iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6142

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: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Data Security by using Binary Bit Planes for Encryption and Inverted Bit LSB Substitution Technique for Hiding

Prof. D.V.R. Mohan[1], B. Chandra Babu[2]
[1,2]*ECE Department, S R K R Engineering College, Bhimavaram, A.P, India*

Abstract: ***The art of sending secret information from sender to receiver plays a prominent role in information security. In recent times, internet plays a major role in transferring digital multimedia data. But the main drawback by using the internet is, information security is less due to the increasing usage of internet. For information security many data hiding methods exists. One such method or technique is LSB technique. In this paper information can be hidden in LSBs of the cover image. In this method a modification to the LSB technique is proposed which is based on the 2nd and 3rd LSBs of cover image. It means there will be an inversion in the LSB bit of cover image based on the pattern of 2nd and 3rd LSBs of cover image i.e. (00, 01, 10 and 11). So this will be an advancement to the LSB technique. In this paper it is proposed for grayscale image. Encryption is also applied for the message image for providing extra security to the secret message. The encryption done here is by using binary bit plane scrambling and XOR. So that there will be dual layer protection to the secret message or information.***
Keywords: ***Encryption, Decryption, Least Significant Bit (LSB), PSNR, MSE, Histogram.***

I. INTRODUCTION

Information security plays a major role in today's world. Since the rise of using the internet, the amount of information security is decreasing rapidly due to the availability of internet to every person. So by using the internet, data security becoming very less. This can be overcome by using data hiding or encryption techniques. Data hiding or information hiding can be done for security reasons [1]. The secret information can be sent from sender to receiver by using cover objects. These cover objects may be text, image, audio, video. For hiding in images, the cover object is an image. Hiding data in images produces the stego image as output. For hiding data in images there are various techniques exists. Data hiding refers to hiding some valid information in cover object whereas the encryption itself scrambles the original data. This means by using data hiding the secret message cannot be visible to anyone or unauthorised user must not suspect the secret message whereas in encryption the secret message is scrambled so the message is visible i.e. unauthorized user knows that the encryption is applied and he tries to decrypt it. By applying both steganography and cryptography there will be dual layer protection to the secret message. Encryption means converting the message into a different form to make the secret message from unauthorised attacks [2]. Image encryption is of two types, position permutation and value transformation. In the position permutation, without changing the pixel value of original image permute image position. In value transformation technique without changing the position the pixel values are replaced by another pixel values.

The sections to follow are section II describes the image encryption and section III will give the implementation of proposed method Section IV illustrates the results and the conclusion is given in section V.

II. ENCRYPTION USING BINARY BIT PLANE SCRAMBLING AND XOR

Encryption is the process of writing a message which cannot be understood by anyone without decrypting it. For encryption a key must be used. The person with this key can decrypt it. In this paper, a simple encryption is done on images it is based on binary bit plane slicing and XOR. The original image is decomposed into bit planes first i.e. eight bit planes because of grey scale image and then these bit planes are permutated. The next step is to XOR these bit planes with key image bit plane to obtain encrypted bit planes. Here key image bit plane 4 is used. The encrypted image is obtained by combining these bit planes [3] [4].

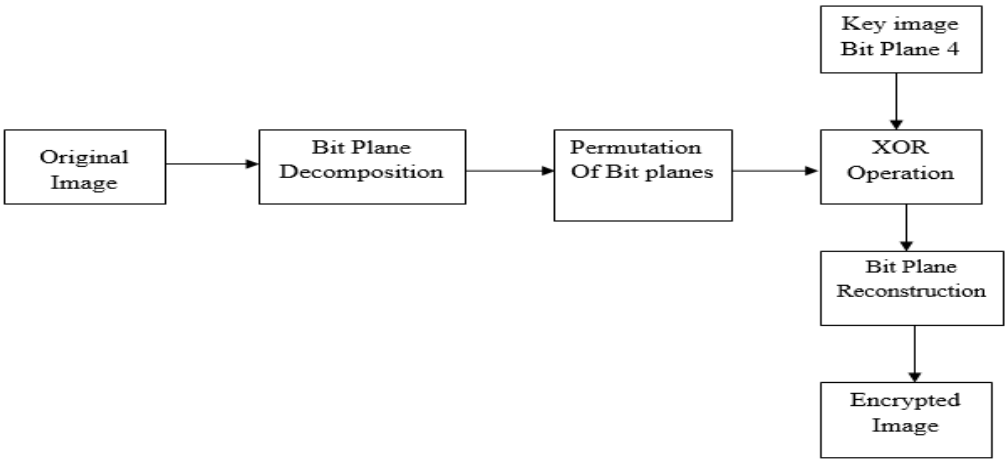


Fig. 1 At the sender side

At the receiver side the encrypted image is decomposed into bit planes first and then XOR with key image bit plane 4 which is used at the sender. These bit planes are then permutated. The original image is obtained by combining these bit planes.

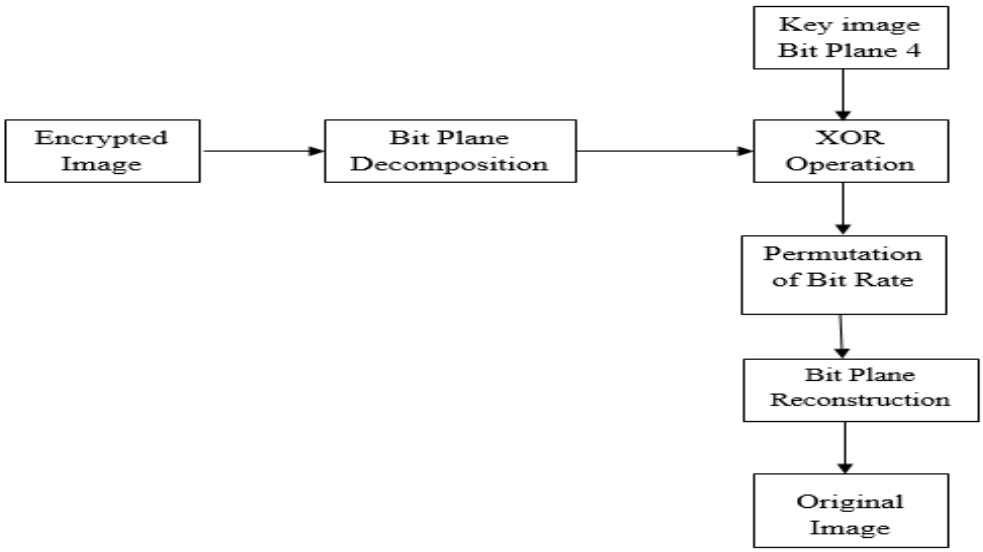


Fig. 2 At the receiver side

III.IMPLEMENTATION

A. Simple LSB Technique

The 8th bit or in other words LSB of all the pixels inside an image with 8 bit depth is changed to a bit of the secret information. Let us consider an example, in this only four pixels are used and the four message bits are 1 0 1 0 as follows

11111010 01101011 11100011 10110101

These are the cover image pixels. The message bits are directly embedded into these pixels.

11111011 01101010 11100011 10110100

It is a spatial domain technique which means the pixel values are directly modified [5].

B. Inverted LSB Technique

In this the LSBs are inverted based on the other bits of the cover image. In this also LSBs are directly embedding but after embedding the LSB inversion is implemented based on the other combination of cover image pixel bits. By using this technique

there will be an increase in the PSNR and decrease in the MSE values. In this the 2nd and 3rd LSBs are taken as combination. In this two bit combination is used so we have four patterns (00, 01, 10 and 11).

After applying LSB: 11111011 01101010 11100011 10110100 out of four three are with 10 (2nd and 3rd) pattern. In these three patterns only one LSB is unchanged and by observing the above example the changed LSBs count is greater than unchanged so invert the LSBs of pattern 10.

After inversion: 11111010 01101011 11100010 10110100 and if we consider more number of pixels i.e. an image contains more number of pixels, then changed LSB and unchanged LSB of particular patterns are observed. If changed LSB count of particular pattern is greater than unchanged LSB count then invert all LSBs of particular pattern to get the pixel benefit [6] [7]. For the receiver to correctly extract the message these counter values may be sent to the receiver using XOR encryption before sending the stego image.

IV. RESULTS

A. *Correlation of Adjacent Pixels*

The correlation of adjacent pixels in an encrypted image can be evaluated by using the equation

$$Cov(m,n) = E(m - E(m))(k - E(k))$$

$$r_{mn} = \frac{Covm(m,n)}{\sqrt{\text{var}(m)}\sqrt{\text{var}(n)}}$$

Here m and n are adjacent pixel grey levels.

B. *Differential Analysis*

The main aim of all encryption methods is that the encrypted image and secret image or original image difference should be high. Two metrics used to calculate these requirements are NPCR and UACI.

NPCR (number of pixel change rate) gives the number of pixels which are different in grey levels in two images. Let C (m,n) and C'(m,n) be the mth row and nth column of pixel of two images.

$$NPCR = \frac{\sum_{m,n} B(m,n)}{N} \times 100$$

Here N is the number of pixels in the image.

D (m,n) is defined as

$$D(m,n) = \begin{cases} 0 & C(m,n) = C'(m,n) \\ 1 & C(m,n) \neq C'(m,n) \end{cases}$$

UACI (Unified average changing rate) which gives the average difference in intensity of encrypted and original images

$$UACI = \frac{1}{N}\left[\sum_{m,n}\frac{|C(m,n) - C'(m,n)|}{255}\right] X 100$$

C. *Image Quality Metrics*

Two other image quality metrics used when hiding data in images are PSNR and MSE.

$$PSNR = 10X \log_{10}\left[\frac{h^2}{MSE}\right]$$

$$MSE = \frac{1}{XY}\sum_{m=1}^{M}\sum_{n=1}^{N}\left[C_{org}(m,n) - C_{enc}(m,n)\right]^2$$

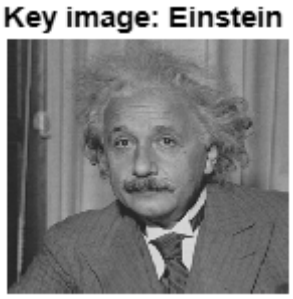


Fig. 3 key image bitplane

Fig. 4 Key image bitpalne 4

Fig. 5 Secret image

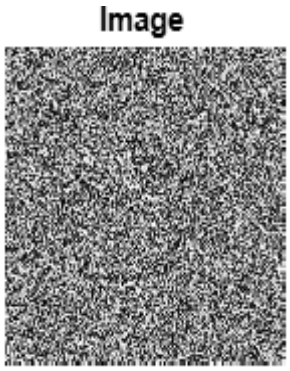


Fig. 6 Encrypted image

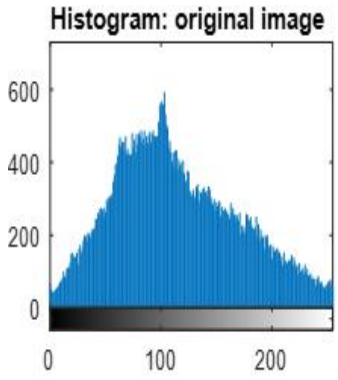


Fig. 7 Histogram of secret image

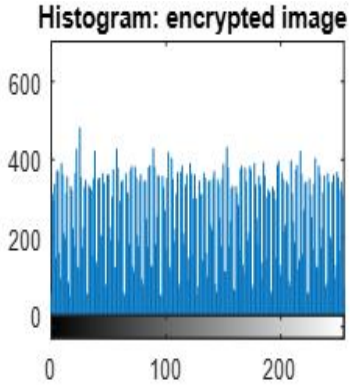


Fig. 8 Histogram of encrypted image

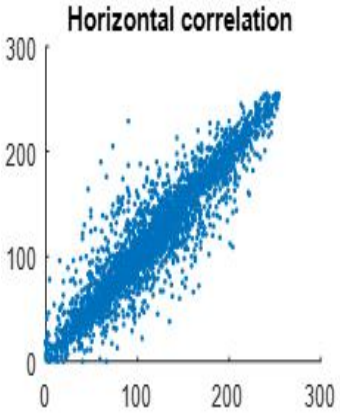


Fig. 9 Horizontal correlation of secret image

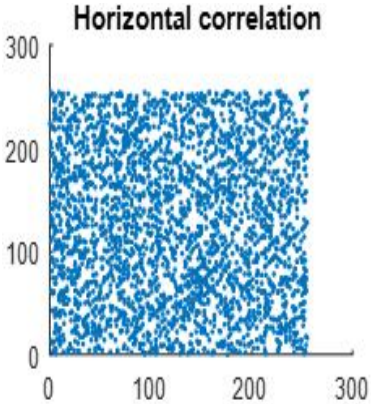


Fig. 10 Horizontal correlation of secret image

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

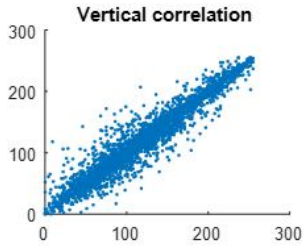


Fig. 11 Vertical correlation of encrypted image

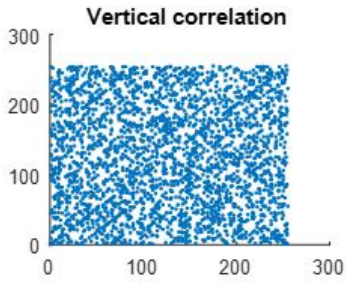


Fig. 12 Vertical correlation of encrypted image

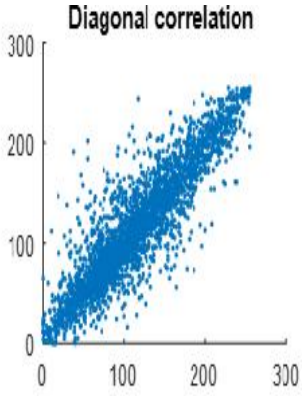


Fig. 13 Diagnonal correlation of secret image

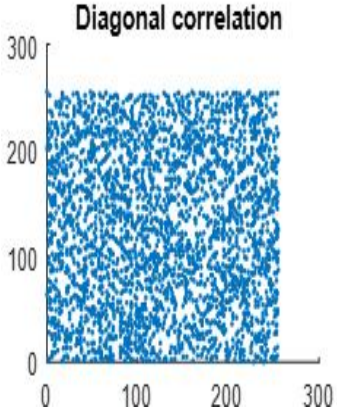


Fig. 14 Diagnonal correlation of encrypted image

Fig. 15 Cover image

fig. 16 Stego image (Inverted LSB)

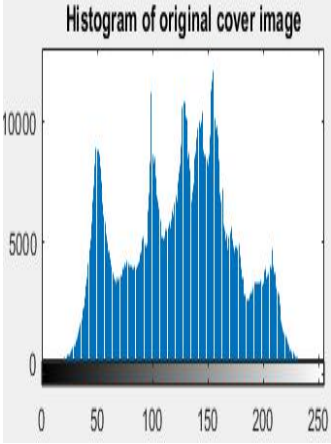


Fig. 17 Histogram of cover image

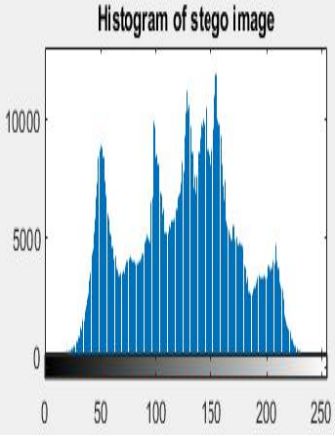


fig. 18 Histogram of stego (Inverted LSB)

Fig.19 Stego image (Simple LSB)

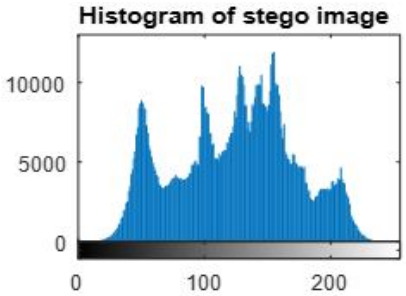


Fig. 20 Histogram of stego (Simple LSB)

The experimental results for bird secret message when encrypted is shown in figures 5-14. And the key image is Einstein image and its bit palne 4 are shown in figures 3 and 4. The image after embedding the secret message i.e encrypted secret message in the Lena cover image produces the stego images and it is observed for simple LSB and Inverted LSB and their corresponding stego images are shown from figures 15-20.

TABLE I. FOR CORRELATION OF ADJACENT PIXELS

Secret image		Correlation of Secret Image	Correlation of Encrypted Image
Bird	Horizontal	0.9372	-0.0050
	Vertical	0.9536	-6.257*e^-4
	Diagonal	0.9079	0.0037

TABLE II. FOR UACI AND NPCR VALUES

Secret image	UACI	NPCR
Bird	12.5135	93.6630

TABLE III. FOR PSNR AND MSE VALUES FOR INVERTED LSB TECHNIQUE AND SIMPLE LSB

Cover Image 1024x1024	Message Image 256x256	Simple LSB		Inversion based on two bits(2nd and 3rd LSBs of cover image)	
		PSNR	MSE	PSNR	MSE
Lena	Bird	53.7961	0.2504	53.8055	0.2499
	Cartoon	53.8009	0.2502	53.8089	0.2497

The correlation coefficients are shown in table I for Bird secret message and UACI, NPCR values are given in table II. The peak signal to noise ratio and mean square error values are tabulated in table III. From this there will be slight increase in the PSNR and decrease in the MSE values for inverted LSB technique than Simple LSB. The experiment is executed by using MATLAB R2016a.

V. CONCLUSIONS

In this paper, dual layer protection is provided for secret information. In this inverted LSB technique PSNR is slightly greater than the simple LSB. And also the security is more in inverted LSB technique than LSB because the LSBs are inverted based on other bits of cover image. Here 7 bits are there leaving the LSB. We can choose any 2 bits out of 7 in 7c2 ways. So 21 combinations have to check and if the attacker wants to extract the message. It is quite difficult to know which LSB is inverted. Encryption using bit plane scrambling combined with XOR is simple and efficient.

REFERENCES

[1] Sukhjinder Singh, Kulbhushan Singla, Dr. Rahul Malhotra, "A Robust Image Steganography Technique Using Quantized Range Table And Local Area Pixel Value Differencing," International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 5, Issue 2, February 2016.

[2] Dr. P. V. Ramaraju, G. Naga Raju, P. Rama krishna, "Image Encryption After Hiding (IEAH) Technique For Color Images," International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.

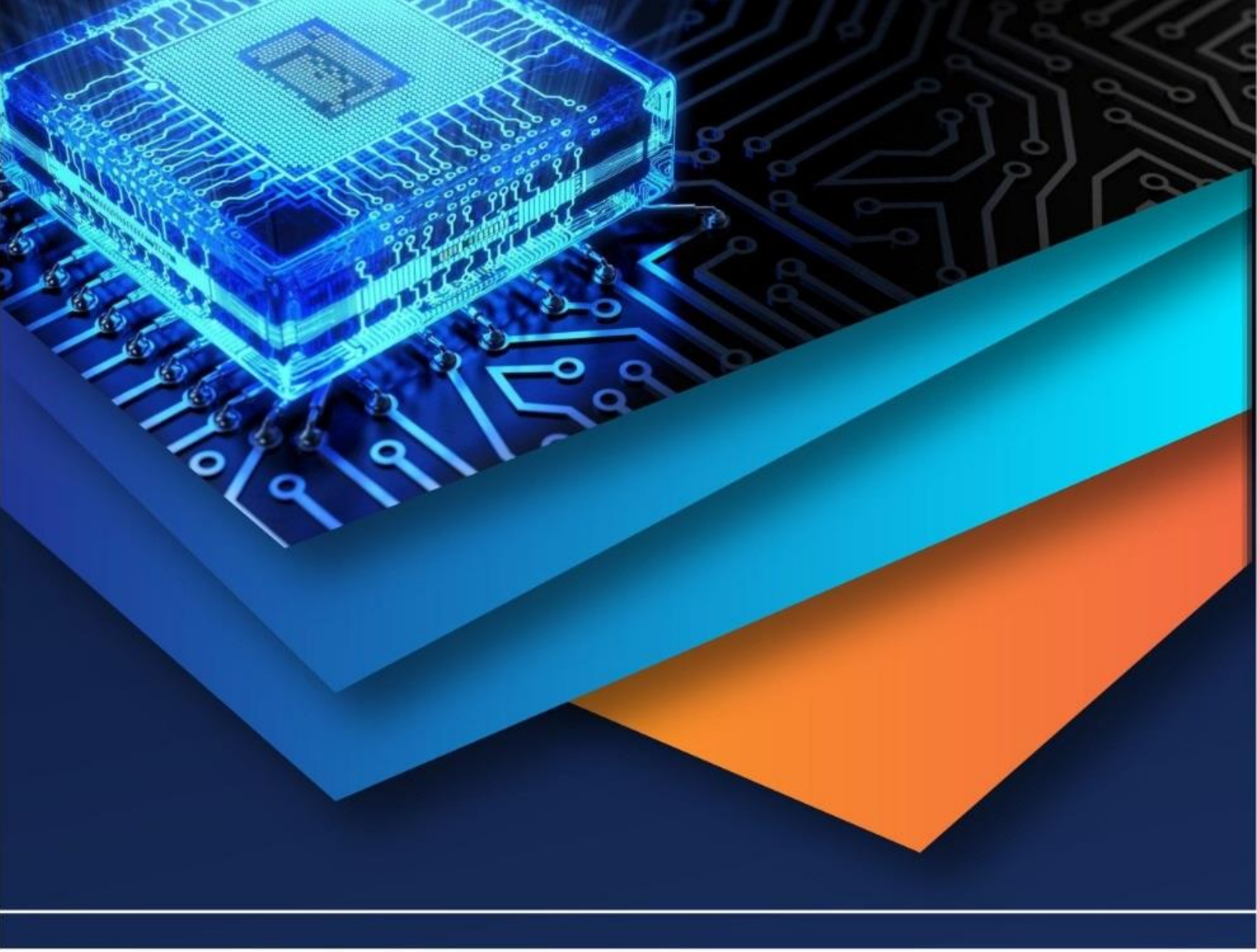
[3] R.Aarthi, Mrs. S.Kavitha, "image encryption using binary bit plane and rotation method for an image security," International Journal of Engineering Development and Research© 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.

[4] R. Vijayaraghavan, S. Sathya and N. R. Raajan, "Security for an Image using Bit-slice Rotation Method–image Encryption," Indian Journal of Science and Technology, Vol 7(4S), 1–7, April 2014.

[5] Varsha and Rajender Singh Chhillar, Ph.D " Data Hiding using Advanced LSB with RSA Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 122 – No.4, July 2015

[6] Nadeem Akhtar, Shahbaaz Khan, Pragati Johri, "An Improved Inverted LSB Image Steganography," 978-1-4799-2900-9/14/$31.00 ©2014 IEEE.

[7] Rupali Bhardwaj, Vaishali Sharma, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution," 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY