iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49467

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: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Designing an Image Encryption user Interface System

Shubham Tiwari[1], Harsh Rathore[2], Rushikesh Salunkhe[2], Neha Thakare[3]
[1, 2, 3, 4]*Electronics and Telecommunication Engineering Ramrao Adik Institute of Technology Mumbai, India*

Abstract: ***"Designing an Image Encryption user Interface using Python and Octave" Data Security has become the paramount in most industries right this moment, especially true in the finance and banking industry. What we have created here is a user interface that lets you add a blur to your image and protect it with a password. We are also using steganography to add to hide a recognition key in the image. The password for the image (taken in as input from the user) and the hidden key into image are then updated in SQL data base. The interface also lets you decrypt any image that was earlier encrypted using program, this is done by initially finding the hidden code in encrypted image then checking it with the keys in the data base if matched the user is asked for a password, the password then entered by the user is checked with password saved for the given key if the image is decrypted. A graphic interface is then created using the tkinter python library for the front end and our encryption code being at the backend. Now let's understand how the encryption is takes place, basically we are using the octave library in python3 to add Gaussian blur to the image. Mathematically the adding Gaussian blur the image is the same as convolving the image with a Gaussian Function. The Gaussian blur is a form of photo-blurring filter that uses a Gaussian feature (which additionally expresses the normal distribution in facts) for calculating the transformation to apply to every pixel within the image.***
Keywords: Image Encryption, Image Security, Steganography, Python, Gaussian Blur.

I. INTRODUCTION

Data is considered by many as the modern equivalent of gold, we as engineers there need to find solutions to protect data, while many image encryption platforms do exist what we plan on creating is a multi-platform interface using which data can be easily encrypted on any of the existing operating systems and platforms (let it be phone, windows or the Mackintosh OS).

Our project is a GUI interface that uses a combination of Gaussian blur and steganography to add a layer of blur on the given image. We are using python programming language and its various image processing/computer vision library.

Encryption is the process of obtaining digital data using one or more mathematical methods, as well as the password or "key" used to clear encryption. The encryption process translates information using an algorithm that makes real information unreadable. The process, for example, can convert the original text, known as abstract text, into another form known as ciphertext. If the authorized user needs to read the data, they may remove the encryption data using the binary key. This will convert ciphertext into plain text so that the authorized user can access the actual information.

Likewise, Image Encryption is the process of encoding secret image with the help of some encryption algorithm in such a way that unauthorized users can't access it.

Image Encryption works on the modern idea of taking the consecutive or random pixel bits of an image and collectively set of latest pixels, that is typical form the original bits.

Image Steganography refers to the method of hiding records inside a picture report. The image selected for this motive is known as the cover image and the image obtained after steganography is known as the stego image.

II. PROPOSED METHOD

Our method works on the basis of Gaussian blur and steganography to password protect image and add a layer of blur on them.

A. Gaussian Blur

A Gaussian Blur (also known as Gaussian smoothing) is the result of blurring an image by a Gaussian Filter. The Gaussian blur is used for calculating the transformation to apply to each pixel in the image. The formula of a Gaussian function in one dimension is

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$$

©IJRASET: All Rights are Reserved

In two dimensions, it is the product of two such Gaussian functions, one in each dimension:

$$G(x) = \frac{1}{2\pi\sigma^2} e - \frac{x^2 + y^2}{2\sigma^2}$$

Where x is the distance from the origin in the horizontal axis, y is the distance from the origin in vertical axis, and σ is the standard deviation of the Gaussian distribution.

The image is first selected by the user and the user is also asked to enter a password which is then hidden in the image using steganography after this the image is then uploaded to a secure data base and after that Gaussian blur is added to the image.

For Decryption, the encrypted image selected by the user is checked for the message, the user is then asked to enter the password which is matched with message and if it is correct the original image is retrieved from the database.

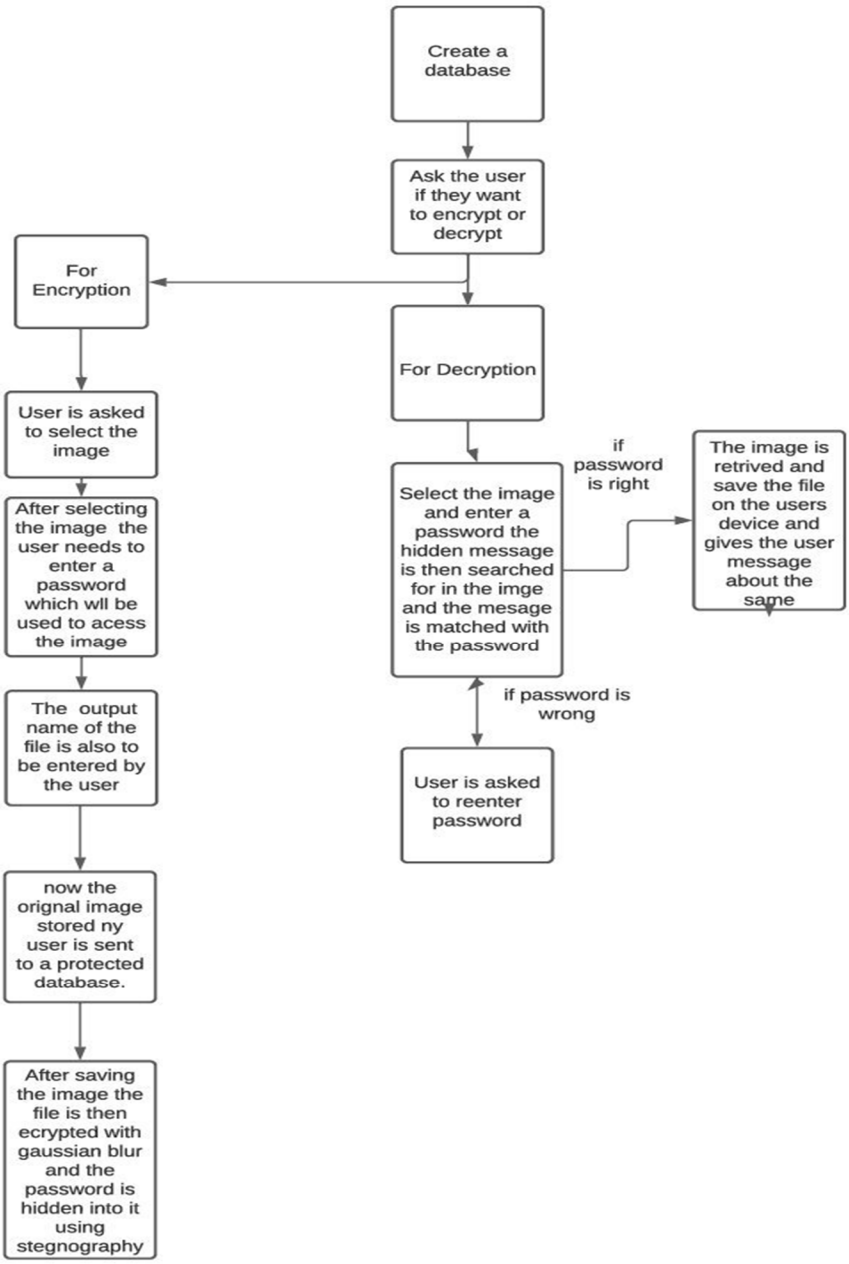


Fig. 1: BLOCK DIAGRAM FOR PROPOSED METHOD

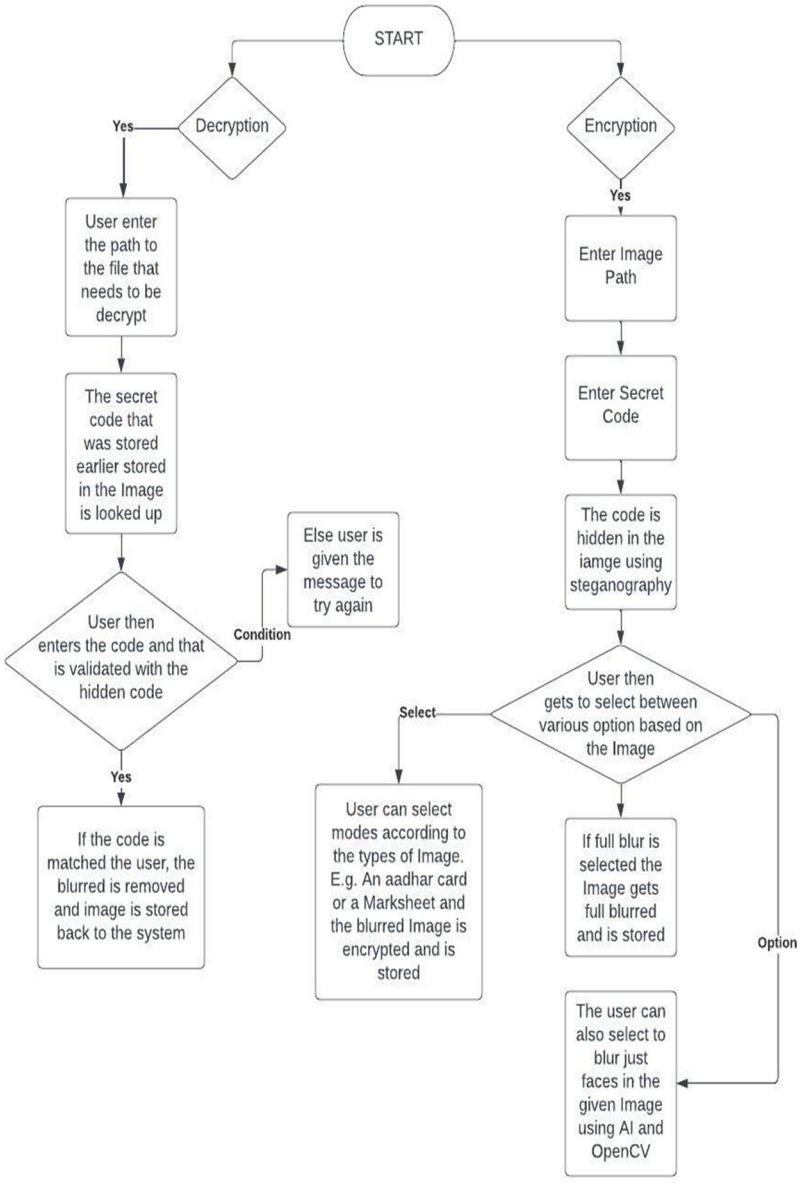


Fig. 2: FLOWCHART OF PROPOSED METHOD

B. To change the strength values, we subtract nits in a certain order and convert the appropriate decimal values. Then in the converted matrix we use the steganography algorithm with a secret key. To increase the complexity and security of the algorithm we also complement the strength values (Gaussian Blur). The algorithm is described below in steps. A plan diagram for this study is provided in Fig. 1 and the flowchart is given in Fig. 2.

C. Encryption Algorithm

1) Read image size 256 x 256
2) Generate a random key for a private image
3) Rotate this animated key left or right keystrokes, the user only defines this key
4) Turn this rounded image into a binary
5) Then shuffle each bit to every binary image pixel and match it
6) Apply steganography techniques to the effect of a sharp image with its keys

7) Then convert each pixel into a decimal again
8) Save the resulting image as an encrypted image on the website

D. Decryption algorithm
1) Read the enclosed image
2) Rotate the enclosed image in the opposite direction in the encoding process
3) Enter steganography by key and turn it into binary
4) Enter a key to the picture
5) Save the resulting image as the original image

III. RESULT ANALYSIS

For analysis, Random pictures of different sizes were taken. Code coded with Python. They are shown Fig. 3-5. In addition to the actual image, the resulting images are also displayed. Histograms are also provided in all images for better understanding.

With regard to random consideration, no third party can associate the result with the first. There is not even one thing related to the two pictures. The image is reproduced twice; cryptanalysis is only possible if the attacker is aware of the tactics followed. Thus, the output does not give an indication of the actual parts of the image or its pattern Histograms can also be investigated for image encryption. Clear in the first and hidden images, the histogram follows the pattern; with a crucified version the case is flat. Therefore, the algorithm is usually tested based on frequencies. To prevent attacks, the need for separate histograms is important. The pattern is spiky and has a significant increase and decrease in the first three, and in exit, the separation will not be done as there are no complete variations.

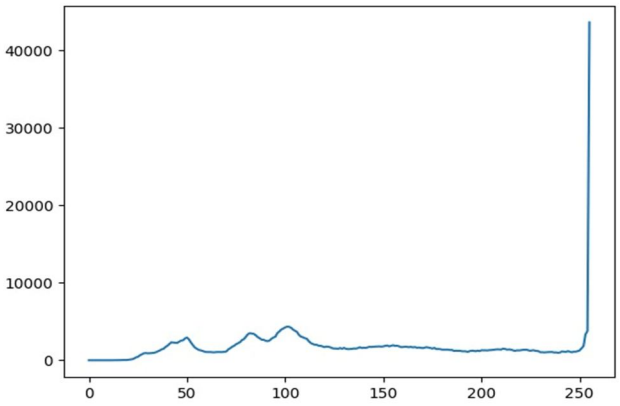
Pixel connections are very important in every way as even a small index can be very helpful in clearing the encryption. Demonstrates algorithm performance.



(a)



(b)



(c)

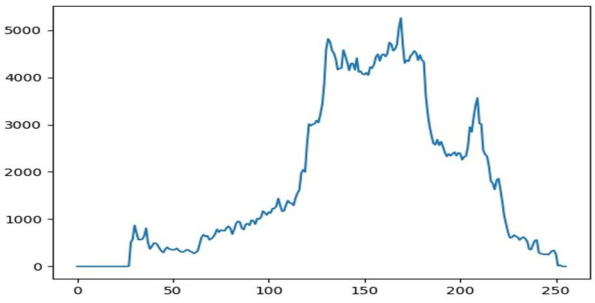
Fig. 3 Face (a) Secret image, (b) Encrypted image Histogram of (c) Encrypted image



(a)

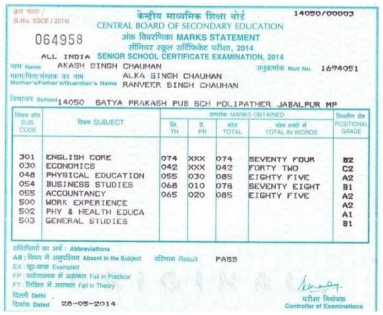


(b)



(c)

Fig. 4 Variable (a) Secret image, (b) Encrypted image Histogram of (c) Encrypted image


केन्द्रीय माध्यमिक शिक्षा बोर्ड 14050/00003
CENTRAL BOARD OF SECONDARY EDUCATION
064958
अंक विवरणिका MARKS STATEMENT
ALL INDIA SENIOR SCHOOL CERTIFICATE EXAMINATION, 2014
AKASH SINGH CHAUHAN
ALKA SINGH CHAUHAN
RANVEER SINGH CHAUHAN
14050 SATYA PRAKASH PUB SCH POLIPATHER JABALPUR MP

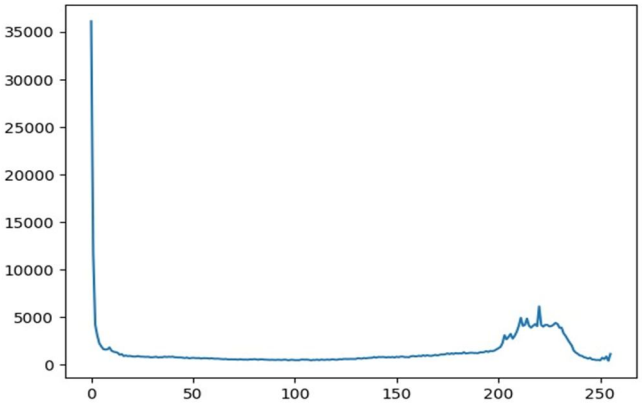
SUB. CODE	SUBJECT	TH	PR	TOTAL	TOTAL IN WORDS	GRADE
301	ENGLISH CORE	074	XXX	074	SEVENTY FOUR	B2
030	ECONOMICS	042	XXX	042	FORTY TWO	C2
048	PHYSICAL EDUCATION	055	030	085	EIGHTY FIVE	A2
054	BUSINESS STUDIES	068	010	078	SEVENTY EIGHT	B1
055	ACCOUNTANCY	065	020	085	EIGHTY FIVE	A2
590	WORK EXPERIENCE					A2
502	PHY & HEALTH EDUCA					A1
503	GENERAL STUDIES					B1

परिणाम Result PASS
28-05-2014

(a)


केन्द्रीय माध्यमिक शिक्षा बोर्ड 14050/00003
CENTRAL BOARD OF SECONDARY EDUCATION
064958
अंक विवरणिका MARKS STATEMENT
ALL INDIA SENIOR SCHOOL CERTIFICATE EXAMINATION, 2014
AKASH SINGH CHAUHAN
ALKA SINGH CHAUHAN
RANVEER SINGH CHAUHAN
14050 SATYA PRAKASH PUB SCH POLIPATHER JABALPUR MP
28-05-2014

(b)



(c)

Fig. 5 Marksheet (a) Secret image, (b) Encrypted image Histogram of (c) Encrypted image

Safety is the main challenge and is measured by using differential assault. A small alternate in pixel price can give deviated end result which cannot be termed as a great encryption.

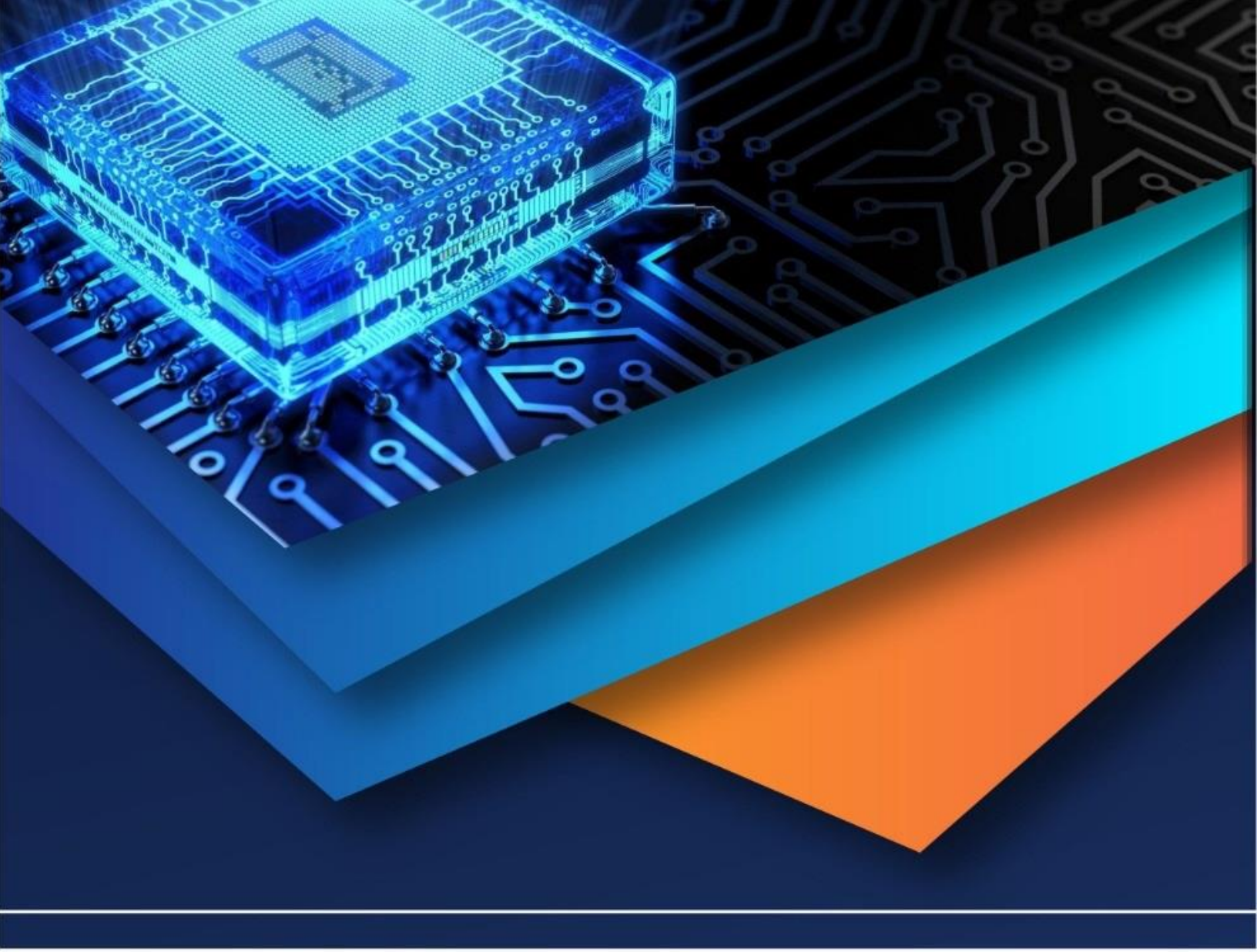
Because of added blur we can clearly observe the luminosity in the output images change significantly due to the added blur. And the lack of visibility of details in the image is caused by this.

IV. CONCLUSION

In the field of information security, growth plays a major role, growth means change, change begins when you think of a new concept. In this study, we introduce one in the field of information security under the topic of image encryption. Image encryption can be defined in the form of an encrypted image encoding process with the help of a specific encryption algorithm in such a way that unauthorized users can't access it. The process, although sound complex, is very effective and easy to use as an additional feather that benefits the image encryption with steganography. The image with the encryption data is completely distorted or obscure, the end result is, stego can be further modified with the help of a key to portray an excellent image of a hacker who, when scrutinized in depth, leaves no trace of the randomization presented in the image

REFERENCES

[1] Narasimhan Aarthie and Rengarajan Amirtharajan, 2014. Image Encryption: An Information Security Perceptive. Journal of Artificial Intelligence, 7: 123-135.
[2] Rengarajan Amirtharajan, P. Archana and J.B.B. Rayappan, 2013. Why Image Encryption for Better Steganography. Research Journal of Information Technology, 5: 341-351.
[3] Rengarajan Amirtharajan, Jiaohua Qin and John Bosco Balaguru Rayappan, 2012. Random Image Steganography and Steganalysis: Present Status and Future Directions. Information Technology Journal, 11: 566-576.
[4] Wolfram Research(2008), GaussianFilter, Wolfram Language function, https://reference.wolfram.com/language/ref /Gaussian Filter.html (updated 2016)
[5] https://doi.org/10.1016/j.patcog.2020.107264



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)