IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

Data Hiding using Image Steganography

Shinde Anushri Sudhakar, Konde Ruchita Bharat, Shinde Sakshi Vishwas, Prof Kumbhoje. M. R
Shri Shiv Chhatrapati College, Junnar, Maharashtra, India

Abstract: *Image Steganography is the artwork of concealing mystery data within the image such that the hacker will now no longer be capable of discover the records within inside the stego images. This is a useful approach to secure our sensitive information. Security has continually been a main difficulty from last many years to existing days. The topic of interest to researchers has long been the development of secure technologies for sending data to anyone other than the recipient without revealing it. Therefore, from nowadays, researchers have evolved many strategies to meet the steady transfer of information and steganography is one in all them. In this paper, we work on two techniques for hiding information in the image. First, we do analysis on LSB for storing information bit. As the technique is known to all, the attacker will be able to easily reveal the information, this makes image steganography unsecured. Secondly, R-Color Channel encoding with RSA set of rules for offering extra protection to information in addition to our information hiding approach. The proposed approach makes use of a red color channel for hiding information bits and the following bits for RGB pixel values of the original image. This paper present the performance analysis of two most popular algorithms, LSB and RSA along with image steganography*

Keywords: Steganography, stego image, LSB, R-Color channel, RSA, cipher text

I. INTRODUCTION

For data exchange, social media has now become an extremely popular technique. Transferring data securely through social media is a big challenge. One of the simplest methods to ensure protection is through encryption. The secret message, on the other hand, is altered and rendered doubtful, so that the attacker is less likely to suspect the presence of confidential information. Capacity, robustness, and invisibility are important parameters in information security. [1, 2].

Steganography comes from the Greek word called stegano. Stegano means to cover and graphy means writing, define it as writing that has been covered. Image steganography is the secret concealment of information in images. The civilization of covert communication is steganography. It's the process of embedding access facts in a manner that hides the facts current state of being. Cover text, cover image, and cover audio message are terms used todescribe the existing files. It is known to that as stego medium following cover-medium with the embedded data within it. To prevent observation or extraction of the embedded data, an encoded key has been employed to hide the encoding process. In image steganography, the data is hidden within the image in such a way that it does not make greater changes in the appearance of the image.

Cryptography is the art of maintaining security by encoding messages in such a way that they are no longer readable. The plain text structure is transformed into cypher text, rendering it useless and unreadable unless the decryption key is accessible. Essentially, they can communicate information between people in such a way that a third party cannot interpret it. It uses public key for encryption and another private key for decryption. In the process sender and receiver both were known with public key but not with private key. There is a key features for secure our data between sender and receiver. The basic sequence of scenario in Fig.1.

There are two options for achieving this objective. One is cryptography, which uses a private key and a public key to send information in the form of Ciphertext. The attacker, on the other hand, cannot readily identify the presence of certainsecret information by viewing it. Steganography is a different approach. Steganography renders communication incomprehensible to the illegitimate receiver [4].

DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

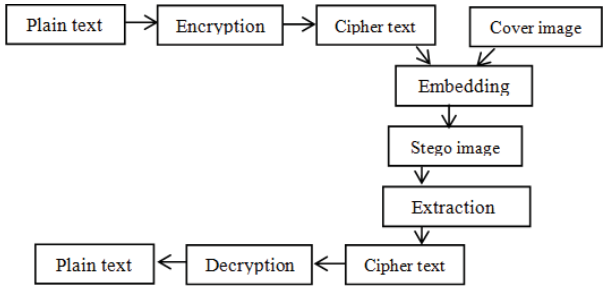


Fig. 1. An Overview of Cryptography and Steganography Process

II. LITERATURE REVIEW

Rawat et. [5] proposes an advanced LSB substitution technique for concealing textual content facts contained in a textual content record into a colour picture. Each letter of confidential message, along with unique characters which includes spaces, enters, <, ?, $, etc., is modified with the helpof given array mapping number, and then every values is become an eight-bit binary integer. Each character's bit is encoded withinside the final LSB of every pixel of the original images. Because simply the final bit of every pixel of the original images is replaced, this technique can produce a hidden embedded images this is absolutely indistinguishable from the authentic images to the human eye.

Preetha et al. [6] gives the encryption using the realistic RSA-OAEP was provided. According to this scheme, it has extra benefits, drastically that its IND-CCA, protection endure notably related to the problem of the RSA problem, even in multi-question settings. An RSA ensures the greatestlevel of security for the business application. Furthermore, this technique may be used to encrypt lengthy messages without using hybrid or symmetric encryption. Masud et al[7]. It has provided an LSB approach for RGB true color images that improves on current LSB replacement techniques to increase the security level of concealed information.

Maiti et al. [8] proposes Data Hiding in Images Using Some Efficient Steganography Techniques" The purpose of this research was to improve the efficiency of steganalysis while also assessing the concealing capacities of previous research work. The steganalysis performance of cutting-edge detectors is near-perfect when compared to current steganographic methods. It is necessary to create new, resilient, and secure concealing techniques that can withstand Steg analytic identification. Hiding methods are distinguished by three complimentary requirements: security against steganalysis, resilience in the face of transmission channel distortions, and capacity in terms of the embedding technique. This work might be expanded to accommodate other picture formats. This work might be expanded to include additional transform techniques as well.

Ming et. al. [9] emphasized on the mechanisms used in steganography tools. Various tools are classified into five groups based on algorithm analyses: Based on Spatial domain steganography method, Based on transform domain steganography method, Based on Document steganography method, Based on File structure steganography method, and various classification, such as videos compression concealing and spread based on spectrum method steganography tools.

Neeta et al. [10] added the Least Significant Bit embedding method, which proposes that facts can be hiddenwithinside the original image's least massive bits (LSB), andthe human eye could be not able to understand the hidden facts. They defined the LSB embedding method and supplied evaluation outcomes for 2, 4, 6 (LSB) for PNG and .bmp pictures. Sharma et al. [11] added state of a art steganography approach primarily based totally on an 8bit grayscale or a 24-bit colour images, and that they engaged the logical operation to take over the certainity of the steganalysis attack.

III. PROPOSED MODEL

Now-a-Days, Data Hiding is a technique that we need more to secure our Personal data, private data, and Sensitivedata. Image encryption provides a way of dealing extremely vast image files. Lossless and lossy compression are the two forms of image encryption. Both techniques preserve storage space while having distinct impacts on any compact concealed data in the image. Lossy is a JPEG (Joint Photographic Experts Group) format file that provides strong

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

encryption but may not preserve the integrity of the original image. As a result, it is referred to as "lossy". Lossless encryption preserves the original picture data precisely, and thus is preferred by steganographic methods.

Least significant Bit based Technique

Least Significant bit insertion, Algorithms and Transformations Masking and Filtering, are the maximum common methods for concealing information in pictures. The most popular and widely used way of recent steganography is to apply the LSB of a images pixel information. When the document is longer than the messagedocument and the images is grayscale, this approach works well. Three bits can be encoded into each pixel when using LSB methods on each byte of a 24-bit picture.

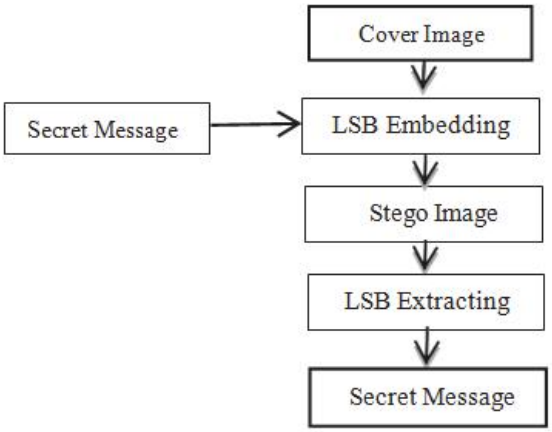


Fig. 2. Represent the LSB Proposed System Architecture

If MSB is changed, the impact of an item is extremely considerable, whereas LSB is smaller. The least massive bit (or eighth bit) of all bytes inside a images is transformed intoa mystery message bit. Digital pictures are classified into three types: 8-bit images, 24bit images, and 32bit images. We can encode three bits of information in each pixel of a 24bit picture, One in every LSB function of the 3 eight-bitvalues. Changing the LSB to increase or decrease the value has little effect on the picture's appearance; in fact, the resulting stego image appears virtually identical to the coverimage. One bit is utilised to hide information in 8bit pictures.The hidden images is extracted from the stego images with the aid of using making use of the opposite process. Following steps are involved in this algorithm.

Embedding Function

1. Inspect the original images in addition to the textualcontent message as a way to be concealed within original images.
2. Transform the color images to a compressed image.
3. Transform a textual content into a binary message.
4. Determine the LSB for every pixel withinside the original images.
5. Replace the LSB of the original images with every bit of the secret message one at a time.
6. Create a stego images.

Extraction Function

1. Inspect the stego images.
2. Determine the LSB of each pixel in the stego images.
3. Extract the bits and transform each 8-bit string into acharacter.

If the LSB of the cover image pixel value E(x, y) equals the content bit m of the conceal content to be embedded E(i,j) remains unaltered; otherwise, set the LSB of E(x, y) toS_m. The following is the message embedding procedure:

If LSB of E(x, y) = 1 and $S_m = 0$, S(x, y) = E(x, y) - 1

If LSB of E(x, y) = 0 and $S_m = 1$, S(x, y) = E(x, y) + 1

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

If LSB of E(x, y) = S_m, S(x, y) = E(x, y)

Where, LSB of E (x, y) denotes the LSB of the cover image E(i,j), and m is the next message bit to be inserted. The stego image is S(i,j). Each pixel, as we know, is made up of three bytes, each of which contains either a 1 or a 0. Assume it hides A message in 3 pixels of a picture (24-bit colors). Suppose the unique three pixels are:

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

A steganographic software might conceal the letter or number 300, whose binary representation is 100101100, which is encoded in the original image least significant bits; the resultant grid is as follows:

(00101101 00011100 11011100)
(10100111 11000100 00001101)
(11010011 10101100 01100010)

In this scenario, only some bits had to be modified in order to correctly place in the character. The modifications discovered in the least important bits are too little for the human eye to detect, therefore the content is efficiently concealed. The advantage of LSB is its integrity, and lots of procedures depend upon it. LSB also provides for a high level of perceptual transparency.

RSA based technique For Text Encryption andDecryption

RSA Stands for Rivest-Shamir-Adleman developed in 1978 [3]. It is an asymmetric algorithm which used public- key encryption algorithm and private-key decryption algorithm. In this algorithm, A key which is known to all users in network i.e. public key and A key which is kept secret not shareable to all i.e. private key. It uses prime numbers to generate a public and private key. It can be used to transfer each secrecy and integral signature. It utilizes block size, with plain text and encrypted text having integersranging from 0 to n-1 for certain n values. The length of n isdefined as 1024 bits or 309 decimal digits. Following steps are involved in this algorithm

1. Chosen any two prime integers x and y. (x!=y)
2. Determine, z = x*y
3. Determine ϕ (n)=(x-1) (y-1)
4. Choose value of a, with GCD (a, ϕ (z)) = 1 which isco-prime, 1 < a < ϕ (z)
5. Determine, b = a^{-1} (mod (ϕ (z))) i.e. ab = 1 mod ϕ (z)
6. Public key will be created as follows: (a,z)
7. Private key will be created as follows: (b,z)
8. Encryption: Calculate cipher text, C = M^e mod(n),where M<z, M is length of plain text
9. Decryption: Calculate plain text, M = C^d mod(n)

In this technique, first encrypted the plain text from the sender side using the RSA algorithm and then embedded in the cover images to attain the embeded images. The embeded images is obtained at the recipient, as well as the embedded information, which is retrieved using a steganographic process and then decrypted using the RSA method. The advantage of this algorithm is that there is no need to transfer keys securely only public elements are shared.

R-Color Channel embedding for Image

For hiding the encoding and decoding cipher text inimages. On the encoding part, encoding a text by changing the red value in the pixel color to the Unicode number of the letter. It would use a for loop in the function to loop to each position in the string for the message. I ended up getting is the letter at the last position repeated to the end of the number of pixels. The image read using PIL (Python Image Library) and is checked if in RGB (Red, Green, Blue) formator not. If yes, then the R-color-channel value is what I have modernize to hide the content wuthin the image. For hidden the content:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

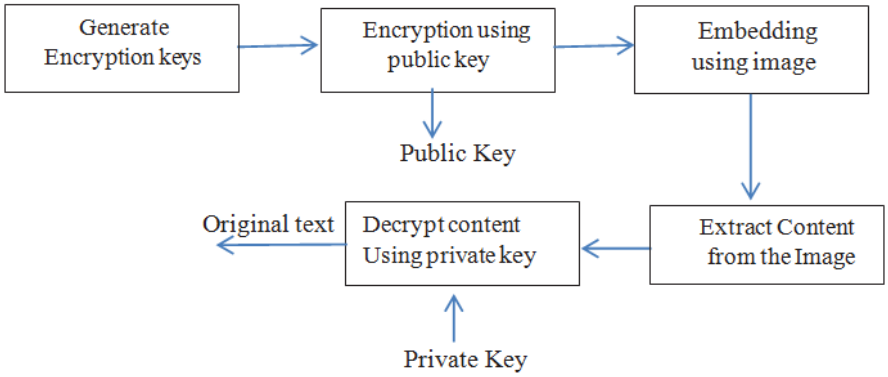


Fig. 3. Show the sequence of R-color Channel Encoding and Decoding

Firstly, starting from (0,0) location of the image and modifying its R-channel value with the length of the message to hide.

Now from the next pixel, an encoded letter willreplace the R-channel value for the corresponding pixel and move on to the next pixel.

Then, the above process will continue until each letter gets hidden. If a row of all pixels gets modifiedthen the next row's pixel will be taken for the process and it continues till 255 character length.

IV. IMAGE QUALITY ASSESSMENT

Comparing stego images outcomes with original images results need some image quality criteria such as mean squared error, peak signal to noise ratio, and capacity.

Mean Squared Error:

Between the images I1(X,Y) and I2(X,Y), the mean- squared error (MSE) is [7]:

$$MSE = \frac{\sum_{X,Y}[I1(X,Y) - I2(X,Y)]^2}{X * Y}$$

The range of rows and columns with inside the enterimages is denoted by X and Y, correspondingly.

Peak Signal-to-Noise Ratio

It prevents this trouble through adjusting the MSEconsistent with the body range:

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

PSNR is deliberate in decibels (dB). This adequate rate for the assessment of reinstating outcomes for a similarimage.

Capacity

It determines the record length of an original image which may be modified without changing the integrity of the original image. Steganographic integration is supposed to maintain the statistical estate of the original image in addition to its perceptual quality. As a result, the ability buildupon on the whole range of bits according to pixel and the range of bits constructed into every pixel. The quantity is displayed according to bit according to pixel(bpp).

V. RESULTS AND DISCUSSION

The color or appearance of the image remain unchanged after using different steganographic methods in this work. The image size remains unchanged. The two levels of security are provided by this proposed work. It hides the existence of undisclosed text from suspicious user. A hacker cannot decrypt the image as the undisclosed text is in addition, encrypted the use of RSA encryption algorithm. The color images are used to test the proposed LSB based steganographic technique. A unique matrix is generated and taken into consideration for LSB substitution withinside

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

the color picture experiment. 3-d matrix isgenerated in RGB picture as it incorporates 3 colour additives i.e., red, green, and blue. These 3 matrices are dealt with one at a time for every colour element for LSBsubstitution. In this experiment, the 24-bit colour picture is used.

The Python matplotlib Tool elaborates the Effect of LSB Technique on image. For implementation purposes import matplotlib.pyplot is used to shown in Fig.5 & 6, [12].

(a) Lenna original image (b) Lena stego image (c) Pepper original image (d) Pepper stego image

Fig. 4.

TABLE I. PERFORMANCE ANALYSIS ON LSB TECHNIQUE

S. No.	Images	MSE	PSNR
1.	Lenna	0.062385	60.1587
2.	Pepper	0.072932	59.5016

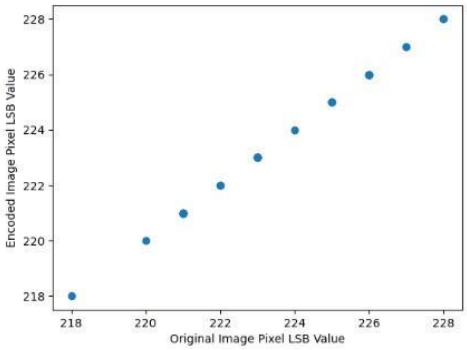


Fig. 5 Effect of LSB Technique on Lena Image

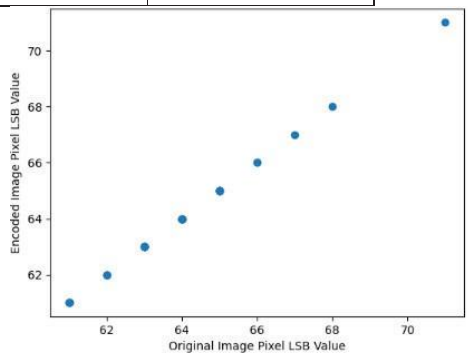
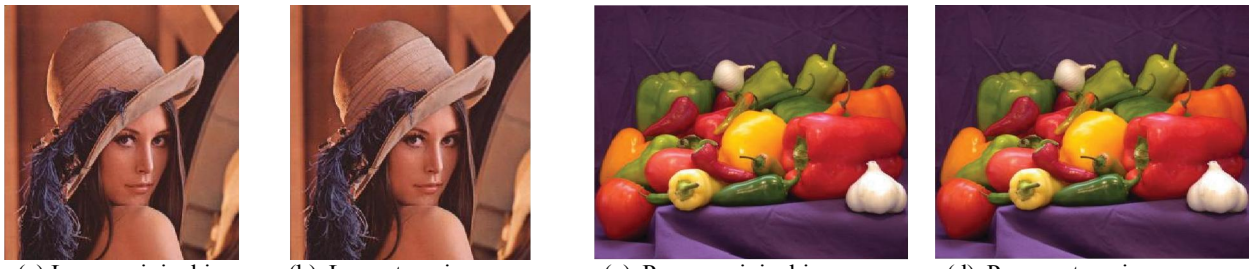


Fig. 6 . Effect of LSB Technique on Pepper Image



(a) Lenna original image (b) Lena stego image (c) Pepper original image (d) Pepper stego image

Fig. 7.

TABLE II. PERFORMANCE ANALYSIS ON RSA TECHNIQUE

S.No.	Images	MSE	PSNR
1.	Lenna	0.842663	48.8743
2.	Pepper	0.104762	57.9287

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

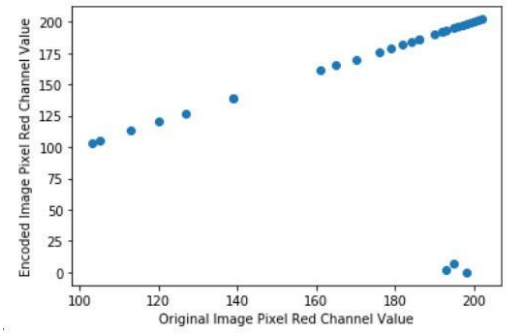


Fig. 8. Effect of RSA Technique on Lena Image

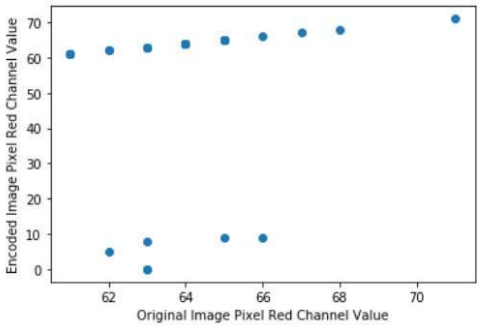


Fig. 9. Effect of RSA Technique on Pepper Image

The Python matplotlib Tool elaborates the Effect of RSA Algorithm on image. For implementation purposes import matplotlib.pyplot is used to shown in Fig.8 & 9, [12].

VI. CONSEQUENCES

A reliable technique based on LSB for image steganography has been offered. It is an effective steganography method to integrate secret messages in cover images with no significant changes have been completed through the LSB methodology. This approach additionally applies a cryptography implementation i.e. RSA set of rules is used to secure the confidential content so that it is difficult to crack the encryption with no key. The RSA set of rules itself is extraordinarily secure, that is why we used this method to elaborate the security of the secret message. In this work, a new manner to hide information in an image with much variant withinside the image bits will offered, making our procedure safe and more systematic than LSB.

REFERENCES

[1] Petitcolas FA, Anderson RJ, Kuhn MG, “Information hiding— a survey”. Proceedings of IEEE, Vol. 87, No. 7, pg. 1062– 1078, 1999.
[2] N. F. Johnson, S. Jajodia, “Steganography: seeing the unseen”, in Computer, Vol. 31, No. 2, pg. 26 - 34, 1998.
[3] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121
[4] Shen S, Huang L, Tian Q, “A novel data hiding for color images based on pixel value difference. and modulus function”. Multimedia Tools Applied Vol. 74, No. 3, pg. 131-141, 2015.
[5] Deepesh Rawat, Vijaya Bhandari, “A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image”, International Journal of Computer Applications, Vol. 64, No. 20, 2013.
[6] M. Preetha et al, “A study and performance analysis of RSA algorithm”. International Journal of Computer Science and Mobile Computing Vol.2 Issue. 6, pg. 126-139, 2013.
[7] Masud K. S.M. Rahman, Hossain, M.L., “A new approach for LSB based image steganography using secret key”. Proceedings of 14th International Conference on Computer and Information Technology, pp. 286-291, 2011.
[8] Chandreyee Maiti*, Debanjana Baksi, Ipsita Zamider, Pinky Gorai, and Dakshina Ranjan Kisku “Data Hiding in Images Using Some Efficient Steganography Techniques” Springer International Conference on Signal Processing, Image Processing, and Pattern Recognition, pp. 195-203, 2011.
[9] M. Chen, R. Zhang, X. Niu and Y. Yang, "Analysis of Current Steganography Tools: Classifications & Features," 2006 International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA, 2006, pp. 384-387,
[10] D. Neeta, K. Snehal and D. Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits," 2006 1st International Conference on Digital Information Management, Bangalore, India, 2007, pp. 173-178.
[11] Vijay Kumar Sharma, Vishal shrivastava, “A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection.”Journal of Theoretical and Applied Information Technology, Vol. 36, No.1, pg: 1992-8645, 2012.
[12] Matplotlib “pyplot tutotrial” [Online] Available: https://matplotlib.org/stable/tutorials/introductory/pyplot.html.