iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37322

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Secure Data Transfer Using Image Steganography

Nisha Manral[1], Deepali Sharma[2]
[1, 2]*Department of Information Technology*

Abstract: ***Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.***

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information . Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated . The strength of steganography can thus be amplified by combining it with cryptography.

II. DIFFERENT KINDS OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [11]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [5]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding

A. Text
B. Image
C. Audio
D. Protocol
E.

III. METHODOLOGY

A. Least Significant Bit

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.For example a grid for 3 pixels of a 24-bit image can be as follows:

©IJRASET: All Rights are Reserved

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size . Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.
In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. This approach is very easy to detect . A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed.
Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key.
In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image. Nowadays, BMP images of 800 × 600 pixels are not often used on the Internet and might arouse suspicion . For this reason, LSB steganography has also been developed for use with other image file formats.

IV. PROPOSED ALGORITHM

This section presents a step-by-step solution to the problem described above. The encryption algorithm at the Sender's end and decryption algorithm at the Receiver's end are detailed below.

A. Encryption Algorithm

Step 1: Select the text file where the original message has been written.
Step 2: Encrypt the content of the text file using the RSA algorithm with the public key of the receiver.
Step 3: Select an appropriate cover image (.jpeg format).
Step 4: Read the header and footer of the selected image in an array buffer.
Step 5: Add the encrypted data at the end of image footer.
Step 6: Sender and receiver are connected to the network.
Step 7: Sender provides the receiver's IP address and then send the Stego-image if the IP address is valid.

B. Decryption Algorithm

Step 1: Receive the Stego-image.
Step 2: Extract the encrypted message from the end of the stego image by reading the image footer.
Step 3: Generate the private key and decrypt the extracted message and then create a text file.
Step 4: Save the text file at the desired location.

©IJRASET: All Rights are Reserved

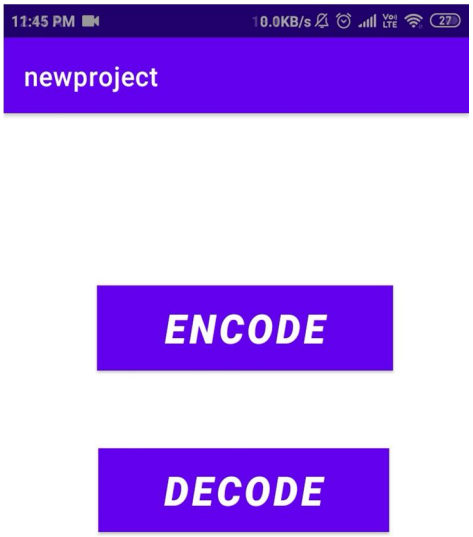
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

V. EXPERIMENTAL RESULTS

1) *Steps 1:* How our app UI look



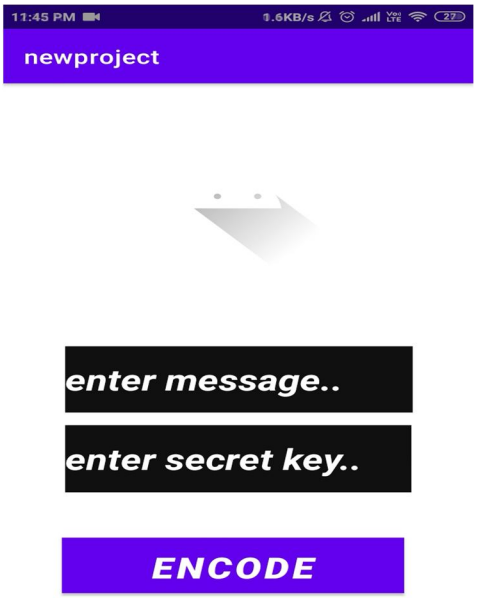
2) *Steps 2:* Our Home consist of an button which redirect us on encode & decode page.



©IJRASET: All Rights are Reserved

3) *Steps 3:* Now firstly we need to encode our text or secret message.

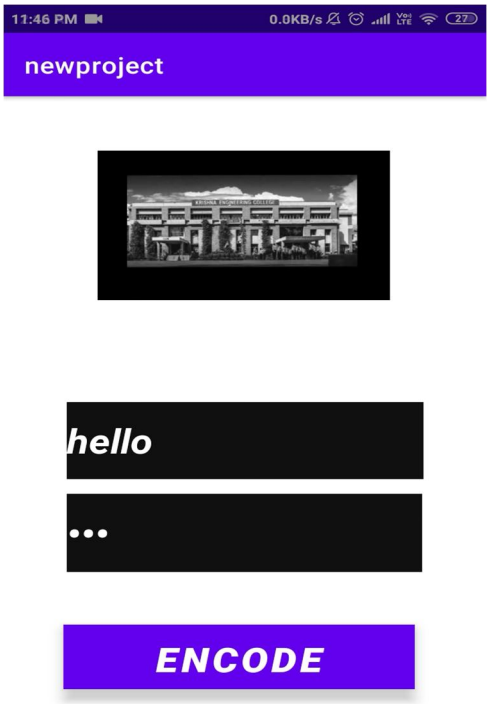
a) Enter your message in the Textfield.



b) Enter your secret key in the password field.

c) Select the image from the gallery we need to encode with .

d) Click on the encode button.



e) Again the page redirect you into Home page.

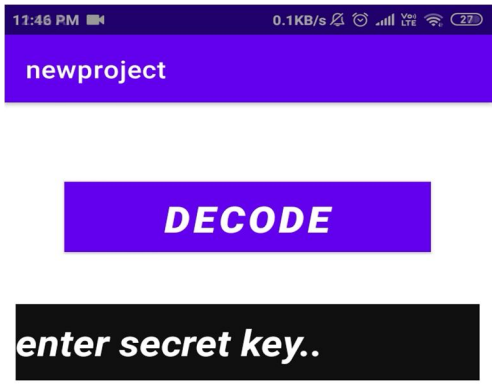
f) It means that our selected image get saved in our phone sd-card memory.

g) You can check it by opening file explorer in your smart phone and find that one new copy of the image is found in your sd-card.

©IJRASET: All Rights are Reserved

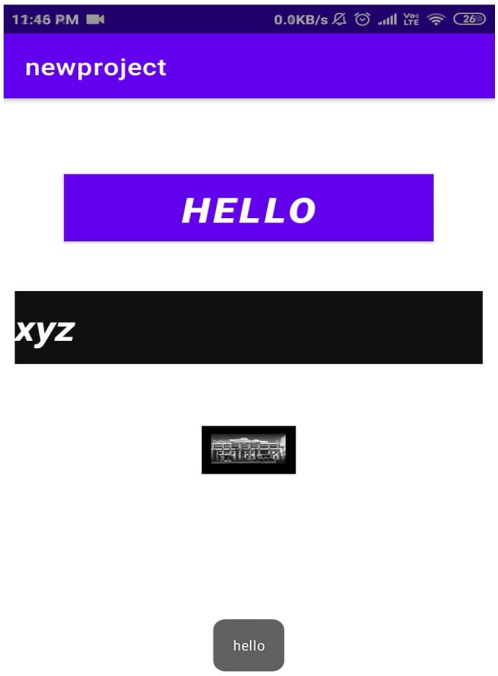
4) Steps 4

a) Click on the steganography button again and this time click on the decode button.



b) Enter your secret key which you use for encoding the text.

c) Select the encoded image from the image view button.



©IJRASET: All Rights are Reserved

VI. CONCLUSION

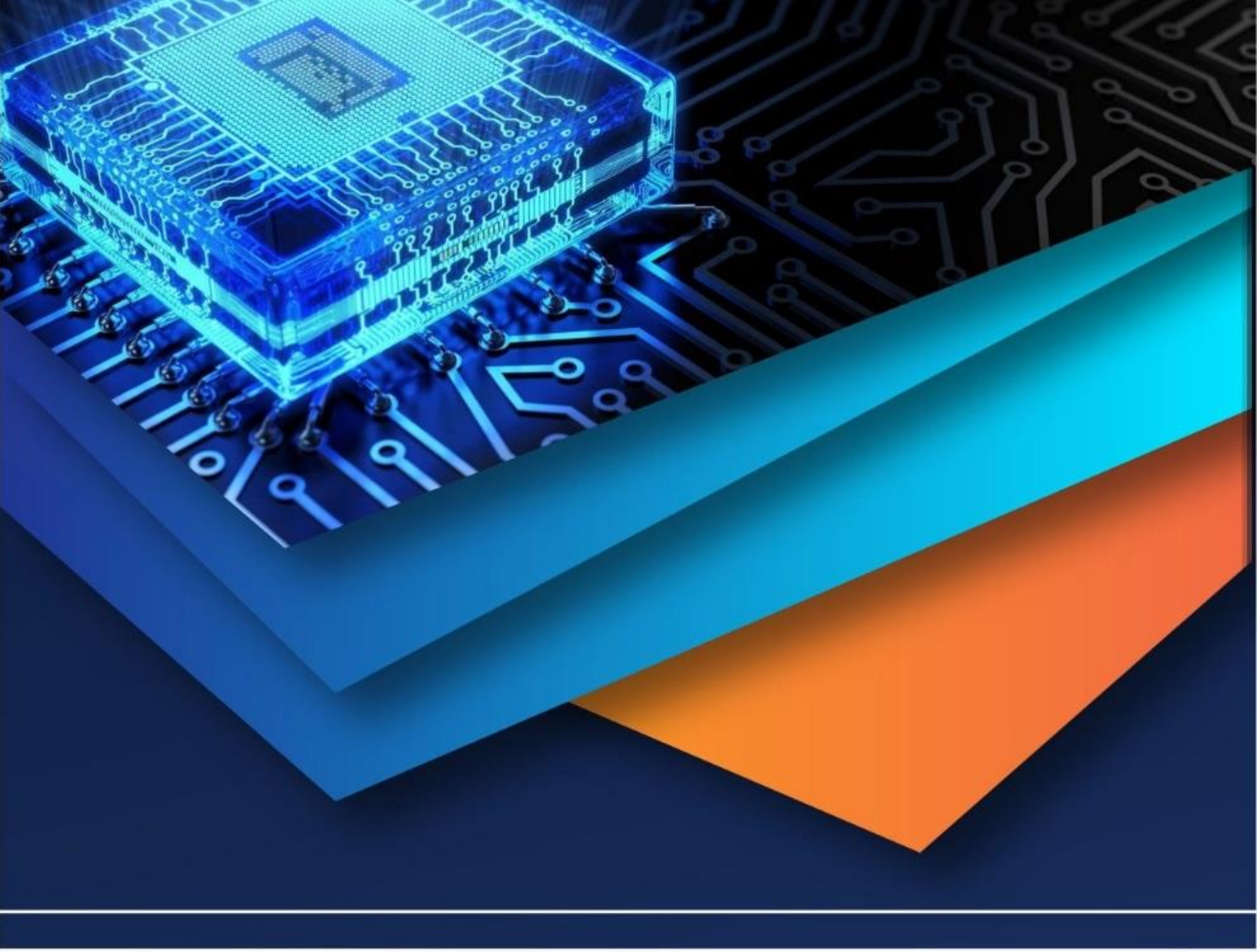
Interest in the use of steganography in our current digital age can be attributed to both the desire of individuals to hide communication through a medium rife with potential listeners, or in the case of digital watermarking, the absolute necessity of maintaining control over one's ownership and the integrity of data as it passes through this medium. This increased interest is evidenced in the sheer number of available tools to provide easy steganographic techniques to the end user, as well as the proliferation of research and press on the topic.

The intent of this presentation was to cover some of the more common methods of data hiding using widespread file formats and easily available tools as an introduction to the primary concepts of steganography. These discussions should serve as a starting point to the exploration of more complex steganographic techniques involving, for example, the use of network packets and unused hard disk space as cover medium, or the more complex methodologies used on our standard image and audio files.

REFERENCES

[1] https://projectideas.co.in/image-steganography-with-3-way-encryption-dotnet/
[2] Introduction to image Steganography youtube videos.
[3] Implementation of LSB Steganography and its Evaluation for Various File Formats.Int.J.Advanced Networking and Application 868.
[4] Cryptography and network security by William Stallings 3rd edition.
[5] Obaida Mohammad Awad Al-Hazaimeh, (2013) "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.
[6] Katzenbeisser, S. and Petitcolas, F.A.P. 2000, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.
[7] Xinpeng Zhang and Shuozhong Wang, (2005), "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.
[8] Jarno Mielikainen, (2006), "LSB Matching Revisited", IEEE signal processing letters, Vol. 13, No. 5.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)