IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

Hiding a Confidential Message into an Image Using Bit Plane Method

R.Nivas[1] , H.Parandaman[2], R.Subhan[3] , Mr.A. Joseph Sathiadhas Ezra, M.E.,(Ph.D.)

U.G. Student, Department of Electronic and Communications Engineering, Meenakshi Sundararajan Engineering College, Arcot Road, Chennai, TamilNadu, India[1]

Assistant Professor, Department of Electronic and Communications Engineering, Meenakshi Sundararajan Engineering College, Arcot Road, Chennai, TamilNadu, India[2]

ABSTRACT: Text encryption is process of hiding the text into the image in order to prevent unauthorized persons to gain access to confidential message. Message is the transfer of information from the sender to the receiver through a particular medium. Encryption is the most effective process for achieving data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. In existing, texts were hidden by the watermark method. This paper proposes the method called bit planes, using that method extract the selected image by hiding the text to the selected planes. An original image is encrypted with a secret key, without knowing the encryption key the text will not be retrieved. During the decryption process, the secret message can be extracted with the secret key.

SCOPE OF THE PROJECT: Fast evaluation of digital data exchange occurs in recent years. Due tothat security of information is much important in data storage and transmission process. Security of internet banking account passwords, email accountspassword etc. requires text protection in digital media. In the same way imagetransmission and storage during industrial and research processes requiresimage protection.

KEYWORDS: Image encryption, Bit plane extraction, Advanced encryption standard (AES) , Steganography.

I. INTRODUCTION

GENERAL: Thetermdigitalimagereferstoprocessingofatwo-dimensionalpicturebyadigitalcomputer. In a broader context, it implies digital processing of any two-dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Nowadays, image processing is among rapidly growing technologies. It forms core research area within engineering and computer science disciplines too.

Image processing basically includes the following three steps:

- Importing the image via image acquisition tools;
- Analysing and manipulating the image;
- Output in which result can be altered image or report that is based on image analysis.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

II. METHODOLOGY

The first block of implementation is to develop a toolbox consisting of a list of demo images set to be displayed to the user at the encryption side, so that he can choose any one of the images from the list for encryption. All the demo images in the toolbox are preprocessed according to the requirement of the project i.e., all the demo images are grayscale images.

Gray scale images are basically those images which we say black and white image. Each pixel of gray scale image has a value lies in between 0 – 255 which decides at which position, the image will be black and at which position, it will be white. If pixel value is 0, it means that pixel color will be fully black and if pixel value is 255, then that pixel will be fully white and pixel having intermediate value will be having shades of black and white. We are given a gray scale image. Since pixel value of gray scale image lies between 0 -255, so its information is contained using 8 bits. So, we can divide that image into 8 planes. This step is followed by the encryption block where the text to be hidden is encrypted using a key generated by a key source which follows the Advanced Encryption Standard. Here the text is encrypted and then the encrypted text is hidden in to the image in this block. The next step involves the decryption and decoding of the encrypted text. This is done in the decryption module where the key is used to retrieve the hidden message.

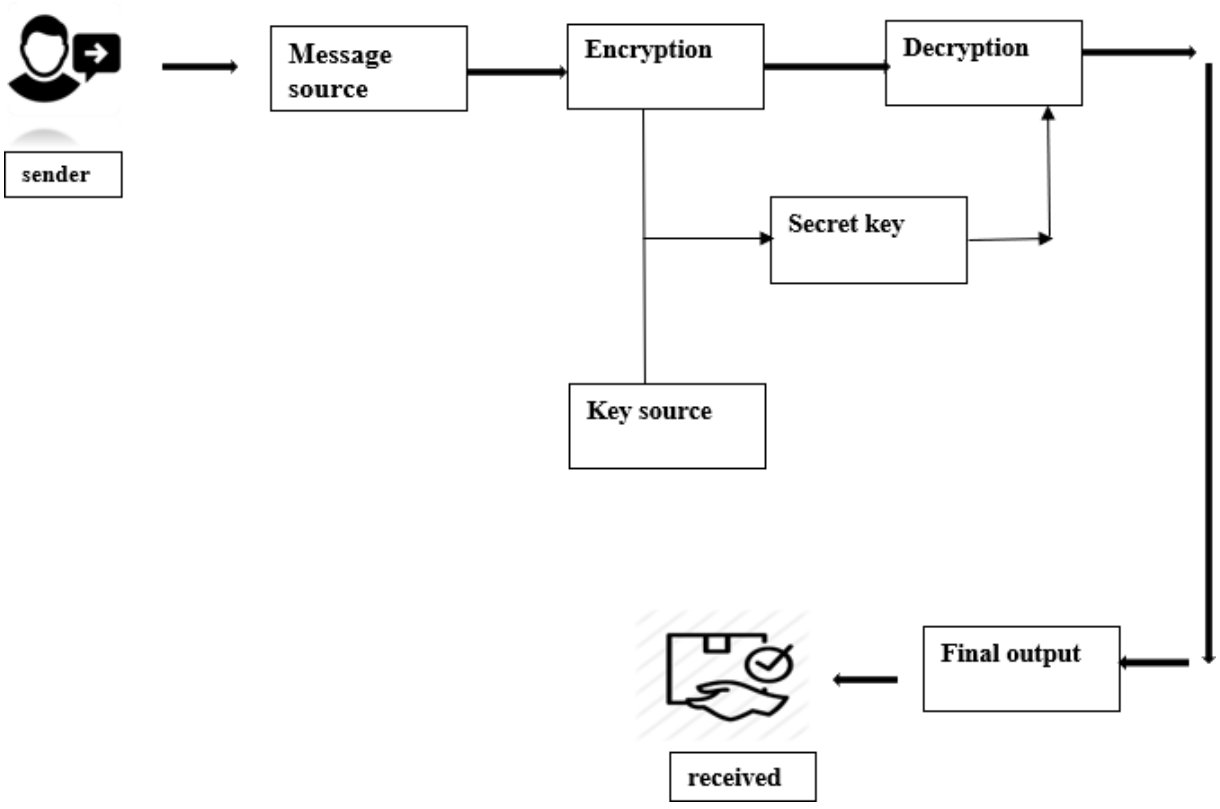

Figure 1. Block diagram

1. PRE-PROCESSING:

LettheuserselectfromalistofallthedemoimagesthatshipwiththeImageProcessing Toolbox. Image is basically combination of individual pixel (dots) information. When we write that image is of 620 X 480 sizes, it means that image has 620 pixels in horizontal direction and 480 pixels in vertical direction. So, altogether there are 620 X 480 pixels and each pixel contains some information aboutimage.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

2. BIT PLANE EXTRACTION:

Grayscaleimagearebasicallythoseimagewhichwesayblackandwhiteimage.Each pixel of gray scale image has a value lies in between 0 – 255 which decides at which position, the image will be black and at which position, it will be white. If pixel value is0,itmeansthatpixelcolorwillbefullyblackandifpixelvalueis255,thenthatpixel will be fully white and pixel having intermediate value will be having shades of black andwhite.WearegivenaGrayscaleImage.Sincepixelvalueofgrayscaleimagelies between0-255,soitsinformationiscontainedusing8bit.So,wecandividethatimage into 8 planes (8 Binary Image). Binary image are those images whose pixel value can be either 0 or 1. So, our task is to extract each bit planes of original image to make 8 binary images Let particular pixel of gray scale image has value 212. So, its binary valuewillbe11010100.So,its1stbitis0,2ndis0,3rdis1,4rthis0,5this1,6this0, 7th is 1, 8th is 1. In this manner, we will take this 8 bit of all pixels and will draw 8 binary images. We have to do this to all the pixels and generate newimages.

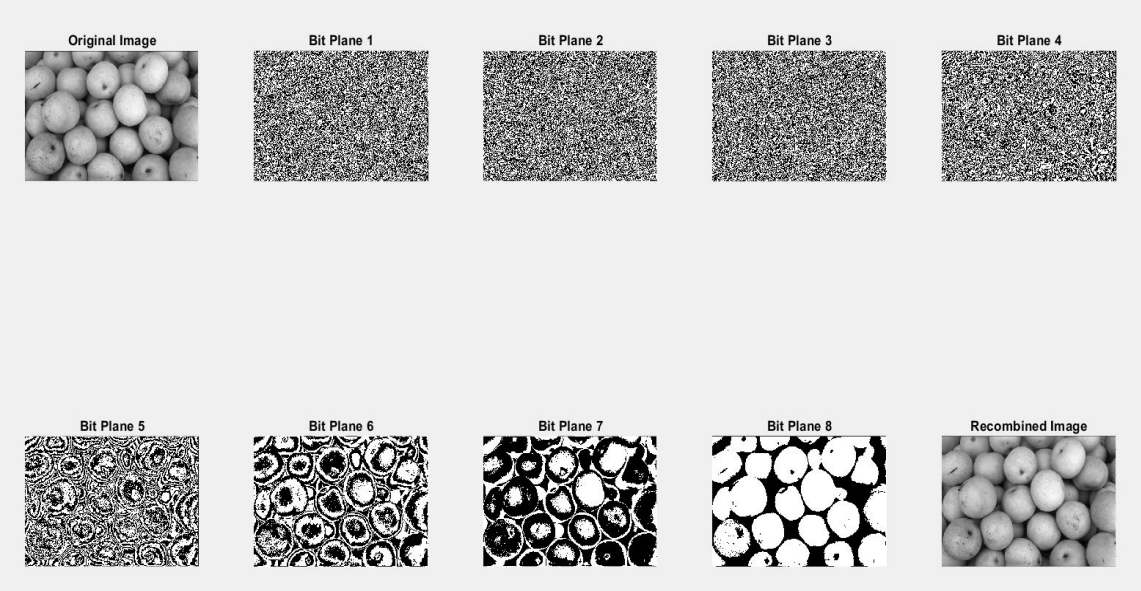

Figure 2 :

3. ENCRYPTION:

In cryptography, encryption is the process of encoding a message or informationin such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligiblecontenttoawould-beinterceptor.Inanencryptionscheme,theintended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can be read only if decrypted.For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm.

It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipientsbutnottounauthorizedusers.Atthebeginningoftheencryptionprocess, the sender must decide what cipher will best disguise the meaning of the message and what variable to use as a key to make the encoded message unique. The most widely used types of ciphers fall into two categories: symmetric and asymmetric. Symmetric ciphers, also referred to as secret key encryption, use a single key.

4. DECRYPTION:

Decryption is the process of taking encoded or encrypted text or other data andconverting itbackintotextthatyouorthecomputercanreadandunderstand.Thistermcouldbeused todescribeamethodofunencryptingthedatamanuallyorunencrypting thedatausingthe proper codes or keys.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

Data may be encrypted to make it difficult for someone to steal the information.Somecompaniesalsoencryptdataforgeneralprotectionofcompanydataand trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable. One of the reasons for implementing an encryption-decryption system is privacy.

As information travels overthe Internet, it is necessary to scrutinise the access from unauthorized organisations or individuals. Due to this, the data is encrypted to reduce data loss and theft. Few common items that are encrypted include text files, images, e-mail messages, user data and directories. The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. For decryption, the system extracts and converts the garbled data and transforms it into words and images that are easily understandablenotonlybyareaderbutalsobyasystem.Decryptioncanbedonemanually orautomatically.

III. EXPERIMENTAL RESULTS

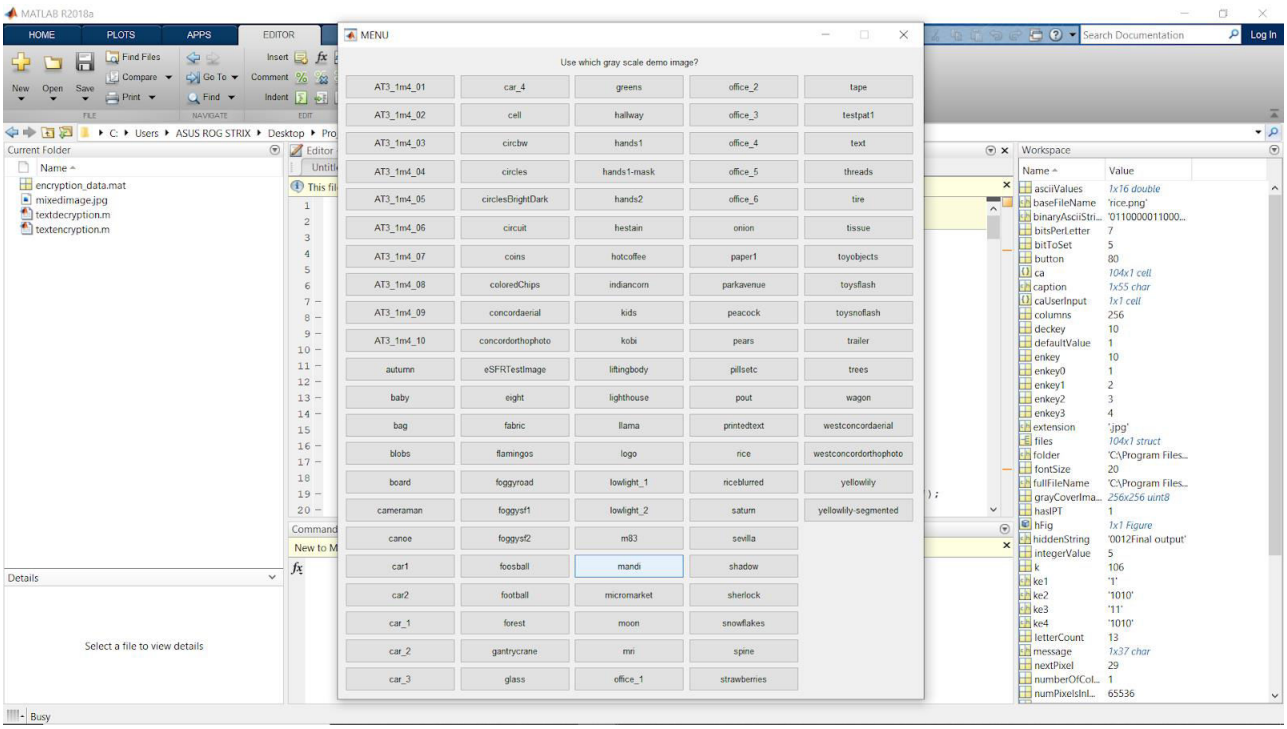

Figure 3. Display The ImageToolbox

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

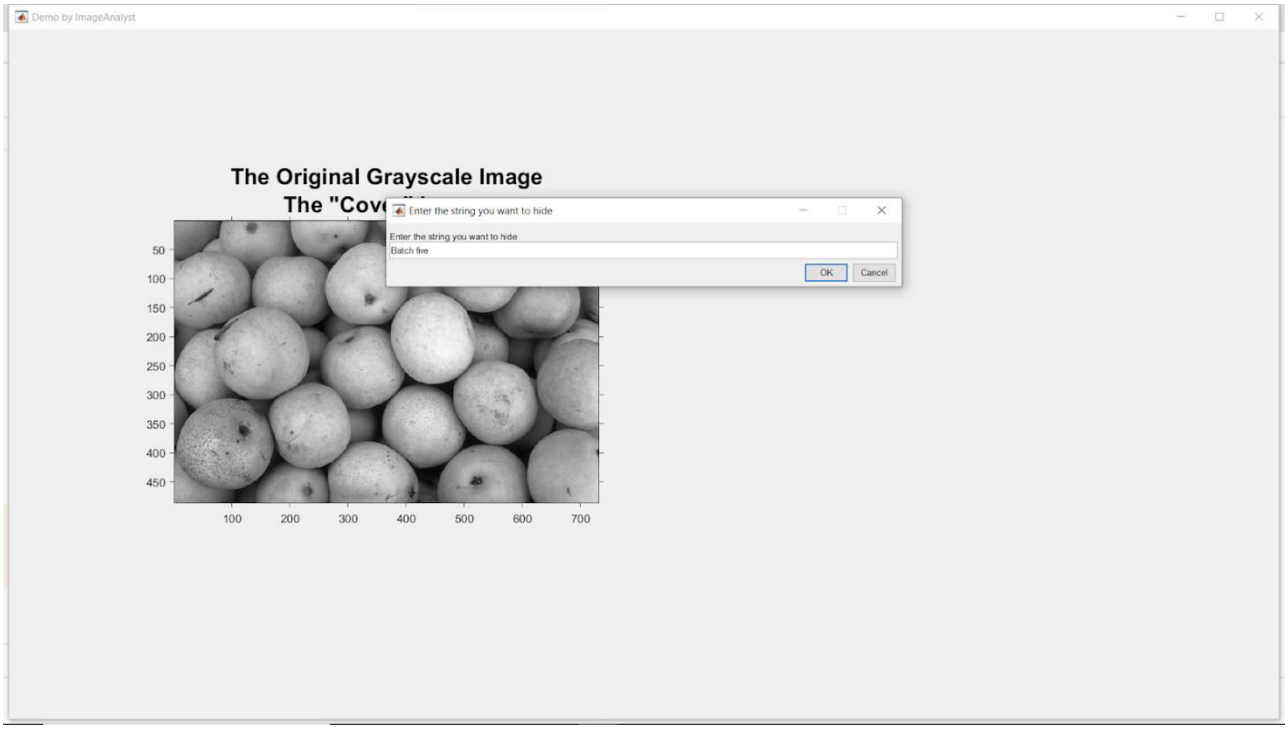

Figure 4. Select the image and add the text

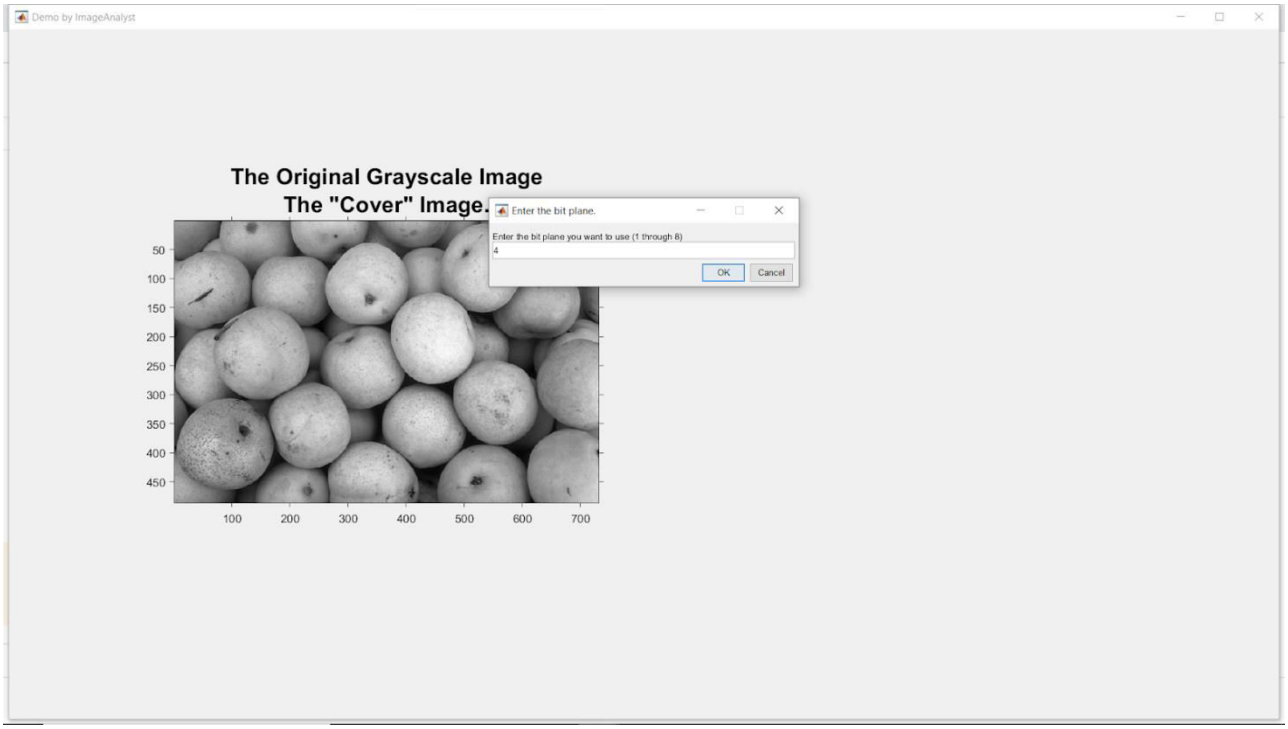

Figure 5. Select the Bit planenumber

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

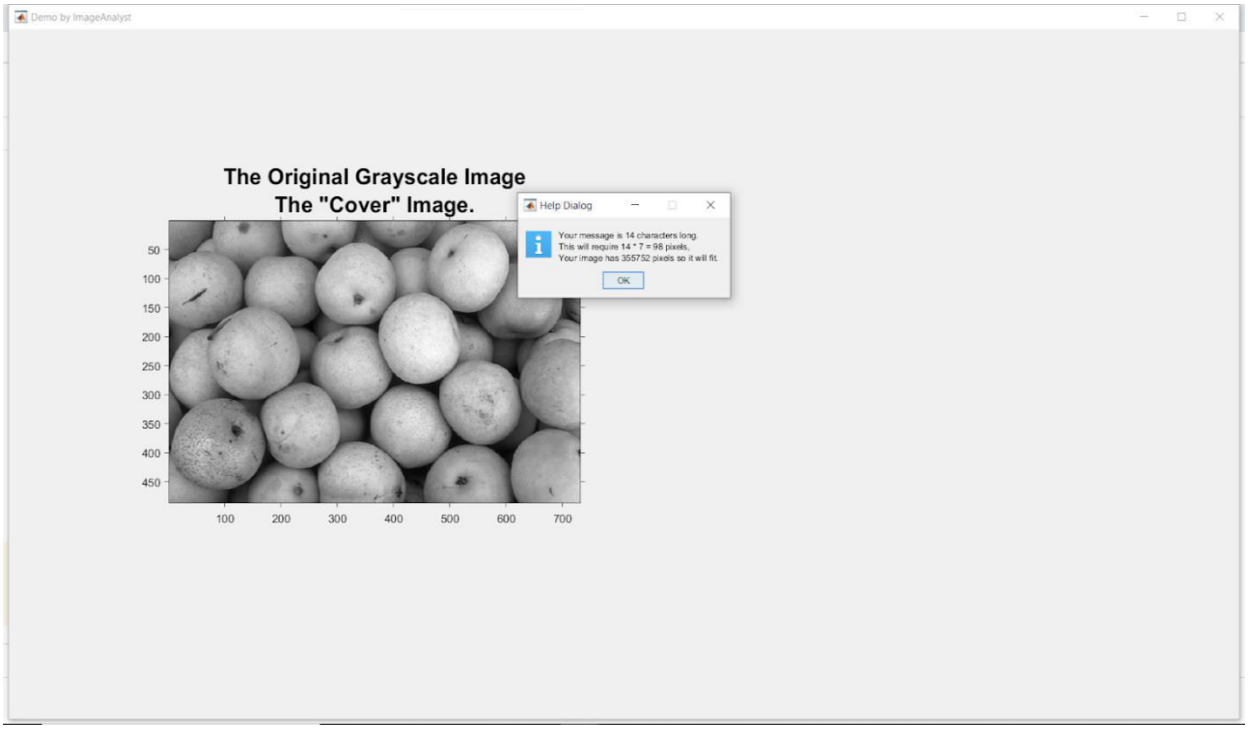

Figure 6. Calculate the number of pixels required

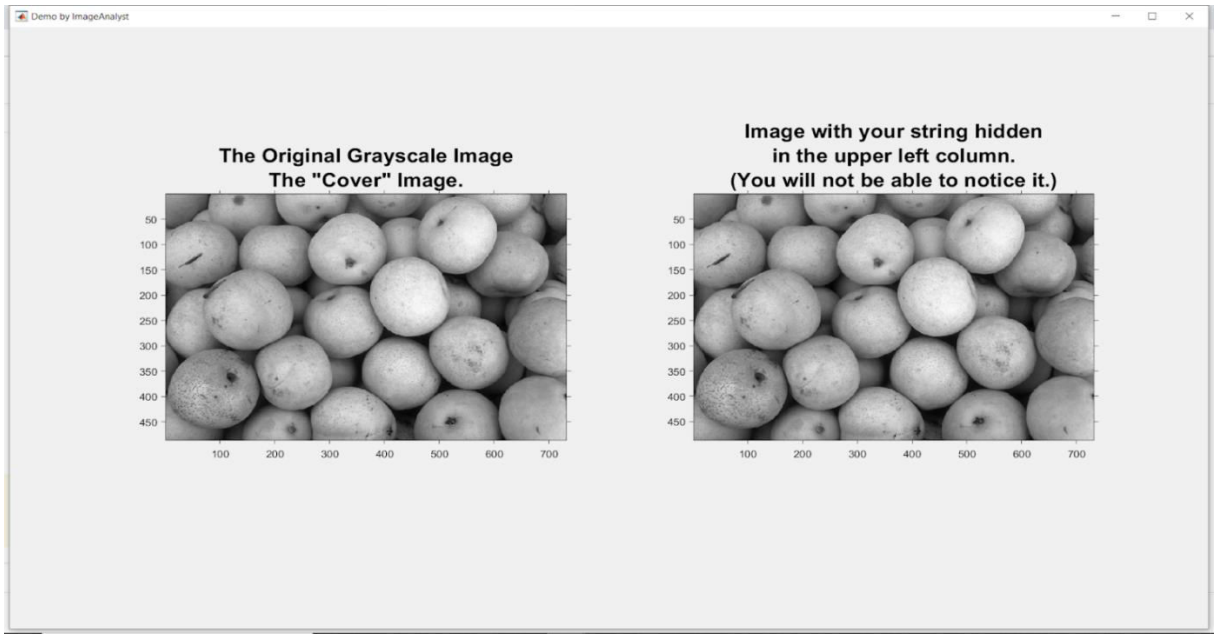

Figure 7.Calculate the number of pixels required

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

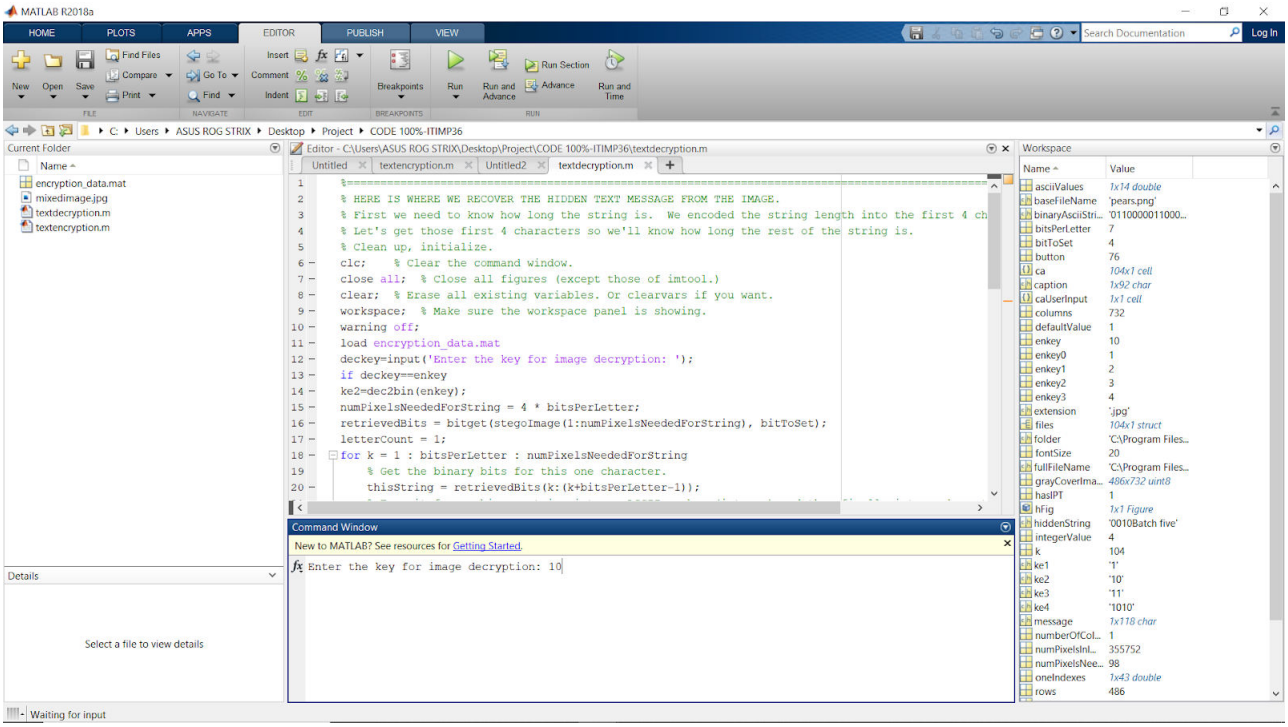

Figure 8.Enter the key for decryption

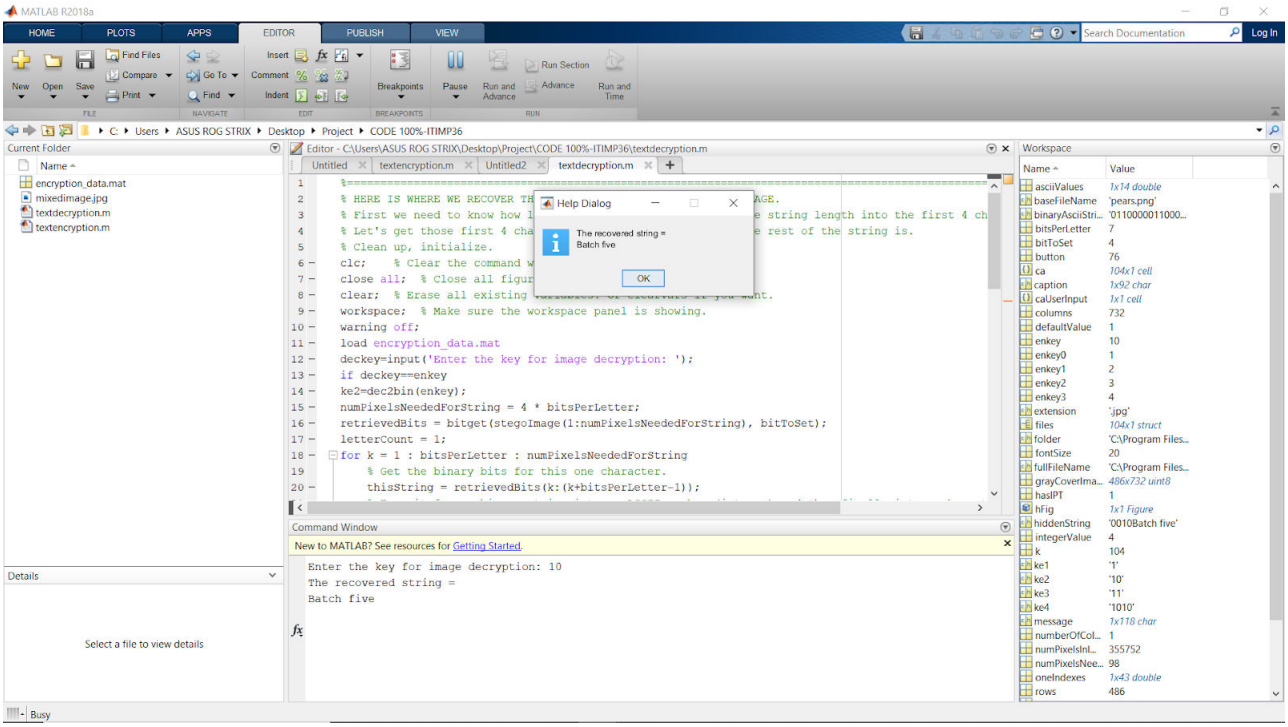

Figure 9.Decrypt the hidden message

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007296 |

IV. CONCLUSION

This paper proposed a novel image encryption algorithm integrating the bit-level permutation with three-bit plane decomposition technologies: binary bit plane decomposition, Gray code bit plane decomposition bit plane decomposition. each position of the LSBs plane with the corresponding position in the MSBs plane to reduce the correlation among neighboring pixels of the plain-text. The proposed algorithm uses a bit plane of a source image as the security key bit plane for protecting image contents. It has potential applications for multimedia communications.

REFERENCES

[1] Nidaa Abdul Mohsin Abbas,“ Image encryption based on Independent Component Analysis and Arnold’s Cat Map.” ,Received 27 May 2015; revised 3 October 2015; accepted 16 October2015, University of Babylon, College of IT, Iraq.

[2] DalelBouslimi, Member, IEEE, GouenouCoatrieux, Member, IEEE, Michel Cozic, and Christian Roux, Fellow, IEEE., “A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images”, VOL. 16, NO. 5, SEPTEMBER 2012.

[3] Hussain Nyeem1, Wageeh Boles2 and Colin Boyd2,3., Nyeem et al, “Digitalimagewatermarking:itsformalmodel,fundamentalpropertiesandpossible attacks.”, EURASIP Journal on Advances in Signal Processing 2014,2014:135.

[4] Shabir A. Parah1 · Javaid A. Sheikh1 · Umer I. Assad2 · Ghulam M. Bhat1., “Hiding in encrypted images: a three tier security data hiding technique”, Received: 19 August 2014 / Revised: 13 August 2015 / Accepted: 27 August2015.

[5] H.-C. Lin, C.-N. Yang, C.-S. Laih, and H.-T. Lin, ``Natural language letter based visualcryptographyscheme,"J.Vis.Commun.ImageRepresent.,vol.24,no.3,pp. 318331,2013.

[6] S.A. Sattar, S. Haque, M. K. Pathan, and Q. Gee, ``Implementation challenges for Nastaliq character recognition," in Proc. Int. Multi Topic Conf. Berlin, Germany: Springer, 2008, pp.279285.

[7] R. G. Sharma, ``Visual cryptographic techniques for secret image sharing: A review," Inf. Secur. J., Global Perspective, vol. 27, nos. 56, pp. 241259, Jan. 2019. doi:10.1080/19393555.2019.1567872.

[8] J.NantelandE.Glaser,``Theimpactoflanguageandcultureonper-ceivedwebsite usability," J. Eng. Technol. Manage., vol. 25, nos. 12, pp. 112122,2008.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details