A new framework for hidden communication via images from source to destination

[1]Kommaraju Gayatri [2]Mrs.R.Tamilkodi [3]Mr.L.VenkateswaraKiran
[1]PG student [2]Associate Professor [3]Assistant Professor
[1,2,3]Department of computer applications
[1,2,3]Godavari institute of engineering & technology, Rajahmundry, AP
[1]gayathrigaye73@gmail.com [2]tamil@giet.ac.in [3]lvkiran@giet.ac.in

Abstract

Secret communication is one of the key issues in today's communication systems in the era of information. Among the data security methods, Steganography is the mask for hiding confidential information through images. It is currently necessary that data be hidden and systems that the attackers cannot understand the message be established through transporting the stegno-image. Researchers have used various algorithms to provide safe network communication, but secure communication is still a challenge. This paper aims to improve security in the field of interactive technology. The proposed algorithm is RGB split (RGBS) allows the message to be inserted into two pixel channels, and the rest of the channel takes the most repeated bit. Two binary bits of secret message can be stored in each image pixel. The source image is divided into four blocks and then the binary representation of secret message is also split into four blocks. Each block binary data embedded using RGBS technique for each image block.This new steganography algorithm is highly effective in hiding the information inside the image.

Keywords: Image steganography, Data hiding, RGBS technique, security, random number generator, Data extracting, LSB, stegno-image.

1. Introduction

Data security issues are high priority in today's world because millions of users often transmit and receive data. Steganography is a communication method that reduces the risk of attack during media interaction and the information that we want to secretly transmit to the destination is hidden in another type of medium, such as an audio file, video file or image file. Nowadays, data transmitted over the network are combined to achieve a security level in terms of steganography and cryptography. Image Steganography is the most popular intelligence data hiding choice for researchers. Information or data that is being encoded to source image is called Hidden Data and the source image encoded with hidden data is called Stegno-Image. This paper introduced new RGBS technique for embedding the data into an image and which is increase the security in the field of communication technology. Steganography can be used for a number of useful applications, such as: online banking security, secure transmission of confidential data between national and international corporations, , security of army and intelligent departments, and the secure circulatory system of secret documents between defence organizations.

2. Literature survey

U. A. Md. Ehasn Ali, Md. Sohrawordi, Md. Palash Uddin [1] proposed an Robust and Secure Image Steganography using LSB and Random Bit Substitution. In that they used LSB method to embedded the message by using random bit position of the pixel value into an image. by using this random bit substitution, the third party users cannot extract a message even though they cannot find the presence of a secret message in the image.

Rita Rana, Er. Dheerendra Singh [2] proposed an Steganography-Hidden Message in Images Using LSB Replacement method with Pre-Determined Random Pixel and Segmentation of Image. In that they made the hidden message is first encrypted using the data encryption standard and second, encrypted data is encrypted into the binary image by segmenting it into pieces. There are three layers of security, making it difficult for a steganalysis to decode the hidden message. Random pixel selection makes it more difficult to identify a message series resulting in a strong stego image. Split text into sections and instead storing it from block 3 instead of block 1 helps to make the message secure.

Abdul Alif Zakaria , Mehdi Hussain , Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris , Norli Anida Abdullah and Ki-Hyun Jung [3] proposed an High Capacity Image Steganography with Minimum Revised Bits Based on Data Mapping and LSB Substitution. In that they introduced data hidden model based on LSB replacement using a mapping bit strategy. In the proposed method, first hide pixel bits and secret information bits were logically separated into groups. First, such logical groups of four personal data bits were mapped with the (4-MSBs of) cover pixel bits in the embedding process. To preserve the mapping status between cover and hidden data, the (2-bit) LSB substitution method was used.

Karthikeyan B, Asha S, Poojasree B [4] proposed an Gray Code Based Data Hiding in an Image using LSB Embedding Technique. In that thay introduced Digital image related algorithms related to the binary and gray code. If you attach and convert the text file to the gray code, hide it in the digital image and then decrypt it.

3. Proposed System

A image with an embedded file inside can sometimes be widely opened to many dangers that risk secret data. The new method is embedding and extracting the data into an image using RGBSDH technique. In proposed system architecture as shown in fig.1 and it explains how it will be processed for data embedding and data extraction using RGBS technique. In sender side upload an image and that image divide into four equal blocks based on height and width of the image then split the secret message into four blocks [2]. Embedded each splitting message into each equal part of image using RGBS technique. After embedding the image is called as stegno-image. The stegno-image is send to receiver through network. The receiver collect the stegno image and retrieve the hidden message using RGBS technique.

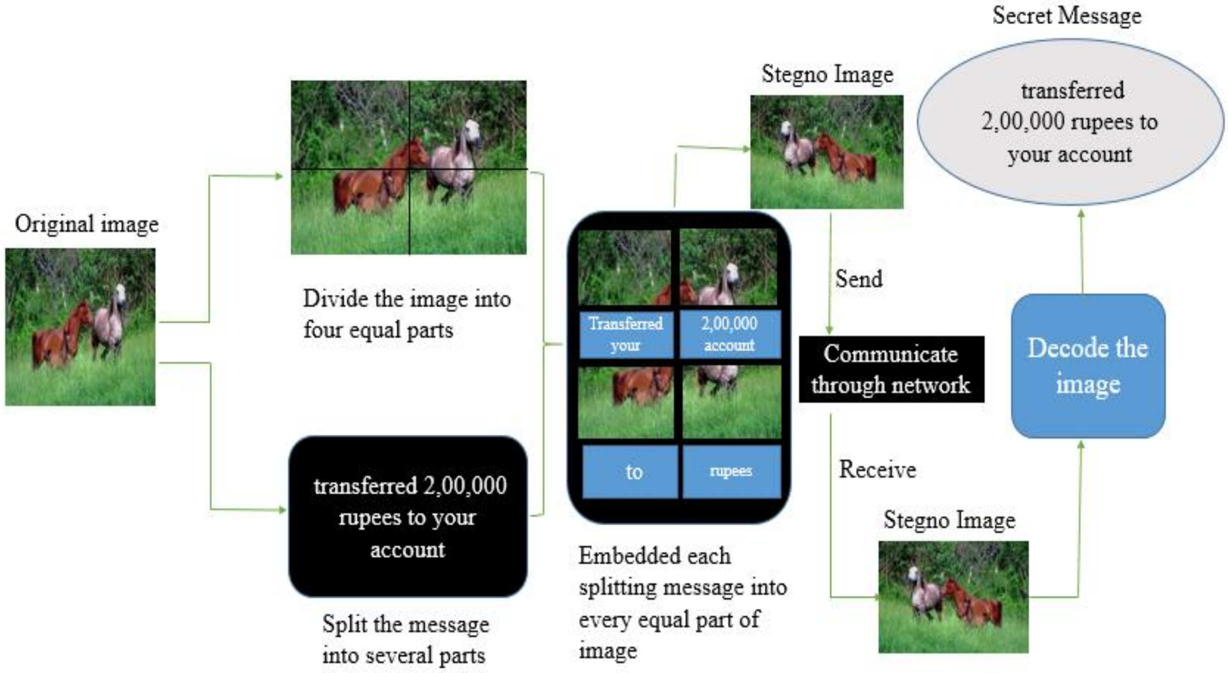

Original image
Divide the image into four equal parts
transferred 2,00,000 rupees to your account
Split the message into several parts
Transferred your
2,00,000 account
to
rupees
Embedded each splitting message into every equal part of image
Stegno Image
Send
Communicate through network
Receive
Stegno Image
Secret Message
transferred 2,00,000 rupees to your account
Decode the image

Figure.1 System architecture for image steganography using RGBS technique

The 24-bit RGB colour images use 8bits each, representing a pixel for the red, green and blue values. The proposed method uses a 8-bits of secret message can embedded in 4-pixels. The overall method shown in fig.(2) and fig.(3).

3.1 Data Embedding Process

In fig.2 shows how RGBS technique used for hiding the secret data into an image. This method converts the secret message into binary form to be embedded into the image. Here for embedding the each letter can take 4-pixels and each pixel can store 2-bits of secret data and also every pixel select one channel in the form of BRGB pattern. In each selected channel can choose most repeated bit (either 0 or 1) and remaining two channels can replace second least significant bits with Exclusive-OR operation [1][3] of secret bit and repeated bit. For example if the message is 01110010 and divide the secret message into four parts (each part contains 2-bits). Each 2- bits of data can store in one pixel. In pixel-1 choose B channel most repeated bit 1 (as shown in fig.1) and in R channel is 00101101 can replace second least significant bit with Exclusive-OR operation of secret bit and repeated bit (0 ⊕ 1 =1) after this process the resultant R-channel is 00101111 then modify the B channel similarly as the procedure of R-channel. After embedding two bits of secret data in pixel-1 then choose R channel in pixel-2 most repeated bit for embedding next 2-bits of secret data and remaining secret bits embedded using these process.

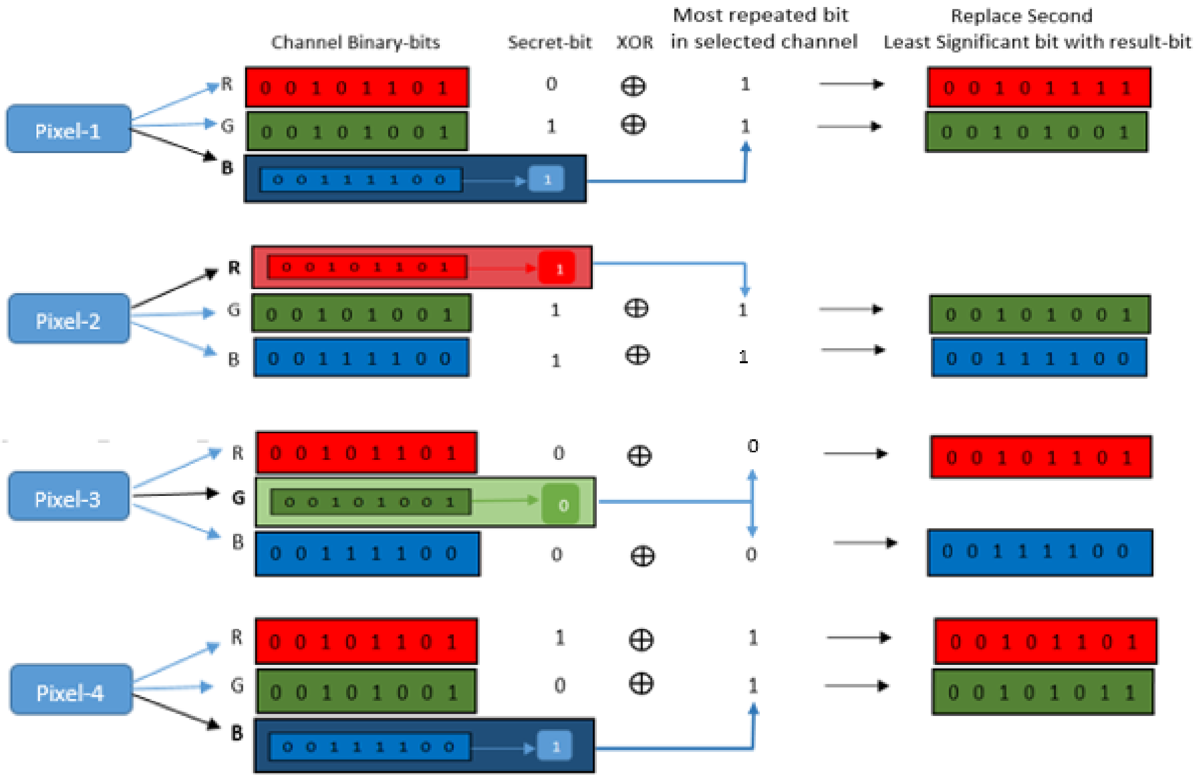


Figure.2 Data embedding process into an image

3.2 Data Extraction Process

In fig.3 explains how data will be retrieve from stegno-image using RGBS technique. In the proposed system use same BRGB pattern for extracting the secret message. In pixel-1 select B-channel most repeated bit then take least significant bits from remaining two channels and extract data using Exclusive-OR [1][3] operation of second least significant bit and selected bit (as shown in fig.3). Similarly using this procedure for extracting the remaining secret data from stegno-image. The resultant secret message is 01110010.

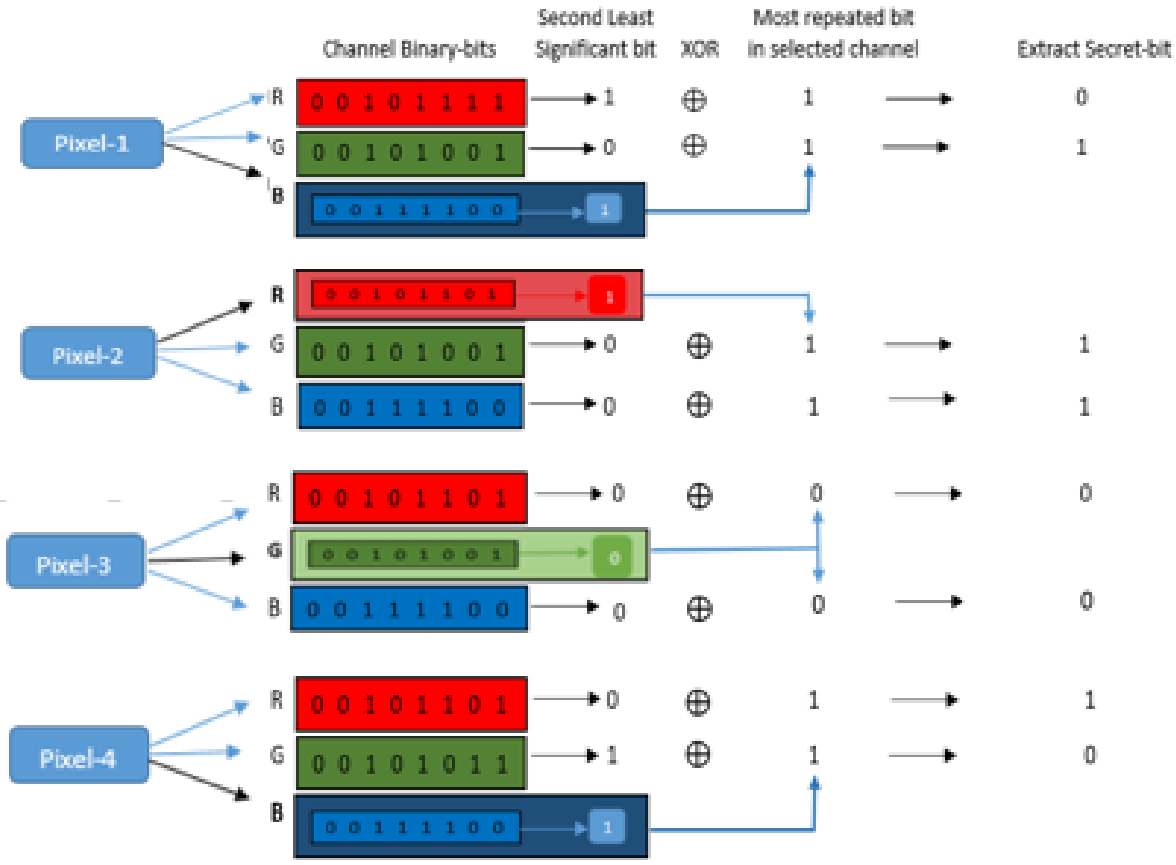


Figure.3 Data extraction process from an stegno-image

3.3 RGBS Algorithm

Step1: Choose Data hiding or Data extraction.

Step2: If Data hiding, go to step3 otherwise go to step13

Step3: Upload an image from browser

Step4: Enter secret message

Step5: Convert secret message into binary form

Step6: Choose most repeated bit from selected channel (BRGB) from each pixel of the image.

Step7: Perform XOR operation [1] [3] of most repeated bit with message bit

Step8: Substitute the result with the second least significant bit of the remaining channels.

Step9: Using above four steps for embedding the data into an image

Step10: Split the image into four blocks [2] based on height and width of the image and also split the message into four blocks

Step11: Each block of the message embedded into each block of the image. This image is called as stegno-image

Step12: For sending the stegno-image to receiver enter the mail address of receiver then click send button

Step13: Upload stegno-image from browser

Step14: Repeat step6, then perform XOR operation [1] of most repeated bit with second least significant bits of two channel in a pixel

Step15: Collect the result as that is the message bit

Step16: Retrieve the resultant message from remaining blocks

4. Performance Measure

4.1 MSE (Mean squared error)

The average squared error is calculated using MSE. This MSE is always considered a risk and MSE a positive function. The greater the MSE, the greater the errors. The degradation of the image increases when the MSE value increases. If the MSE value is zero then the image matching is perfect pixel by pixel.

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[i(i,j) - K(i,j)]2 \qquad (1)$$

Where m is the horizontal pixel count, n is the vertical count of pixels; i(i, j) is a filtered picture at the co-ordinates of i andj; and k(i, j) is the bruised picture at i- and j-coordinates.

4.2 PSNR (Peak signal-to-noise ratio)

In order to calculate values in the form of decibels (dB), PSNR, Peak-Signal-to-Noise-Ratio is used. The relationship between the maximum signal power and the noise is used to find. This ratio is used to measure the quality between the original and the restored image.

$$\text{PSNR}=10\log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right) \qquad (2)$$

Where, MAX=maximum pixel value of an image.

The proposed for RGBS technique was used using 24-bit cover image with height 384,width 256 as shown in table 1 and with the calculation of the MSE and PSNR.

Cover Image	Text size	MSE	PSNR
	60	0.0021393	91.2886
	100	0.0049345	86.1067
	60	0.0025698	90.9578
	100	0.0039686	89.4569

	60	0.0021576	91.1456
	100	0.0048649	87.6974

Table 1: The measures of MSE and PSNR

5. Experimental Results

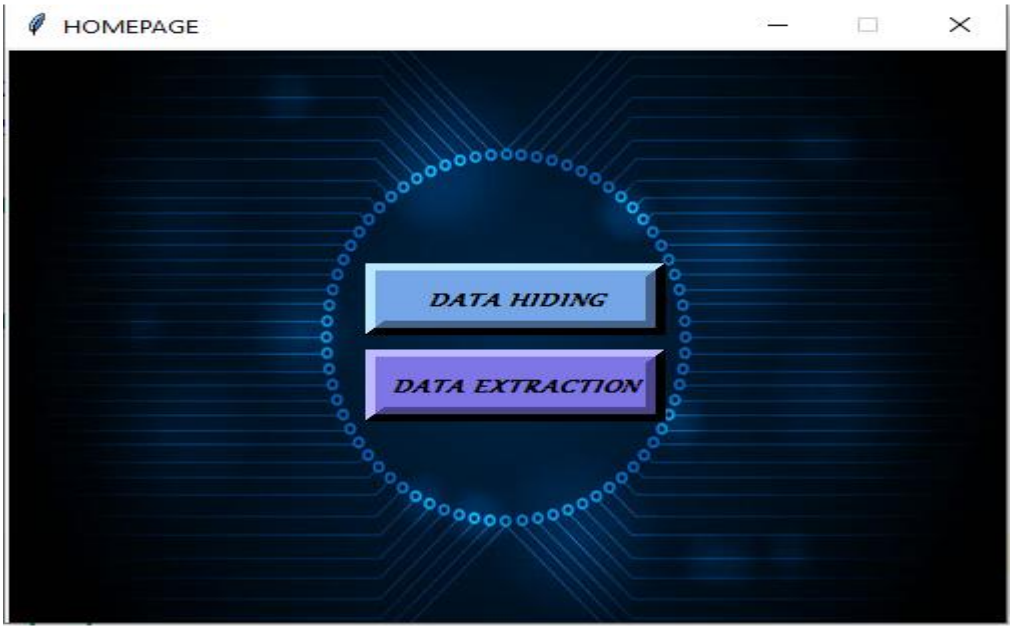
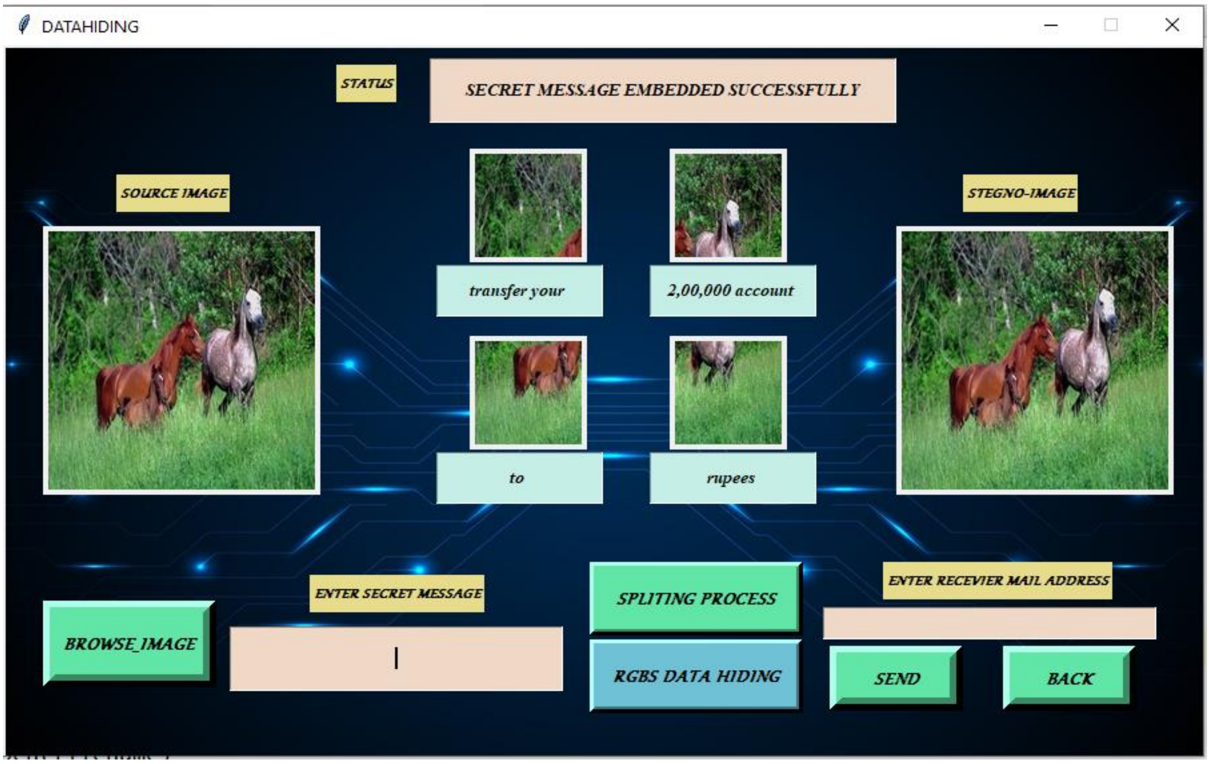


Figure.5 Home page



STATUS: SECRET MESSAGE EMBEDDED SUCCESSFULLY

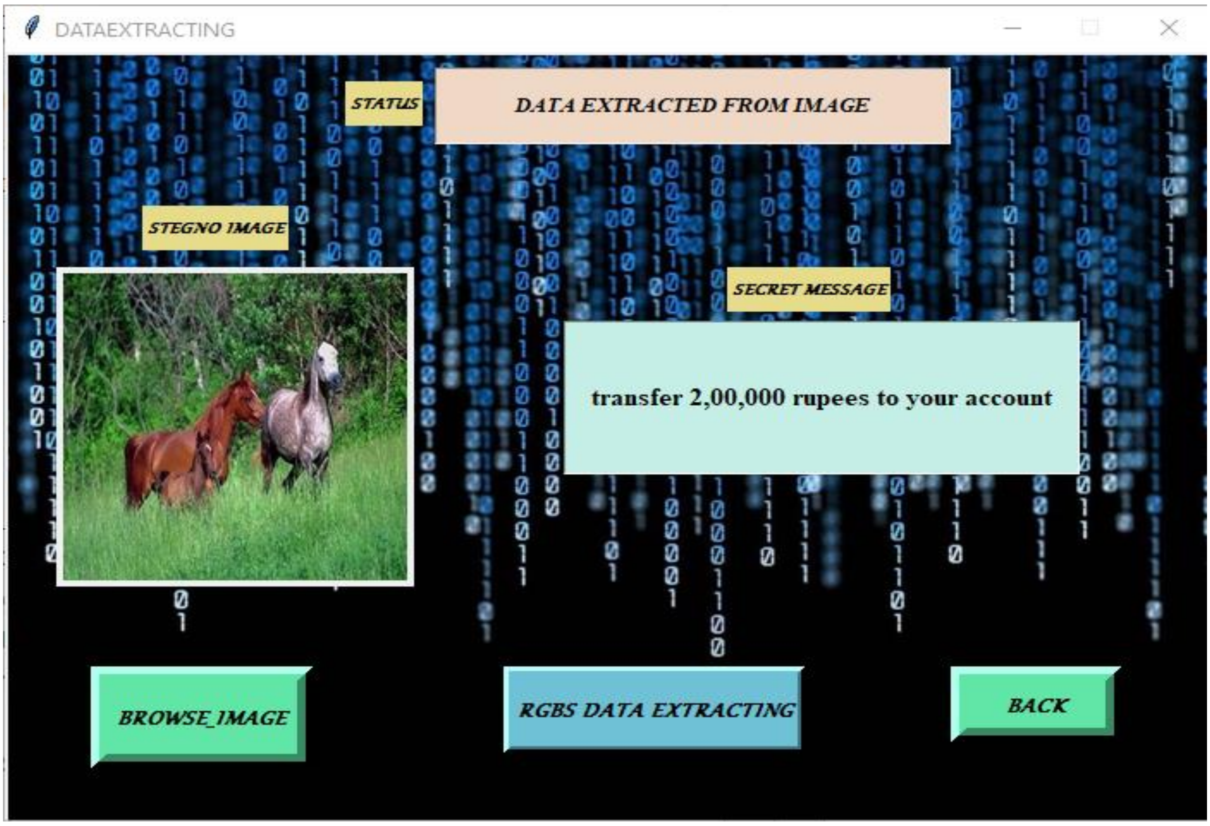
transfer your

2,00,000 account

to

rupees

Figure.6 Data Hiding



DATA EXTRACTED FROM IMAGE

transfer 2,00,000 rupees to your account

Figure.7 Data Extraction

5. Conclusion

Computer-based communications are important and central in modern life to communicate digitally and to transfer and exchange electronic documents between them. In order to secured and protected communication over Internet, the proposed method of image steganography hides the message bit using RGBS technique. Choose most repeated bit from selected channel (BRGB pattern) and take remaining two channels second least significant bits then perform Exclusive-OR operation of second least significant bits with selected bit in other two channels. The differences between the original and the Stegno images are distinguished with the help of PSNR and MSE. These two shows that RGBS approach delivers good performance to embedded the data into an image.

6. References

[1]. U. A. Md. Ehasn Ali, Md. Sohrawordi, Md. Palash Uddin "A Robust and Secured Image Steganography using LSB and Random Bit Substitution" American Journal of Engineering Research (AJER) Volume-8, Issue-2, pp-39-44, 2019

[2]. Rita Rana & Er. Dheerendra Singh "Steganography-Concealing Messages in Images Using LSB Replacement Technique with Pre-Determined Random Pixel and Segmentation of Image" International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 113-116

[3]. Abdul Alif Zakaria , Mehdi Hussain , Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris , Norli Anida Abdullah and Ki-Hyun Jung "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution", 9 September 2018

[4]. Karthikeyan B, Asha S, Poojasree B,"Gray Code Based Data Hiding in an Image using LSB Embedding Technique", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019

[5]. Mohammed A. Saleh," Image Steganography Techniques - A Review Paper", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 9, September 2018

[6]. Fakhar Ullah Mangla , Saira Nokhaiz , Muhammad Ramzan , Ikram Ullah Lali, "A novel steganography technique using grayscale image segmentation", International Journal of Advanced and Applied Sciences, 6(5) 2019, Pages: 84-91

[7]. Rehman Ullah Khan, Muh. InamUiHaq, YahyaKhan, Oon Yin Bee, Shahren Ahmad ZadiAdruce,Mai S. Ishak , Tan Kock Wah, "A Novel Algorithm for Test Steganography ",International Journal of Soft Computing 12(1): 20-25,2017

[8]. Blerim Rexha, Petrit Rama, Bujar Krasniqi and Gentiana Seferi," Efficiency of LSB and PVD Algorithms Used in Steganography Applications", International Journal of Computer Engineering and Information Technology, VOL. 10, NO. 2, February 2018, 20–29

[9]. Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth," Review Paper on Image Steganography", Volume 6, Issue 6, June 2016 ,International Journal of Advanced Research in Computer Science and Software Engineering

[10].Poonam Yadav , Maitreyee Dutta ," A Overview of various Steganographic Domains and its applications", International Journal of Engineering Trends and Technology (IJETT) – Volume 52 Number 3 October 2017

[11].Ramkumar, D. and I. Jacob Raglend," Performance Analysis of Image Security based on Encrypted Hybrid Compression", American Journal of Applied Sciences 11 (7): 1128-1134, 2014

[12].Stuti Goel, Arun Rana, Manpreet Kaur," A DCT-Based Robust Methodology for Image Steganography", IJCST Vol. 4, ISSue 3, July - SepT 2013

[13].Suchitra. B, Priya. M, Raju.J," Image Steganography Based On DCT Algorithm for Data Hiding", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 11, November 2013

[14].Mr. Jayesh Surana, Aniruddh Sonsale, Bhavesh Joshi, Deepesh Sharma, Nilesh Choudhary," Steganography Techniques", 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939

[15].Rosziati Ibrahim and Teoh Suk Kuan," Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application 2 (2011) 102-108

[16].Priyanka Jagota," Image Steagnography: A Review", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 6 June 2015, Page No. 12429-12434

[17].R. Vijayarajeswari, A. Rajivkannan, J. Santhosh," A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN", Circuits and Systems, 2016, 7, 1341-1351

[18].C.P.Sumathi, T.Santanam and G.Umamaheswari," A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013

[19].Priyanka Tirkey, Dipika Kudiyam, Neha Dhruw, Deepshikha Markam, Miss Rumi Ghosh," Image Steganography Using LSB Along With IDEA Algorithm", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 12 Dec. 2016, Page No. 19583-19586

[20].R.Poornima and R.J.Iswarya,"An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013

[21].Bhavana.S and K.L.Sudha,"Text Steganography using LSB Insertion method along with chaos Theory", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.2, April 2012

[22].S. Rajkumar and G. Malathi ,"A Comparative Analysis on Image Quality Assessment for Real Time Satellite Images", Indian Journal of Science and Technology, Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/96766, September 2016