SECURE DATA TRANSFER USING LSB-GREY SCALE ALGORITHM

Ms. D. Gayathri[1], Karumanchi Charan Kumar[2], Kondamudi Sai Pavan Rohith

[1] Assistant Professor, Dept of CSE, SCSVMV (Deemed to be university),Kanchipuram, Tamilnadu, INDIA
[2] Student, Dept of CSE, SCSVMV (Deemed to be university),Kanchipuram, Tamilnadu, INDIA
[3] Student, Dept of CSE, SCSVMV (Deemed to be university),Kanchipuram, Tamilnadu, INDIA

---***---

Abstract - *A huge amount of steganographic programs use the LSB as the method for hiding a message in different bits of colorimages, and grayscale images. It's a belief that changes to the LSBs of colors cant be detected due to noise that is always present in digital images. we introduce a new and very accurate, reliable method that can detect LSB encoding in randomly scattered pixels in both color images and grayscale or color images. The number of groups for the LSB and the "shifted LSB plane", we could easily extract messages as short as 0.03bytes per pixel. The world's interconnectivity became more advent with the use ofthe Internet and new emerging technology. There is a huge volume of personal, commercial, defensive, and governmental information on data sharing infrastructures worldwide. Data confidentiality is becoming a great priority due to intellectual assetsthat can be easily accessed through the internet. Two fundamentally different networks that are present till date are, data networksand synchronous networks composed of switches. The internet is considered a data network. Since the current network ecosystem consists of computerized routers, information can be obtained by special algorithms, such as "Trojan horses," inserted in the routers. The synchronous eco-system that consists of switches does not create any type of buffering in data and hence are not threatened by intruders. This is the reason security is compromised in data networks, such as the internet, and other browsing platforms that connect to the internet.*

Key Words**: *Least Significant Bit Algorithm, Data Embedding, Data Extraction, Data Encoding, Data Extracting.***

1. INTRODUCTION

Hiding information has been an art since centuries which has got its improvement and advancement and has always accompanied information security to make sure the message reaches the desired recipient without dataleak. Over the decades, cryptography and steganography are the two strict methods for securing data using different algorithms, hiding and conveying messages individually. The methods used information in order to encrypt or cover their existence respectively. Cryptography has been an art with science for hiding messages toensure secrecy in data and/or information security but steganography is simply an art of secret writing, Crypto-steganographic method is aimed at combining both the methods for a great information security. The initial purpose of this paper is to build up a new method of hiding secret text messages in a digital image, by introducing cryptography and steganography on a single platform. A new way with a better algorithm is proposed and implemented to reach heights with this.

1.1 LEAST SIGNIFICANT BIT ALGORITHM

LSB made the modern day technology to know its significance and the use of it by its better way of encryption and decryption which cant be decoded by any other algorithm.

When implementing LSB techniques to each byte in a pixel of a 24 bit color/grayscale image, 3 bits of data can be embedded into each pixel.

If the pixel value with LSB of cover image C(i,j) is equal to the bit with message SM of secret message which is to be embedded, C(i,j) remains constant if not set the LSB of C(i,j) to SM.

message embedding Procedure is given below:S(i,j)= C(i,j)-1, if LSB (C(i,j)) = 1 and

SM= 0

S(i,j)= C(i,j)+1, if LSB (C(i,j)) = 0 and SM = 1

S(I,j)= C(i,j), if LSB (C(i,j)) = SM

Where LSB (C(i,j)) represents the LSB of C(i,j) and "SM" is the next bit with a message to be embedded. S(i,j) isgoing to be the stego image.

1.2 DATA EMBEDDING

Step1: Extract the pixels of the cover image.Step2: Extract the characters of the text.

Step3: Extract the characters from the Stego key.

Step4: Choose the initial pixel and take characters of the Stego key and insert them in the initial component ofthe pixel.

Step5: Place some error symbol to show the end of the key. 0 has been used as an error symbol in this algorithm.

Step6: Insert characters of text file in each first component of next pixel s by replacing it. Step7: Repeat step 6 till all the characters have been embedded in the image.

2. DATA EXTRACTION

Step1: Extract the pixels of the stego image.

Step2: Now, start from the initial pixel and extract secret key characters from the initial component of the pixel.else Follow

Step3: Upto terminating symbol, otherwise follow step 4.

Step4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.

Step5: If the key is correct, then go to the next pixel and extract secret message characters from the firstcomponent of next pixels. Initialize Step 5 till up to terminating symbol 0 , else follow step 6.

Step6: Extract secret message.

2. PROCESS

This project starts with an opening page which gives two options to the user to choose either he wants toencode the image or decode the encoded one.

Once the user selects the encoding option then he will be prompted to the page which asks the image that has tobe encoded and secret key, and the message to be embedded which has to be entered by the user. once the userclicks the encode option by entering the required data it starts encoding the data in the image by selecting the bits according to the algorithm.

Once after the encoding is done then the user needs to save the image by clicking the save button in the UI. The saved picture will be found only in one place, a particular place in the device. In particular we have set the path to the downloads which contains the image renamed as ENCODED.PNG without changing any size of the image.

To DECODE the image user has to navigate into the downloads folder in the root of the device and select theimage which was shared.

After selecting the image the user will be prompted to enter the secret key which was set by the ENCODER. If the key was correct then the image will be extracted and then the data will be correctly displayed.

3. OUTPUTS

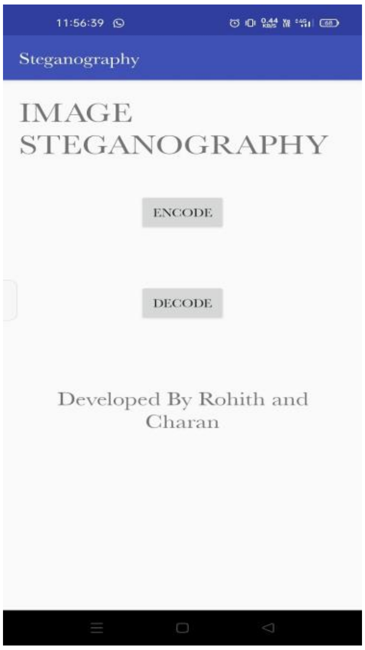
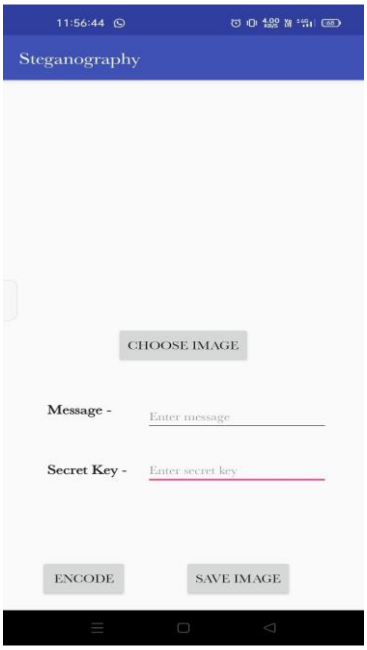
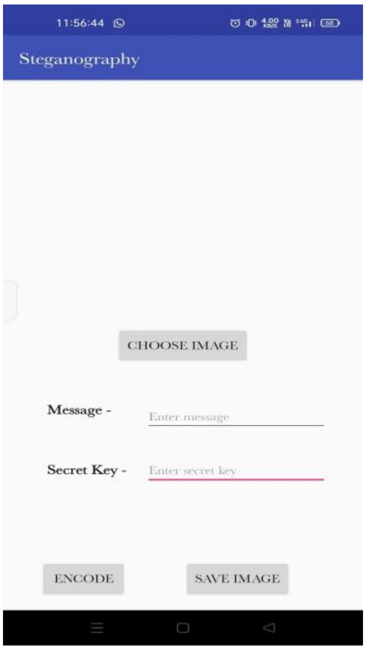
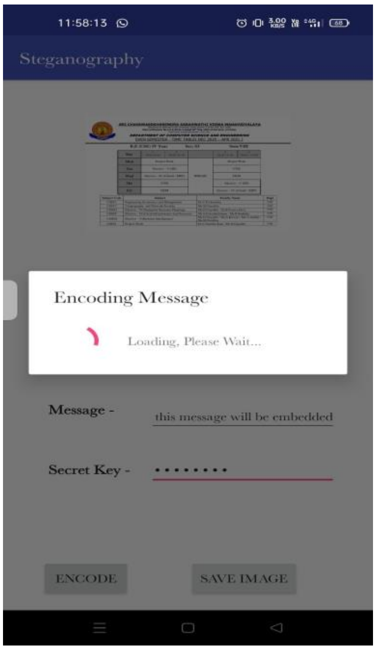


IMAGE STEGANOGRAPHY

Developed By Rohith and Charan





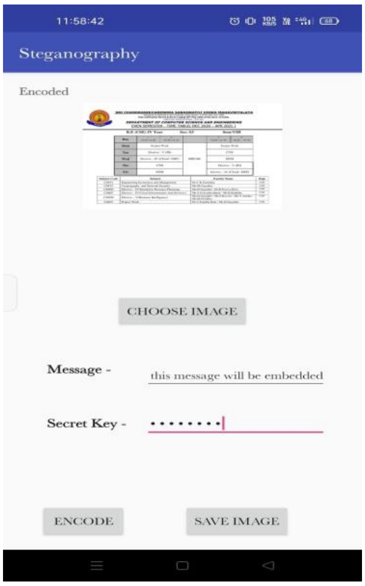


Encoding Message

Loading, Please Wait...

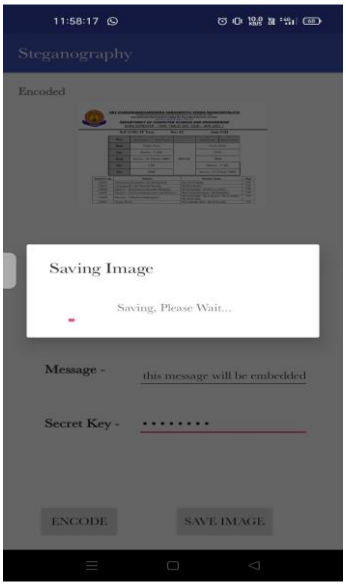
Message - this message will be embedded

Secret Key - ••••••••



Message - this message will be embedded

Secret Key - ••••••••

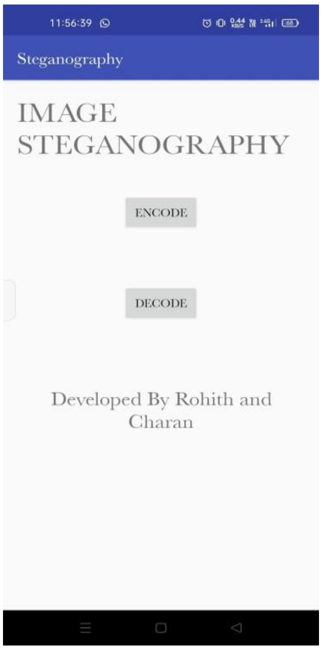


Saving Image

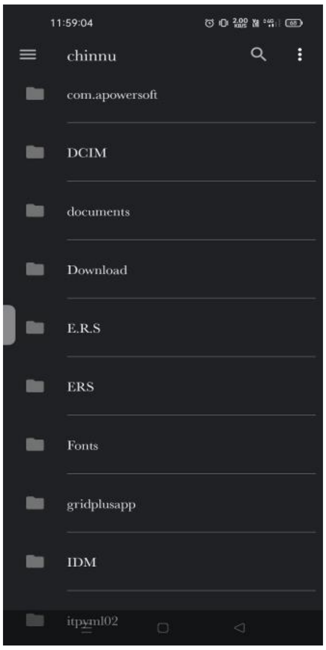
Saving, Please Wait...

Message - this message will be embedded

Secret Key - ••••••••



Developed By Rohith and Charan



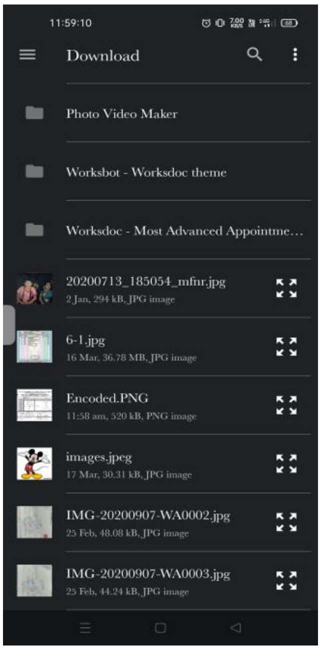


Photo Video Maker

Worksbot - Worksdoc theme

Worksdoc - Most Advanced Appointme…

20200713_185054_mfnr.jpg
2 Jan, 294 kB, JPG image

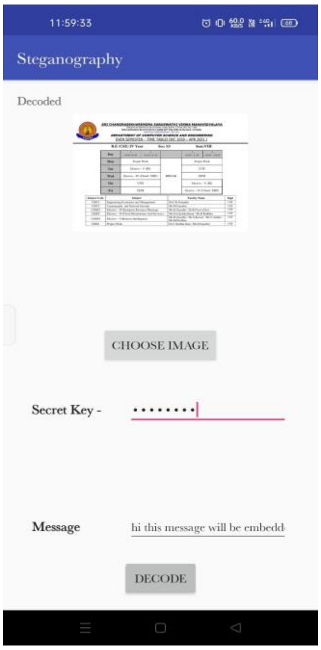
6-1.jpg
16 Mar, 36.78 MB, JPG image

Encoded.PNG
11:58 am, 520 kB, PNG image

images.jpeg
17 Mar, 30.31 kB, JPG image

IMG-20200907-WA0002.jpg
25 Feb, 48.08 kB, JPG image

IMG-20200907-WA0003.jpg
25 Feb, 44.24 kB, JPG image



Secret Key - ••••••••

Message hi this message will be embedd

4. CONCLUSION

By using the LSB algorithm we can send messages without any security issues.It is possible to send text messages from any image using LSB algorithm. It can be used to send data on network secure. In our project we have successfully done image Steganography, where we hide data inside the carrier image using LSB algorithm at receiver side. After receiving the stego image at the receiver side we can also get the data. the image Steganography can be done in the grayscale image and also in colour image. A software implementation of a Steganography scheme provides the benefits of flexibility, speed of implementation, and lower cost over time.

REFERENCES

[1]. Nolkha, Avneesh, Sunil Kumar, and V. S. Dhaka. "Image Steganography Using LSB Substitution: A Comparative Analysis on Different Color Models." In Smart Systems and IoT: Innovations in Computing, pp. 711-718. Springer, Singapore, 2020.

[2]. Vyas, Archana O., and Sanjay V. Dudul. "A Novel Approach of Object Oriented Image Steganography UsingLSB." In ICDS MLA 2019, pp. 144-151. Springer, Singapore, 2020.

[3]. ALabaichi, Ashwak, Maisa'A. Abid Ali K. Al-Dabbas, and Adnan Salih. "Image steganography using least significant bit and secret map techniques." International journal of electrical & computer engineering (2088-8708) 10, no. 1 (2020).

BIOGRAPHIES

	Ms. D. Gayathri Assistant Professor at SCSVMV UniversityCSE Department
	Kondamudi Sai Pavan Rohith Student at SCSVMV University CSE Department 11179A122
	Karumanchi charan kumar Student at SCSVMV UniversityCSE department 11179A113