A Secure Image Steganography Algorithm Based On Least Significant Bit And Bit-Plane Slicing

Bodavula Rahul
Department of ECE
Vardhaman College of Engineering,India
bodavularahul@gmail.com

Shahed Afride
Department of ECE
Vardhaman College of Engineering,India
shahedafride0011@gmail.com

Kandi Uday Kiran Goud
Department of ECE
Vardhaman College of Engineering,India
Kudaykirangoud@gmail.com

Mr.CH.Ramakrishna
Assistant Professor,Department of ECE
Vardhaman College of Engineering
rahulvar434@vardhaman.org

Abstract—**Steganography is the practise of obscuring data, such as text, photos, or videos, under a cover image. Because the secret information is concealed, it cannot be seen by human eyes. Conventional image steganography, CNN-based image steganography, and GAN-based image steganography are the three primary types of picture steganography methods. Algorithms unrelated to machine learning or deep learning are used in frameworks referred to as classical approaches. An image's pixel quality is higher because the majority of its pixels are not used. The underlying principle of LSB methods is that little changes in pixel values would not produce discernible changes. A binary representation of the confidential information is created. The least significant bits in the noisy region are found by scanning the cover image. After that, the LSBs of the cover image's binary bits are changed to those from the hidden picture. Because overloading the cover image could cause noticeable alterations that reveal the presence of the secret information, the substitute approach must be used carefully.**

Keywords: Image Steganography, CNN(ConvolutionalNeuralNetwork),GAN(GenerativeAdversarialNetwork),LSB (LeastSignificantByte).

I.INTRODUCTION

Data security is a serious worry in today's society. Steganography aims to make a secret message invisible to the human eye by enclosing it inside of a digital cover, such as a picture, text, music, or video. Several types of steganography have been used since the year 2500. With the advent of computers and the development of digital signal processing, coding theory, and information theory, steganography transitions to the digital realm. The focus of this study is on image steganography. The security and predictability of the technology are enhanced by inserting message bits in a new set of virtual bit planes produced via pixel value decomposition.[1].The accuracy of unfiltered real-life face age and gender assessments has yet to be proven. Despite the progress made by the computer vision community in terms of continual improvements.

A digital image is said to be grayscale if each pixel's colour information is a monochrome signal. Grayscale is typically used to colour this type of image, with black representing the colour with the weakest tones and white representing the colour with the strongest. A composite image that seems exactly like the original image but may really include a hidden image or a secret message can be made by embedding any type of data in one of its 8 bits, which have 255 levels. "Watermarking" is a phrase used to describe one of these embedding methods. Most of the time, the watermark is only a shadow of a picture with a slight brightness/darkness modification. This paper proposes a novel method for creating the watermark. Instead than employing an image or text injection like earlier methods, the watermark is created using a Cubic-spline curve that is embedded into the image using Bit Plane Slicing. The goals of a watermark include control indicators, content protection, and the legality, dependability, and integrity of the data. [2].

The following sections of this paper are organised as follows. A summary of some earlier studies on Image Steganography is given in Section II. The specifics of our suggested framework and the structure of our multi-task learning model are presented in Section III. The experimental experiments IV , quantitative performance of our model, and visual evaluation of model outputs are then presented in Section V. In Section VI, the paper is finally finished.

II.RELATED WORK

Seungmin Rho et.al In this paper MLSB-SM, a revolutionary magic least significant bit replacement technique, is proposed for RGB pictures. The hue-saturation-intensity (HSI) colour model's achromatic component (Iplane) and multi-level encryption (MLE) in the spatial domain are the foundations of the suggested approach. The supplied image is rotated and made to use the HSI colour space. The Iplane is divided into four identical sub-images, each of which is rotated at a different angle with the aid of a secret key.Four blocks of the confidential information are created, and an MLE technique is used to encrypt them (MLEA).Using LSB replacement, each message sub-block is embedded into a single rotational sub-image depending on a predetermined pattern.Comparing the suggested method to a variety of other widely used techniques confirms that it not only enhances the stego pictures' aesthetic quality but also provides good imperceptibility and different security levels. [4].

ShilpaPund-Dange et.al In this paper, the Catalan-Lucas Series and the ModifiedSteganographic algorithm are used to present a novel steganographic technique. Instead of using 8 bits, this method uses 16 bits to represent each RBG component of the image as a Catalan Lucas number sequence.Bit Plane Slicing divides the cover image into 48 virtual planes and the hidden content into 16 virtual planes. The presented approach transforms a portion of the 48 virtual planes of the cover image into the 16 virtual planes of the secret message.[5].

Minglin Liu et.al In this paper, we suggest a adversarial embedding method for steganography of images. We produce stegos first, as opposed to previous pertinent studies, and then combine numerous cover gradients to determine the cost adjustment directions. Then, in contrast to earlier studies where the embedding costs were varied entirely or partially at random, In accordance with the amplitudes of cover gradients and their costs, we carefully choose the candidate costs. The security of five contemporary steganographic techniques, as tested on both retrained CNN-based and traditional steganalyzers, can be considerably increased by changing just a small part of embedding costs [6].

ELSHAZLY Emad et.al The least significant bits of each component of colour photos as well as the integer wavelet transform approximation coefficients of grayscale images are used in this paper's proposed safe steganography algorithm to conceal a bitstream of the secret text (LSBs). The MATLAB programming language is used to carry out the approved steganography procedures include embedding and extracting steps. The key challenges with steganography are its invisibility, payload capacity, security in terms of peak signal to noise ratio, and endurance. To assess the statistical separation between cover pictures and stego-images, the mean square error and PSNR are utilised. The normalised cross correlation is used to determine the strength of their association [7].

B.Chitradevi et.al In order to conceal data in an image, this paper gives a brief overview of the image steganography technique that use the Least Significant Bit method.The network offers a way for people to communicate and disseminate information. The security of information has grown to be a significant problem with the expansion of data transfer across computer networks. There are many methods for concealing data, but steganography is the most well-known.Steganography is the practise of unseen communication. The way the message's existence can be concealed is through steganography. This is performed by concealing the existence of the communicated information by incorporating it into another piece of information [8].

Mayukh Das et.al The paper focuses on bit plane extraction and shows how it can be used to the task indicated above. It has been discussed how to encrypt and decode data. Any writing that might include important information is referred to as the data to be buried in this context. No audio or video files are included. Grayscale images, which serve as the reference image covering the data, have received the most attention, more and more study approaches for data hiding are emerging along with the advancement of computer security. I have made an effort to apply one methodology in this regard. The code's simplicity is one of this work's primary advantages. The user can learn the approach and create their own data-hiding strategies thanks to it. But there are also certain restrictions. The biggest flaw is that the final decoded image is a little distorted even though it is viewable. This issue requires the use of an advanced image processing approach. However, data masking methods have developed from regional use to widespread adoption. The depth of exploration can be further intensified using a new technique [9].

SHRIKANT S. KHAIRE et.al The basic principles of steganography and numerous attributes required for data concealment are the main topics of this study. What's more, the study uses a steganographic technique with a 50–60% concealment capacity. This kind of steganography is known as Bit Plane Complexity Segmentation (BPCS). The binary image is split into an instructive region and a region that looks like noise according to the basic BPCS technique. In the vessel image's region that resembles noise, the secret information is concealed without any image degradation. We employed two photos in our experiment: a vessel image of 512 x 512 pixels and a secret image of 256 x 256 pixels. We used the BPCS Principle by Eiji Kawaguchi and Richard O.Eason. To determine the image hiding capacity, we ran this experiment with three different sets of photographs [10].

O. I. Al-Sanjary et.al In this paper two new encryption methods that improve the security and precision of technology.This study proposed a novel technique to make the approaches more user-friendly and manageable while simultaneously increasing security.As a result, the study presented in this paper intends to create two new types of encryption: Advanced Encryption Standard and Least Significant Bit It also outlines the conditions that must be met for the best steganographic algorithm and presents the steganographic approaches that are appropriate for various purposes.[11]

III.THE PROPOSED FRAMEWORK

A.Steganography

Steganography is a method of hiding sensitive information by encasing it in a conventional, non-secret file or communication; the information is then recovered from the container at the desired location. Data protection or data concealment can be achieved via steganography and encryption. The term "steganography" is derived from the Greek terms "steganos" and "graph" (meaning to write). Text, photos, videos, and music, among other types of digital information, can all be used to conceal data that can be concealed within virtually any other type of digital content.Before being inserted to the cover text file or data stream with an apparently innocent appearance, the hidden text,or the information intended to be concealed using steganography, is frequently encrypted.

B.Lsb

Eight bits are used to represent each pixel in a grayscale image. Only by "1" is a pixel referred to as the Least Significant bit since its value affects the pixel value. As a result, this attribute is used to conceal the image's data. If the last two bits are specified, they are LSB bits and only affect the value of the pixel by "3." Additional data can be stored because of this. Least Significant Bit (LSB) steganography is one of these techniques that is the most basic. A data bit is used to replace of the picture. We encrypt the raw data before embedding it in the image to improve security because this method is susceptible to steganalysis.

The processing time is increased by the encryption process, but it also increases security. This approach is fairly simple. With this method, a bit of the secret message is substituted for any or all of the least important bytes in an image. Other techniques for hiding messages in multimedia carrier data have evolved using the LSB embedding method as its base. Additionally, LSB embedding can be used to certain data domains, such as embedding a secret message into a JPEG image's frequency coefficients or an RGB bitmap's colour values. LSB embedding is applicable to a wide range of data types and formats. Because of this, LSB embedding is one of the most important steganography techniques now in use. The LSB method has been used as a starting point for a number of related approaches. For instance, a minor adjustment is made to the secret message's binary code conversion.The Huffman encoding technique employing binary bits is used to encode the secret message. The LSB method is then used to incorporate the encoded bits into the cover image. For RGB photos, a different version of the LSB technique is employed. The cover image has three channels. The R, G, and B planes divide the secret information into the ratios 2:2:4 and 5:5:4. The secret bits are hidden utilising the color-related pixels that are thought to change colour, and the frequency domain is used for the quantum image domain.

A hybrid of cryptography and steganography is used to swap out the most crucial areas of the secret image for the LSB of the cover image. The key is consistently encrypted while the pixels are selected using a pseudo-random number generator. By substituting the secret message for the k least bits, the k-LSB technique is applied. To locate and uncover the hidden picture in steganalysis, an entropy filter is employed.

C.Bit planeslicing

One or more bits of the byte are used for each pixel when an image is represented via bit plane slicing. The original grey level is converted to a binary image because only the MSB can be used to represent a pixel. Bit plane slicing has three primary objectives:

1.Creating a binary image from a grayscale image.
2.Using fewer bits to represent an image and scaling it down to a smaller size
3.Simply focusing, one can improve the image.

Example:

The provided image is a 3-bit image because the highest grey level is 7. The image is binary-converted, and the bit planes are separated.

6	7	6	6	7
0	0	0	1	2
1	1	1	2	3
4	5	5	4	2
6	6	6	7	7

110	111	110	110	111
000	000	000	001	010
001	001	001	010	011
100	101	101	100	010
110	110	110	111	111

1	1	1	1	1
0	0	0	0	0
0	0	0	0	0
1	1	1	1	0
1	1	1	1	1

MSB

1	1	1	1	1
0	0	0	0	1
0	0	0	1	1
0	0	0	0	1
1	1	1	1	1

central bit

0	1	0	0	1
0	0	0	1	0
1	1	1	0	1
0	1	1	0	0
0	0	0	1	1

LSB

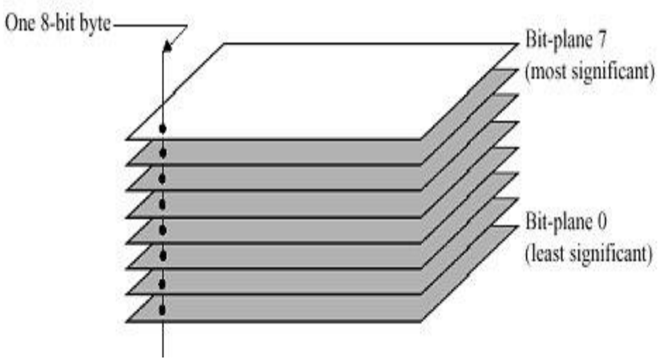

Figure 1.: Bit plane slicing

Note: This Figure is taken from https://www.shubbak.de/2014/03/20/03-image-compression/ website

Block diagram :

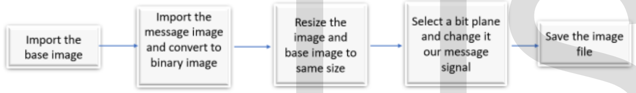
Import the base image
Import the message image and convert to binary image
Resize the image and base image to same size
Select a bit plane and change it our message signal
Save the image file

Figure 2 : Block diagram of encryption process

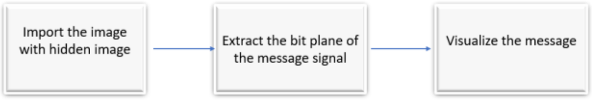
Import the image with hidden image
Extract the bit plane of the message signal
Visualize the message

Figure 3:Block diagram of decryption process

Encryption algorithm ::

Input:
cover image,secret message (which is in jpg format)
Output:
stego image

1. Import the starting image. The system's matlab programme files should contain the same base image in jpg format.
2. Then, make the message image by writing the hidden message that you wish to send to the recipient in paint, saving the file as a jpg, and saving it in the same folder as the base image.
3. The message image will now be converted to a binary image. Therefore, since we cannot convert RGB images directly to binary, we must first convert them to grayscale images using the rgb2gray command. Using the command imbinarize, turn the grayscale image you just created into a binary image.

Decryption algorithm :

Input:
stego image
Output:
secret message

1. . Import the image with hidden image i.e.,stegoimage that is in the bmp format with the help of the command imread.
2. Extract the bitplane of the message signal with the help of command bitget.
3. Visualize the message.

IV.EXPERIMENTAL RESULTS:

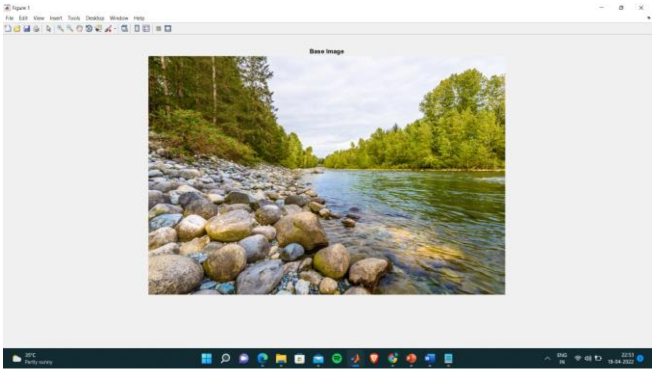

Figure 4: Base image i.e., cover image

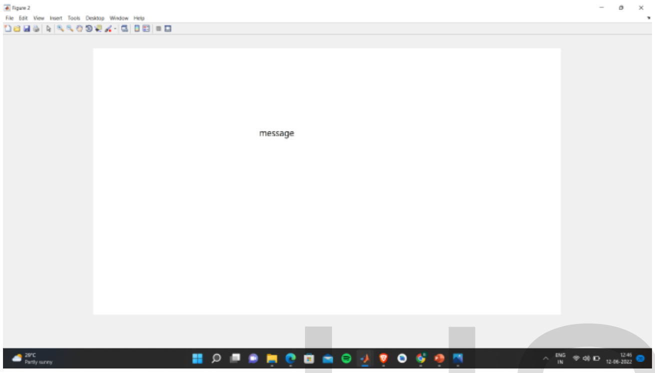

Figure 5 : Message Image Before Binarize

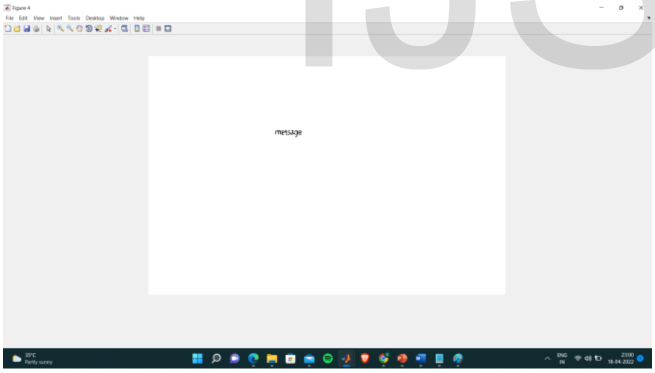

Figure 6 : Message Image After Binarize

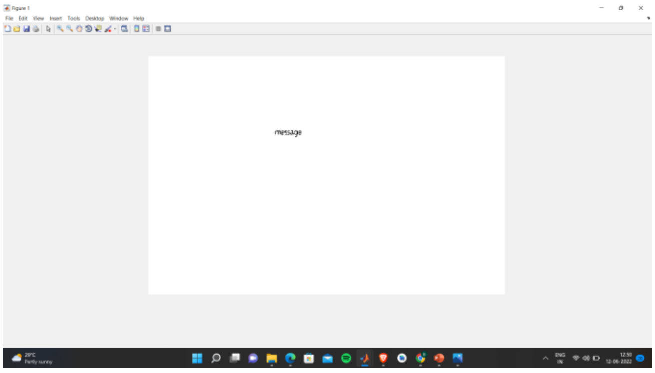

Figure 7 : Message Image After Resize With Base Image

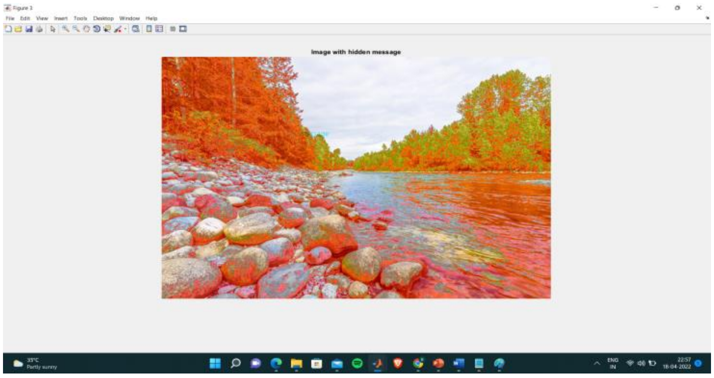
Figure 3
File Edit View Insert Tools Desktop Window Help
Image with hidden message

Figure 8 : Base Image With Hidden Message i.e Stegoimage In Bit Plane 8

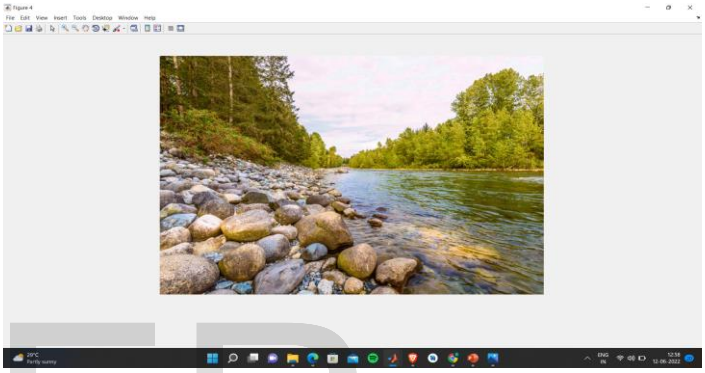

Figure 9: Stegoimage in bit plane 5

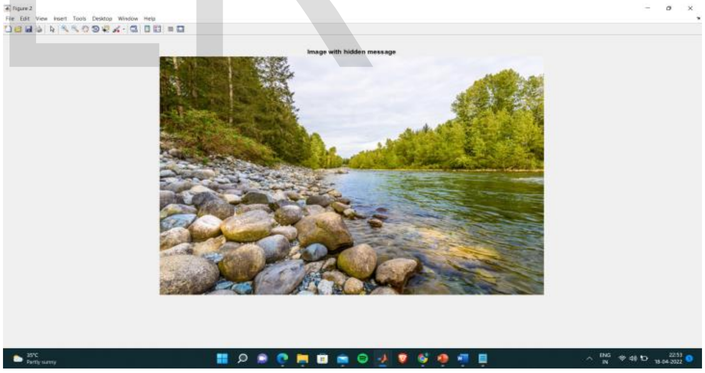
Figure 2
File Edit View Insert Tools Desktop Window Help
Image with hidden message

Figure 10 : stegoimage in bit plane 1

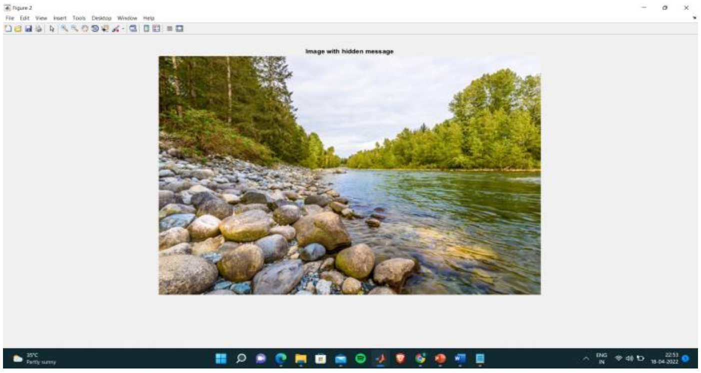
Figure 2
File Edit View Insert Tools Desktop Window Help
Image with hidden message

Figure 11: Stegoimage That Contains Hidden Image In It.

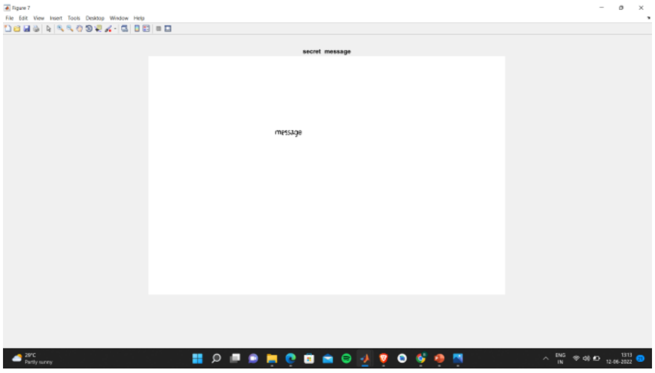

Figure 12: hidden message image is retrieved from stegoimage

V.COMPARATIVE ANALYSIS

Table.1.Analysis with other proposed models.

Refernces	Software used	PSNR value(in Db)	Complexity	Payload Capacity	Image Type Supported
[11]	Inbuild software	48.66	High	Maximum 4 bits per pixel per data channel	Gray scale image
[7]	MATLAB	59.78	Medium	1.583 bpp	Gray scale and colour image
OUR WORK	MATLAB	80.54	Low	1 bit per 8 pixels	Gray scale and colour iamge

VI . CONCLUSION

Information transfer security is essential in the automated era. Therefore, the suggested approach will offer security by encrypting and decrypting the message using LSB and bit plane slicing. Sensitive information can be effectively concealed with steganography.The LSB Technique is applied and Bit Plane Slicing Technique to the images in order to create secure stego-images. The image resolution rarely changes and is negligibly affected when the message is embedded into the image and the image is encrypted. So, unauthorised personnel cannot harm the data in any way. The algorithm is applicable to cover and secret images of the same size in both 8-bit and 24-bit formats, making it simple to implement in both grayscale and colour images. The first is the Least Significant Bit (LSB), often known as the striking rationality, and the second is the most recent scheme with LSB+bit plane slicing. The outcomes of the individual checks have been examined for the estimations of PSNR. It can be shown that the LSB+bit plane slicing calculation results in better demands for the PSNR. This is one of the conclusions that have been looked into in this work, and work is still being done to advance the computations for still better code unconventionality and nature of time complexity.

Better PSNR, MSE, and RMSE values from the suggested replacement technique indicate that, in comparison to any traditional LSB approach, the quality of the cover image is being modified less during the steganography hidden message embedding process. Comparing the suggested method quantitatively to the LSB algorithm reveals that it maintains better image quality over a variety of images and secret contents. The secret message is additionally improved by the proposed approach since character sequences that underwent optimization prevent them from being deciphered. Future work on the suggested approach might find more comparable spatial domain optimizations and improve the quality of the embedded photos.

More and more research approaches are emerging for the goal of data concealment as computer security advances. I have made an effort to put one methodology into practise for this. The straightforwardness of the code is one of this work's key advantages. It enables a user to comprehend the procedure and create custom data-hiding strategies. There are certain restrictions, though. The main drawback is that, despite being readable, the resulting decoded image is slightly warped. To tackle this issue, a sophisticated image processing technique is required. Data masking methods, however, have progressed from regional use to widespread adoption. The level of exploration can be increased further by using a new technique.

REFERENCES

[1] S.T.Rahamn, author = ”Huda Dheyauldeen Najeeb”, title = ”New Techniques of Watermark Images using Bit Plane Slicing and Cubic-spline Interpolation”, journal = ” Ibn Al-Haitham Jour. for Pure & Appl. Sci. 32 (3) 2019”

[2] H. Dibeklio˘glu, author = ”H. Dibeklio˘glu, F. Alnajar, A. Ali Salah and T. Gevers”, title = ”Combining Facial Dynamics With Appearance for Age Estimation”, journal = ”IEEE Transactions on Image Processing”, volume = ”24”, pages=”1928-1943” year = ”June 2015”

[3] K. Zhang et al, author=K. Zhang et al, journal=IEEE Access, title=Age Group and Gender Estimation in the Wild With Deep RoR Architecture, year=2017, volume=5, pages=22492-22503

[4] Seungmin Rho, author = “Seungmin Rho,Sung Wook Baik “, title = “A Novel Magic LSB Substitution Method (M-LSB-SM) using Multi-Level Encryption and Achromatic Component of an Image”.

[5] ShilpaPund-Dange, author = ”ShilpaPund-Dange”,”Chitra G Desai”, title = ”A novel Approach of Steganography using Bit plane Slicing

and Catalan-Lucas Number Sequence", journal = " International Journal on Recent and Innovation Trends in Computing and Communication",Volume = "6", Issue = "6",ISSN = 2321-8169

[6] Minglin Liu, author =”Minglin Liu”,”Weiqi Luo” ,title = “A New Adversarial Embedding Method for Enhancing Image Steganography”,journal = “IEEE Transactions On Information Forensics And Security”,volume = ”16”, year = ”2021”.

[7] ELSHAZLY Emad, author =”ELSHAZLY Emad”,”ABDELWAHAB Safey”, title = ”A secure image steganography algorithm based on least significant bit and integer wavelet transform”, journal = “Journal of Systems Engineering and Electronics”,Volume = “29”, Issue = “3”, year = “June 2018”, pages = 639 – 649.

[8] B.Chitradevi,author =B.Chitradevi,N.Thinaharan and M.Vasanthi” title = ”Data Hiding Using Least Significant Bit Steganography in Digital Images”,ISSN: 2349 – 4891,year = 2017.

[9] Mayukh Das, author =”Mayukh Das”, title = ”An Effective Method to Hide Texts Using Bit Plane Extraction”,journal = “IOSR Journal of Computer Engineering”,Volume = “17”, Issue = “2”, year = “Mar – Apr. 2015”, pages = 17 – 23.

[10] Mayukh Das, author =”Shrikant S. Khaire”, title = ”Steganography–Bit Plane Complexity Segmentation (BPCS) Technique”,journal = “International Journal of Engineering Science and Technology”,Volume = “2(9)”,year = “2010”,ISSN: 0975-5462

[11] O. I. Al-Sanjary,, author =” O. I. Al-Sanjary”, title = ” "A New Approach to Optimum Steganographic Algorithm for Secure Image,”,conference = “IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)”, 2020, pp. 97-102, doi: 10.1109/I2CACIS49202.2020.9140186.