International Journal of Multidisciplinary Research And Studies

Available online at
https://ijmras.com/index.php/ijmras/article/view/630

Page no.- 13/13

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND STUDIES
ISSN: 2640 7272
Volume:06; Issue:09 (2023)
Doi: 10.33826/ijmras/v06i09.3

Hiding Random text using Steganography

KOLAPO RIDWAN OLAYINKA

Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.

**Corresponding Email: ashiwaju93@gmail.com*

Abstract

The introduction of steganography has brought a lot of improvement to information security. Security issues is taken into account a significant concern which is why management systems offices still opt to follow the normal way of addressing record keeping. This study aims to ensure data security using Steganography.

The method used in for the steganography technique in this study is the RGB techniques, as every pixel is considered to be a combination of RGB. The entire message to be hidden is split-ed into equal 2-bit values and embedded in the red pixelvalue of the image. This is passed until the end of the image. The message length is also embedded in the image by the software solution designed. The same software must be used to receive, decode the image, and extract the message.

The result of this study is presented as a software solution and the images used for information hiding are not limited to any type of image as images from different source and types can be used for hiding text, also the image used for steganography resulted to having higher dimension size as this compensate for the addition security level.

In conclusion, steganography system is aimed to protect the confidentiality of data and present it as an image as this will not easily attract security threat.

Keywords: Steganography, Plaintext, Ciphertext.

1. INTRODUCTION

Cryptographic and Steganography techniques play an important role within the fieldof information security. The simplest thanks to secure a message is cryptography and steganography. The term Steganography comprises two ancient Greek words, Steganoand Graphy and both words refere to “Cover Writing”. Steganography was first used centuries ago, instance of the usage of steganography was how steganography was used to send a secret message by inking secret messages on his slave’s skull, who travelled only after the hair had grown to cover the tattoo. [1]

Steganography is another means of securing message during data communication. Although both cryptography and steganography shares the same objectives, the approaches vary. In contrast with cryptography, steganography retains its original databy hiding it in other media. Whereas cryptography transform the original data into cipher-text. The drawback of cryptography is the existence of the original data, irrespective of whether the original data are subjected to encryption. Therefore, steganography methods offer a supplementary security layer for the message while communicating the data. Robustness in steganography are cryptography are viewed differently. When an attacker is able to access the actual data, then the cryptographic system is no longer secure. in contrast, if the attacker has authority over the secret data in the steganography system, the system is considered to no longer be secure. [2]

Security, imperceptibility and capacity are the three attributes of steganography required to conceal secret data. In addition to robustness, these attributes are the most influential factors that determine the efficacy of a steganography setup. According to its use, there are certain specific requirements for managing a number of steganographic designs. Steganography and watermarking have these attributes for data embedding. However, a common tradeoff is between the size of secret data and the quality of the stego files. Suppose a large quantity of secret data is to be embedded.In that case, modifying the stego files is harder because the imperceptibility is more difficult to achieve because of a possibility of distortion. [2]

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

2. RELATED WORKS

[3] review different steganography techniques that can be used in securing digital assets on the internet against active and passive attacks of eavesdroppers. The concernof the study is to open up research channel to improve the techniques of secure and reliable communication protecting intellectual property rights and message security. The study has taken into consideration techniques that when being implemented it does not alter the quality of the image used for hiding the text as this is a major shortcoming of some of the steganography techniques.

[4]Implemented a mathematical setup using double layer security technique. The study implemented Affine and Ceaser technique to secure electronic health records to help enhance effectiveness and to strengthen security of electronic health record system. The cryptographic technique used in this study can be combined with a steganography technique as it is stated that it will increase computational time for an attack to be made successful.

[5] Proposed an improved image steganography framework for neural style transfer based on Y channel information and a novel structure loss, composed of an encoder, astyle transfer network and a decoder. This study solves the problem associated with artistic design as Neural style transfer has accelerated the tampering, synthesis and dissemination of a large number of digital image resources without permission which then leads to a large number of copyright dispute. This proposed framework allows the encoder to embed the gray-scale secret image into Y channel of the cover image and then generate a steganographic image while the decoder can directly extract the secret image from a stylized stego image output by the style transfer network. This proposed framework used the PSNR metric to measure its effectiveness as it proves tobe effective to protecting secret information like copyright.

[6] propose a new form of steganography, on-line hiding of information on the output screens of the instrument. The method used in this study can be used for announcing asecret message in public place which can be extended to other means such as electronic advertising board around sports stadium, railway station or airport. This method of steganography is very similar to image steganography and video steganography. The proposed form has some metric attributes on its checklist which include; the integrity of the hidden information did not change after embedding; the

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

[7] stego object remains almost unchanged to naked eye; the accuracy of the extracted data is intact.

[8] Developed a software solution for hiding data and information in digital image format, as it is mostly in demand on the internet. This paper mainly focuses to present Steganography overview, its demand, advantages and the techniques involved in it. In this paper there is also an attempt to identify which Steganography techniques are more useful and what are their requirements and also it shows which application will have more compatibility with which steganography technique.

3. METHODOLOGY

3.1 Pseudocodes for Hiding the text into a selected image;

Step 1: Extract the pixels of the image and store it in an array.

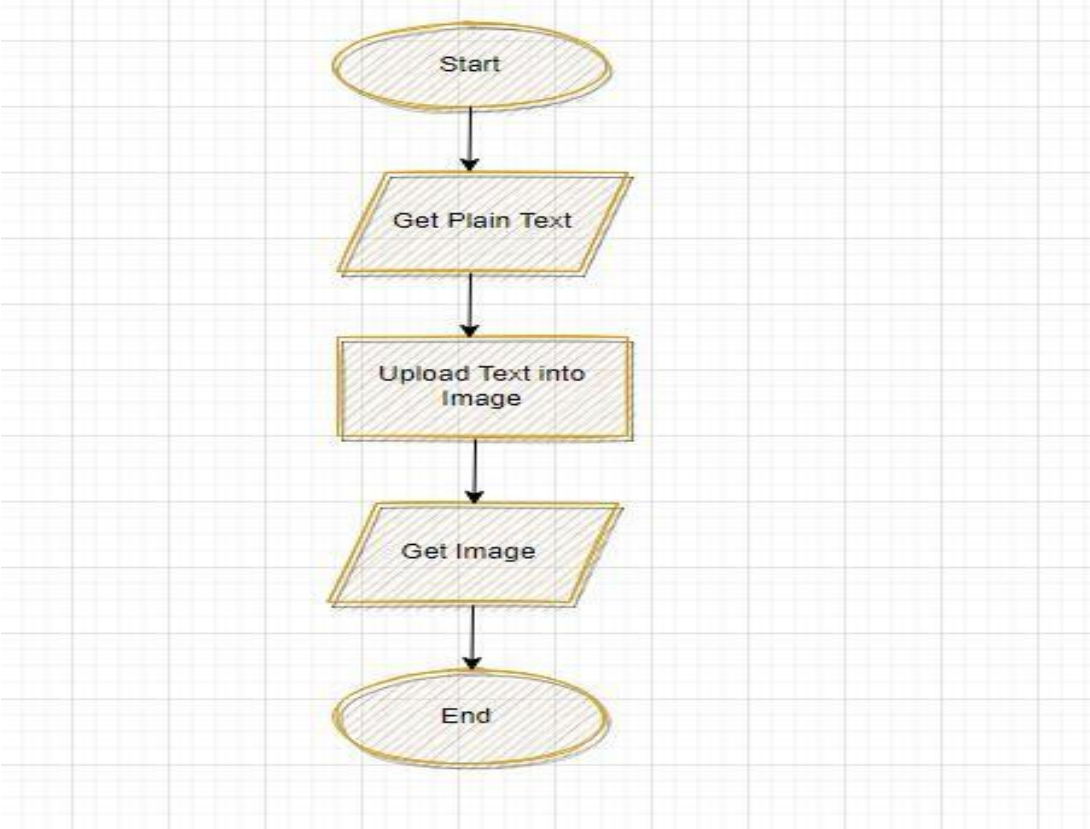
Step 2: Convert text box text into binary bits and store them in an array.

Step 3: Loop through all the pixels of the image to check if the Red value <= 16.

Step 4: If the value of Red in RGB is <=16 create a new value of R as “01” +Two bitsof the Message Array + Old Red Value and rewrite the pixel value.

Step 5: Repeat step 3 till all the bits of the character array have been embedded.Step 6: Write the new Image.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*



3.2 Pseudocodes for Extracting the Text from the image;

Step 1: Extract the pixels of the stego image and store it in an array.

Step 2: Loop through all the pixels of the image to check if the first two bits of Redvalue = “01”.

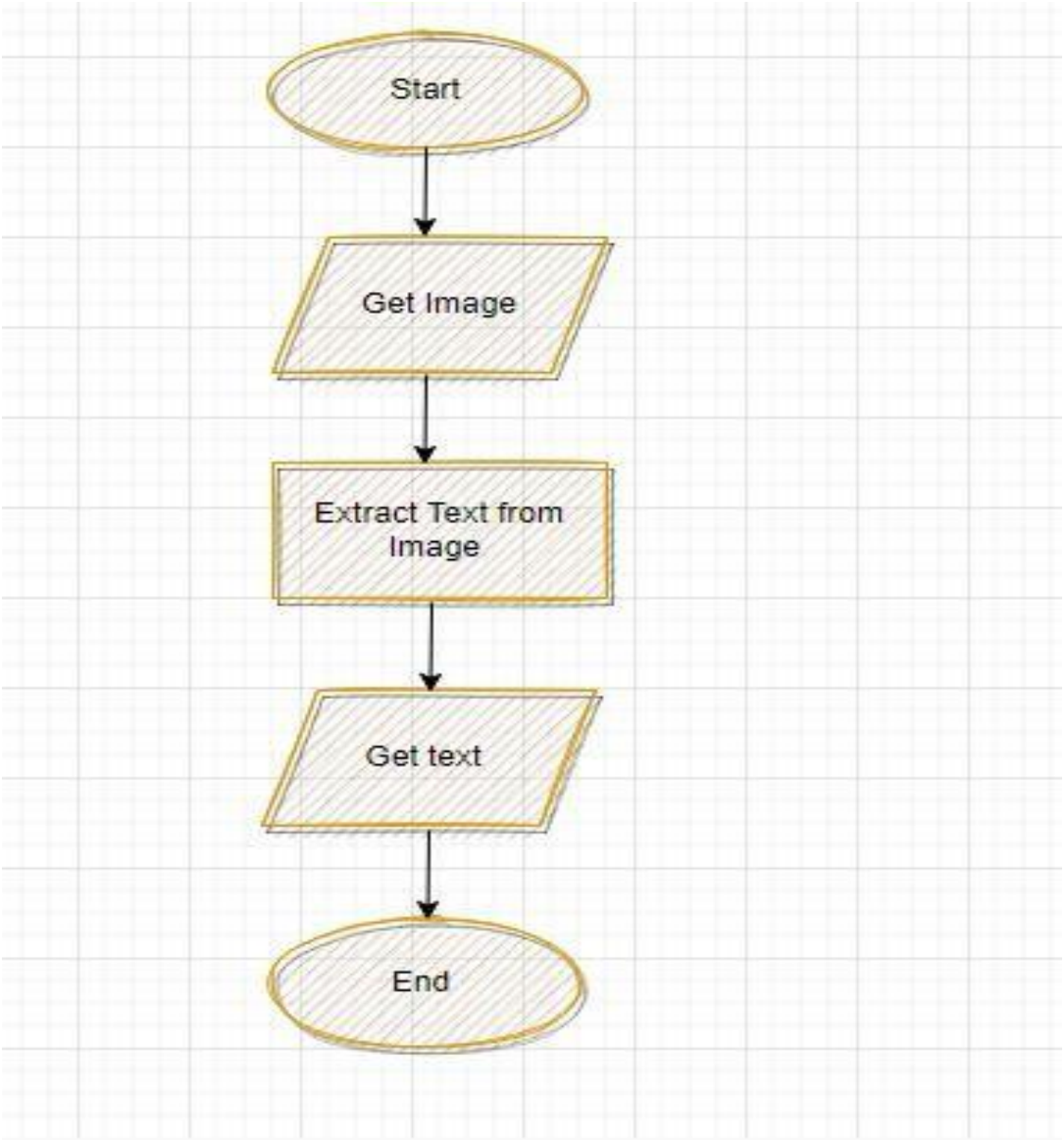
Step 3: If step 2 is true then extract the 3rd and 4th bit of the red and store it in a bit character array and rewrite the Red pixel value with the last four bits.

Step 4: Repeat step 2 till all the bits of the character array have been retrieved.

Step 5: Write the new Image

Step 6: Combine 8 bits of the character bit array retrieved and extract the text.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*



4. RESULTS AND DISCUSSION

The figure below is the interface for the steganography phase of this study. This interface provides the user with the flexibility to either encode certain text into an image or the extract the text out of the image using the encode button as shown in the figure below.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

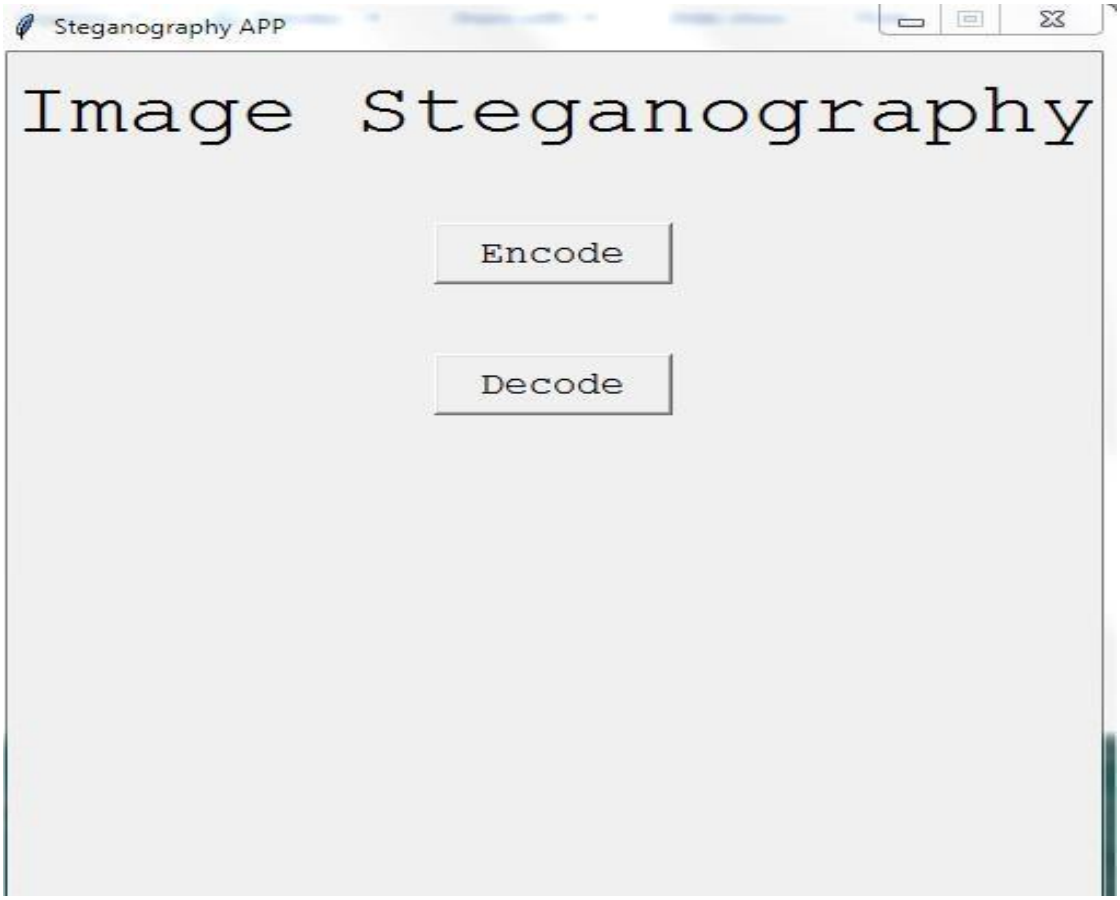


Figure 4.1 Interface showing the Steganography Page

The interface below allows the user to select image to be used for hiding of text, oneof the most interesting and flexible part of this phase is that it allows user to select anyimage from the user's computing device as this design does not limit the user to just certain image to be used for hiding text into the image.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

Figure 4.2 Interface showing the "SELECT IMAGE" phase for the steganography Technique

The figure below shows what the interface looks like after an image has been selectedfrom the list of images on the user's device. The image presented below is the image that will hide the text in this study.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

Figure 4.3 Interface Showing the "SELECTED IMAGE" where text is to hidden

The figure below shows two things, the first activity shown in the figure below is the text to be hidden in the image, the second activity is the success message shown to indicate that the text has been successfully encoded into the image. Without the success message been presented there is no way the user can confirm the operation of hiding the text into an image was successfully carried out.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

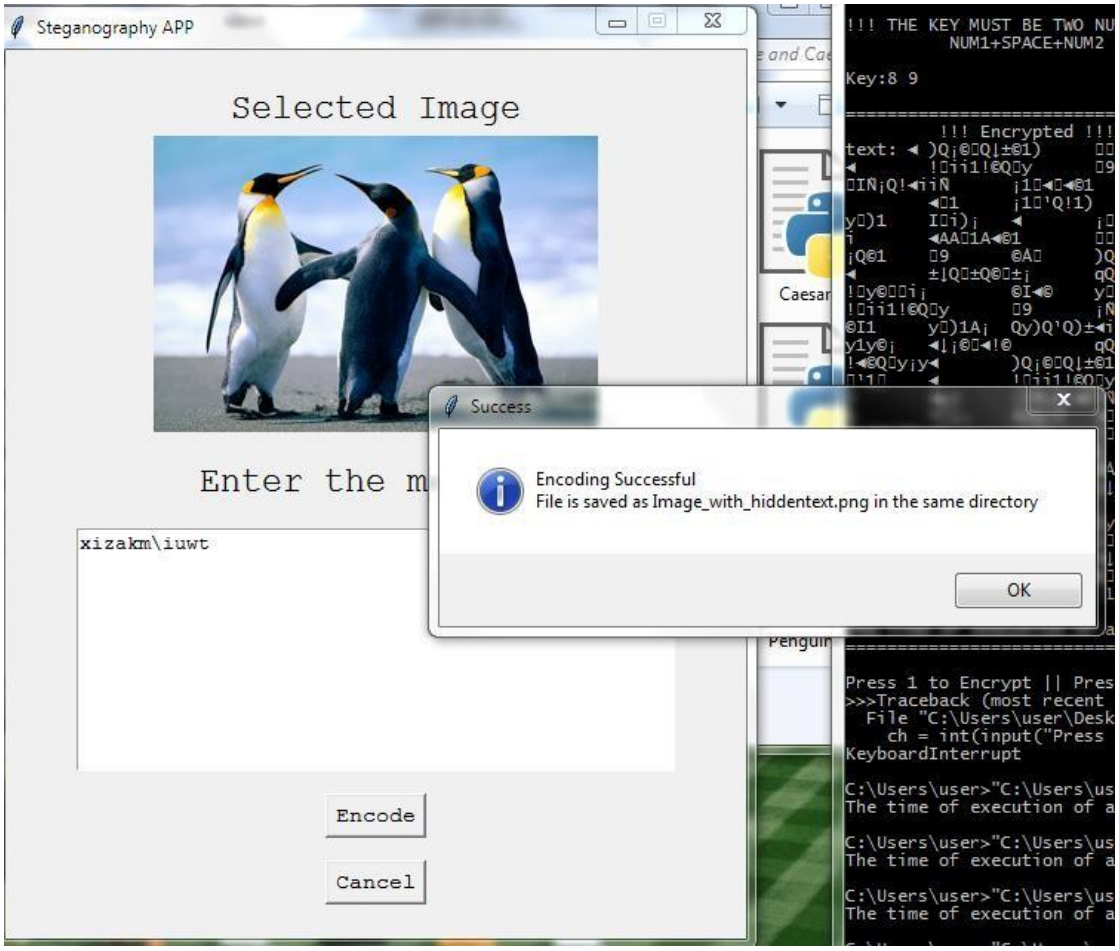


Figure 4.4 Interface showing the Encoding Phase with the Success message

The table below shows the Word Length which is the number of characters of the Cipher-text embedded in the image, the time analysis taken to hide this text into the image which is captured as the encoding time, the time it takes to extract this textback from the image, which is recorded as the decoding time, the Dimension of the image before hiding the text into the image and the size of the image on disk before hiding the text into the image.

Word Length	Encoding Time (ms)	DecodingTime (ms)	Image Dimension Before encoding	Image Size Before encoding(kb)

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

11	30.15	16.62	1024*768	760
687	52.95	19.19	1024*768	760
1374	46.42	14.36	1024*768	760

Table 4.1 Showing Word Length, Encoding Time, Decoding Time and Dimension of the Steganography Image Before Encoding

The table below shows the Word Length which is the number of characters of the Cipher-text embedded in the image, the time it takes to hide this text into the image which is captured as the encoding time, the time it takes to extract this text back from the image, which is recorded as the decoding time, the Dimension of the image after hiding the text into the image and the size of the image on disk after hiding the text into the image.

Word Length	Encoding Time (ms)	Decoding Time (ms)	Image Dimension After encoding	Image Size After encoding(mb)
11	30.15	16.62	1024*768	1.24
687	52.95	19.19	1024*768	1.24
1374	46.42	14.36	1024*768	1.24

Table 4.2 Showing Word Length, Encoding Time, Decoding Time and Dimension of the Steganography Image After Encoding

5. CONCLUSION

The steganograpgy technique used in this study can be applied in watermarking, fingerprinting, detection of unauthorized or illegally copied material.

This paper describes a technique to successfully embed text into image, as every pixelis

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

considered to be a combination of RGB. The entire message to be hidden is split-ed

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*

into equal 2-bit values and embedded in the red pixel value of the image. This ispassed until the end of the image.

Future works can be done in embedding the text in other media formats such as Audioand Videos as Image was used in this study. However, this research work and software solution provides a good starting point for anyone interested in steganography.

REFERENCES

1. Zinah Talaat Rashid AL-Windawi. "Security Enhancement of Image Steganography Using Embedded Integrity Features". Master in Computer Science,Middle East University. May, 2017.
2. American Journal of Engineering Research (AJER) e-ISSN : 2320- 0847 p-ISSN :2320-0936 Volume-02, Issue-11, pp-122-128 www.ajer.org Steganography: A Review of Information Security Research and Development in Muslim World YunuraAzuraYunus, SalwaAbRahman, Jamaludin Ibrahim Kuliyyah of Information and Communication Technology International Islamic University Malaysia.
3. Dipti Kumari, Pradeep Kumar, Dr. Meena Arora, "A Review: Hiding Text in ImageUsing different Steganography Approaches. International Journal of Research and Scientific Innovation Volume IV, Issue VS, May 2017. ISSN 2321-2705. Pg 69-73.
4. Kolapo Ridwan Olayinka and Sakpere Wilson. "Towards Securing Electronic Health Records Using Ceasar and Affine Cryptographic Techniques" International Journal for Research Trends and Innovation, Volume 7, Issue 12, 2022. ISSN: 2456-3315. Pg 46-50.
5. Wenjie Lin, Xueke Zhu, Wujian Ye, Chin-Chen Chang, Yijun Liu and ChengminLiu. "An Improved Image SteganographyFramework Based on Y Channel Information for Neural Style Transfer". IEEE Volume 2022, Article ID 2641615.
6. Shashikala Channalli, Ajay Jadhav. "Steganography An Art of Hiding Data". International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141
7. Ritu Sindhu and Pragati Singh. "Information Hiding using Steganography". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April, 2020. Pg 1549-1554.

KOLAPO RIDWAN OLAYINKA*, *Computer Science Department, Lead City University, Ibadan, Oyo State, Nigeria.*