixel is spoken to by 3 bytes to demonstrate the force of red, green, and blue in that pixel. This work indicated appealing outcomes particularly in the limit of the information bits to be covered up with connection to the RGB picture pixels.

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 bit is utilized inside the component(s).

Koyi Lakshmi Prasad et al.,, "A Novel Secured RGB LSB Stegano-graphy with Enhanced Stego-Image Quality",[2]

In this paper another steganography strategy exhibited, examined and actualized. The proposed strategy conceals the mystery message dependent on contrasting and looking through the least noteworthy bits of RGB picture in a request of(3bits to R-segment 3bits to Gcomponent-2bits 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 won't 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.

Stegano-graphy is the study of composing concealed messages so that nobody separated from the expected beneficiary is aware of the presence of the messages. Steganography is a greek source word which is articulated as Stehg-uh-nah-grunf-ee where steganous implies mystery or secured and graphie implies composing. In this paper another steganography procedure is displayed, actualized and examined. The proposed RGB LSB strategy shrouds the mystery message dependent on the examination and looking about the indistinguishable bits between the mystery messages and picture pixel esteems. The proposed technique is contrasted and LSB benchmarking strategy and accomplished an effective picture with upgraded stego-picture quality. The primary inspiration driving the improvement of picture stegano-graphy strategies is its approach to use in different associations to impart between its individuals. It tends to be likewise used to convey between military, insight and mystery specialists. The fundamental point of picture stegano-graphy is to maintain a strategic distance from consideration of the programmers when transmitting shrouded data.

Mamta Juneja et al.,, "An Improved LSB based Steganography Technique for RGB Color Images",[3]

This examination paper proposes a verified, strong methodology of data security utilizing stegano-graphy. 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.

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.

This examination accomplishes the objective of actualizing another steganography approach for pictures. It incorporates three new procedures viz. the half and half element recognition method; two parts based LSB substitution strategy and the versatile LSB substitution system. It accomplished the objective of improved subtlety (determined by utilizing PSNR) with least MSE (mean square blunder) as contrasted and existing methods. It accomplished an improved concealing limit while using 12 bits out of the all out 24 bits of every pixel of RGB shading picture in the edge zones just as smooth zones of the spread picture.

Babita et al., "Secure Image Steganography Algorithm utilizing RGB Image Format and Encryption Technique",[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 spared as B-M-P picture record with the goal that no lossy pressure can happen and the first message don't wreck and can be separate for what it's worth.

The fundamental wordings utilized in the Steganography frameworks are the 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.

A. E. Mustafa et al.,"A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit"[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 Stegano-graphy. In contemporary terms, Stegano-graphy 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 Stegano-graphy 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 LSB-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.

The most outstanding systems to information covering up in pictures are least noteworthy piece (L-S-B) substitution, and concealing and separating strategies. L-S-B is a basic way to deal with inserting data in a picture. In any case, picture control can wreck the concealed data in this picture. Applying L-S-B method to every byte of a 24-piece picture, three bits can be encoded into every pixel, as every pixel is spoken to by three bytes. Applying L-S-B system to every byte of a 8-piece picture, just one piece can be encoded into every pixel, as every pixel is spoken to by one byte.

III. METHODOLOGY

The System architecture is shown below.

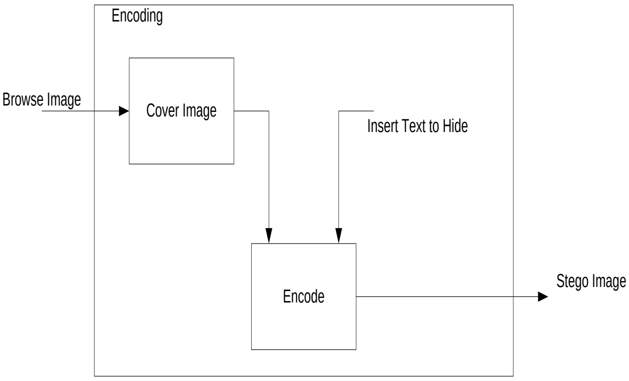


Fig 1: Data Hiding into Cover Image

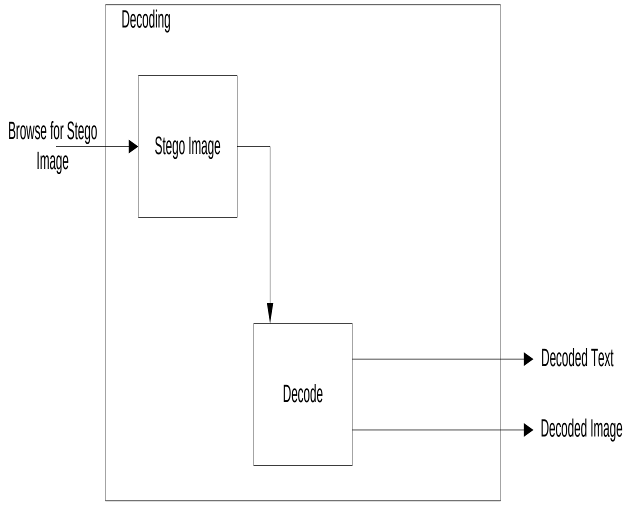


Fig 2: Data Unhiding from Stegno Image

The previously mentioned framework engineering has the accompanying two modules.

1. Encoding

2. Decoding

For Encoding

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

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

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

Stage 4: Stegano-graphic 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 doesn't have pixel regards to address a particular character, the stegano-graphic 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.

For Decoding

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.

IV. ALGORITHMS

This is minimal complex of the steganography systems arranged in the use of L-S-B, and thusly the most helpless. Introducing process contains the progressive substitution of each Least Basic Bit (L-SB-) 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:

Step1: 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 byte of information and disguise the primary byte of information.

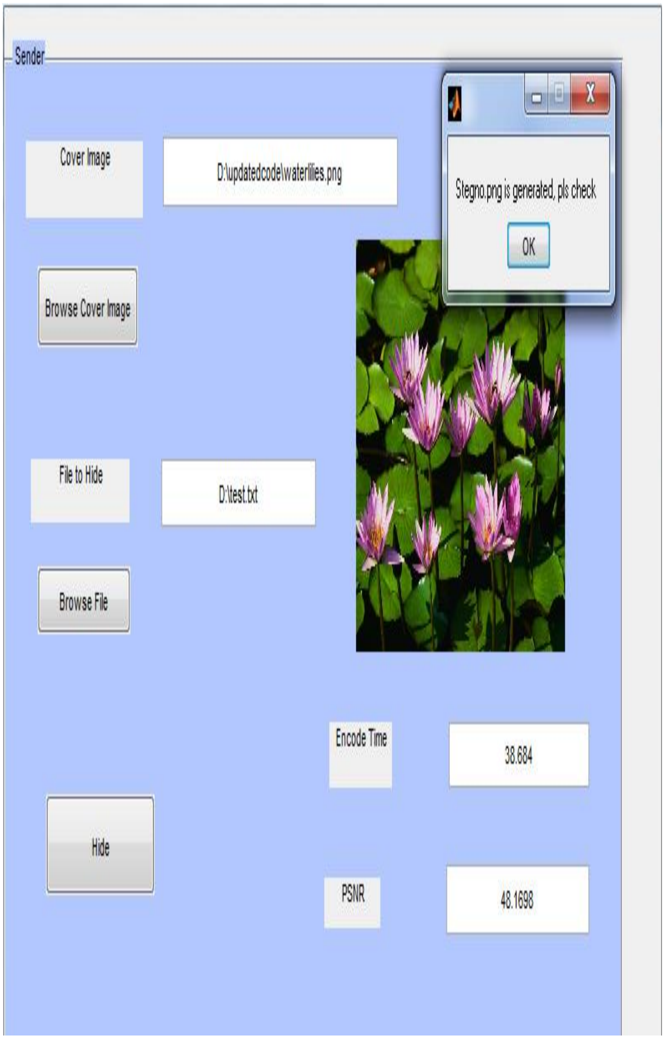
Stage 7: Continue the stage 6 for all pixels. Pictures in the wake of inserting information utilizing LSB Steganography

IV. 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 it shows



Cover Image: D:\updatedcode\waterlilies.png

Stegno.png is generated, pls check

File to Hide: D:\test.txt

Encode Time: 38.684

PSNR: 48.1698

Figure 3: Process of Hiding the Data

Fig 4. Shows the Stegnographic image after hiding the data into the cover image

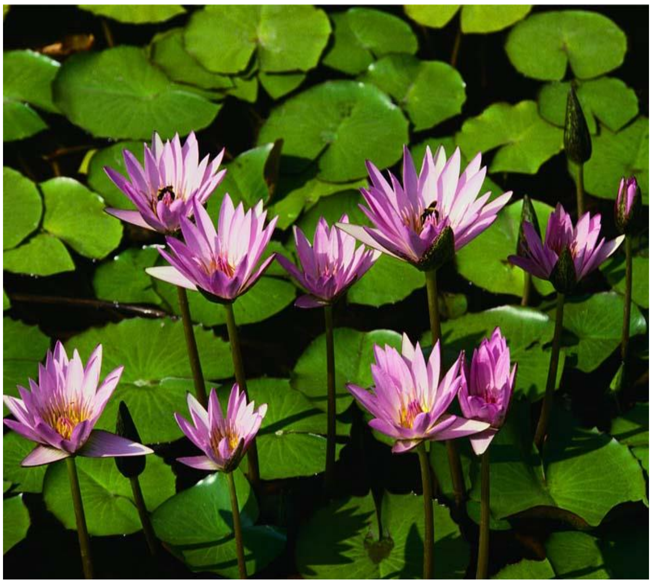
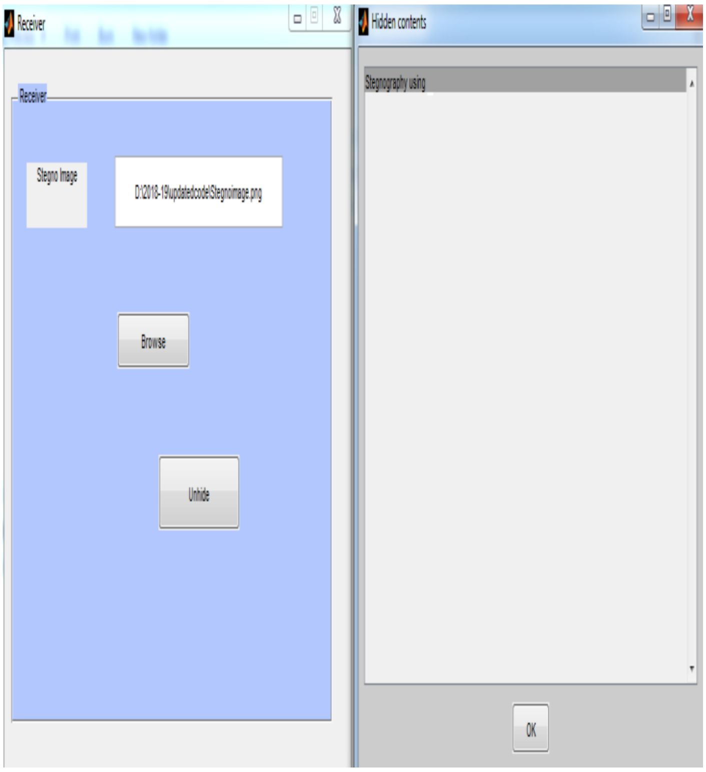


Figure 4: Stegno Image after Hiding the Data

Fig 5. Explains the unhide or decoding the stegno image. And also it displays the data contains in the text after unhiding process.



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

Stegnography using

Figure 5: Process of Unhiding Data from the Stegno Image.

V. CONCLUSION

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

REFRENCES

[1] Namita Tiwari and Madhu Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and its Applications 4(4):53-62, January 2010.

[2] Koyi Lakshmi Prasad and T. Ch. 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] Mamta Juneja and Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", IJCCE 2013 Vol.2(4): 513-517 ISSN: 2010-3743.

[4] Babita and 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, 2011, Issue No. 21, pp. 751-766.

[6] Lee, Yeuan-Kwen and Ling Hwei Chen. "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement."Ninth National Conference on Information Security (1999): 8-15.

[7] A. Joseph Raphael, Dr. V. Sundaram," Cryptography And Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[8] JHP Eloff T Morkel and MS Olivier." An overview of image steganography". Fifth Annual Information Security South Africa Conference (ISSA2005), 2005

[9] Sushil Jajodia. Neil F. Johnson. "Exploring steganography: Seeing the unseen". Computer Practices: IEEE Journal, 1998.

[10] Karen Bailey. Kevin Curran. "Evaluation of image based steganography methods". International Journal of Digital Evidence, 2, September 2003.

[11] Khosravi, Sara,Abbasi Dezfouli, MashallahA New Method to Steganography Whit Processing Picture in Three Colors (RGB) , Int. J. Comp. Tech. Appl., Vol 2 (2), 274-279