iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35792

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: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Improved Algorithm of Steganography Combined with Cryptography

Anees Banu[1], CH. Satya Kavya[2], V. Kiranmayee[3], Dr. Chatopadhyay[4]
[1, 2, 3, 4]*Department Electronics and communication Engg, Sreenidhi Institute of science and technology ,Ghatkesar, Hyderabad*

Abstract: ***When it comes to preventing unauthorised access to, destruction of, or inspection of confidential data, information security has always been a major factor. Multimedia information is now used in every field throughout the world. The confidential information that is used in these areas must be kept secure. There are a variety of methods for keeping data secure. One of these is steganography, which is concealing information within other data into a format that the cover information remains unchanged. Cryptography, an encryption process that scrambles data into a written form that is sometimes referred to as a hash, is an auxiliary approach for securing information. Steganography and cryptography each have their own set of benefits and drawbacks. Even though both technologies give security, it is usually a good practise to combine Cryptographic algorithms to create additional layers of security. When cryptographic with steganography are combined, a multi-layer security paradigm is created. The proposed work's main goal is to add an additional layer of protection by using cryptography and steganography to encrypt and embed secret data conveyed across an insecure channel.***

I. INTRODUCTION

There has been a gigantic improvement in the correspondence field in late time. Subsequently the security and secrecy of data has become an essential and significant necessity for correspondence. With the quick improvement of the Web and interactive media procedures, we utilize computerized information like writings, pictures, pictures, sounds in our everyday life. Immense data can be sent through PC organizations. Be that as it may, the security of information over the web isn't sufficient, and the information can be captured by an unlawful or unapproved client. Consequently guaranteeing the Security and Classification of information transmission is vital and current need. This necessity can be accomplished by various procedures like Steganography and Cryptography are identified rand generally utilized methods that control info or wrap their reality individually. Steganography is the craftsmanship and study of convey in a way which shrouds the existence of the restricted information. Anyway Cryptography scrambles information so it gets incomprehensible. Steganography conceals the restricted information with the goal that it can't be seen. Cryptography frameworks can be extensively characterized into two kinds. Symmetric-key frameworks in that a solitary key is utilized by , the sender and the beneficiary, and Public key frameworks in which two keys are utilized, a public key which is known to be everybody and also a private-key which is known uniquely to the beneficiary of messages.

In Cryptography, a code information may make doubt to the beneficiary while an undetectable message made with steganographic strategies won't. Steganography can be helpful when the utilization of cryptography is unsafe or disallowed. The investigation methods for unraveling figure messages is called as cryptanalysis and procedures for identifying covered up messages in the stego-media is called as steganalysis. The previous alludes to the arrangement of techniques for getting the importance of encoded data, while the last is the craft of finding secretive messages. This report is zeroing in on a strategy for joining together cryptography and steganography for pictures.

A. What Is Stegnography?

Steganography came to what in particular is presently the United States as ahead of schedule as the Revolutionary War, during which it appeared as mystery message drops, code words, and undetectable inks utilized for correspondences between General George Washington and a gathering of spies [Kipper04]. It proceeded being used through extra conflicts, including World War I and II. Following the awfulness of September 11, 2001, examinations uncovered that Al'Queda psychological militants may have sent pictures containing covered up messages through usenet. Proof exists fundamentally as Islamic radical sites that give data on the best way to insert information in pictures [Kipper04]. Despite the fact that the utilization of steganography in arranging 9/11 was not affirmed, the chance of its utilization started new interest in steganography, and prompted further examination into its utilization and its avoidance.

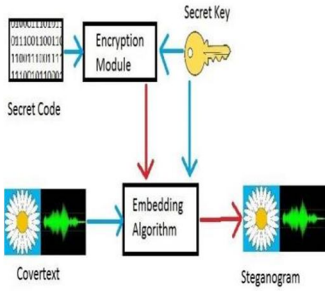


Fig 1.1:Block Diagram of basic Stegnography

II. WHAT IS CRPTOGRAPHY?

Cryptology is related with a way toward changed over conventional plain context into ambiguous context and the another way around. It is a way for keeping away and communicating inform in a defined structure so that solid those for which it is planned can be perused and deal with it. Cryptography wraps message from adjustment, however can like-wise be used for client validity. The prefix "grave " shows "covered up" or "vault" - and postfix "- graphy" means "composing."

A. Cryptography Methods

Current cryptography worries about the accompanying 4 destinations:

1) Classification: The data cannot be perceived by anybody accidentally
2) Uprightness: The data can be modified away and travel among senders and expected recipient with the modification identified
3) Non-disavowal: The sender of the data can deny in later stage aims in the creation of the data
4) Verification: The maker and collector can ask each others personality and the beginning/objective of the data.

Strategies or conventions that will meet a few or the entirety of the above measures are called as cryptosystem.

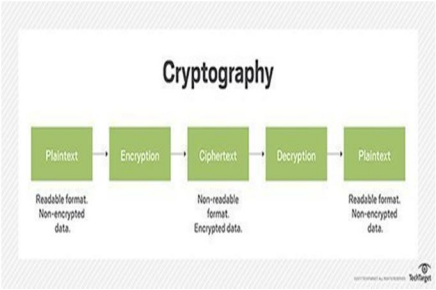


Fig 2: Basic Block Diagram of Cryptography

III. LITERATURE SURVEY

A. DCT was Joined with DWT.

Vijay Kumar and Dinesh Kumar el al (2010) introduced an advanced picture steganography strategy in which DCT was joined with DWT. The experimentation was finished utilizing various assaults. The outcomes show that PSNR esteem increment as contrast with past framework. The proposed strategy first concentrates the DCT coefficients of mystery picture by utilizing DCT procedure. From that point forward, picture highlights are removed from cover picture and from DCT coefficients by applying DWT method on both independently. This paper showed high vigor against many picture handling assaults.

B. LSB Benchmark Procedure.

Atallah M el al (2012) present Another Strategy in Picture Steganography with Improved Picture Quality. In which Steganography is word taken from the two Greek words as "steganos" and "graphie" which signify "disguised" and "stating" individually. Mutually it alluded as disguised (covered up or covered) the message. Different procedures are utilized with the end goal of picture steganography. In this paper the method utilized by the creator works by perceiving the comparable pieces among message and picture. The examination is finished by utilizing the LSB benchmark strategy.

C. AES Calculation

Md. Khalid, ImanRahmani and kamiyaarora, Naina Buddy el al (2014) presented the carefully signature strategy which carries out the confirmation, uprightness and non-renouncement and apply the AES calculation on carefully marked message to shape the scrambled message to executes the secrecy and fractional security. Insert that message into the picture with utilizing the LSB to deliver the stego picture.

D. DCT and LSB Strategy

Kamal and LovnisBansal el al (2014) utilized the mix of both DCT and LSB strategy utilizing 32*32 DCT division plan. In which RSA calculation utilized for execute the hilter kilter cryptography for better uprightness and for no deficiency of information and in which neural organizations are utilized for separate the information bits with least influencing the first examples of picture.

E. Hash – LSB with RSA Calculation and DWT Strategies

Nikita Sharma, Meha Khera el al (2015) present the Hash – LSB with RSA calculation and DWT strategies in consolidated structure, in which odds of safety as far as lesser perceptibility, and lesser bending in a picture would be more on the grounds that here the message is scrambled first prior to implanting into a picture.

F. Double Steganography

Prof Ms.Ashwini B. Akkawar, Prof. Komal B. Bijwe et al (2016) gave an audit [10] which analyze the strategies for double steganography alongside their solidarity and shortcomings. Initially, DES Encryption is utilized for Picture Steganography and afterward utilizing the LSB strategy and AES calculation for double security. At long last, steganography inside steganography methods utilized for conquer every one of the disadvantages of past once and bring about improved form of double steganography. They are utilizing the AES and DES calculation for encryption however there are more calculation accessible for security those gave the better exhibition as contrast with these calculation.

IV. PROBLEM FORMULATION

A. Existing System

Steganography might be a strategy to cover any sensibly documents into a conveying record. The work of the cover picture basically based steganography is extra qualified than various transmission records on account of its memory and size necessities. Pictures of square measure the placement of pic. Picture is partner degree electronic mechanism for the chronicle, reiteration and broadcasting of moving visual pictures. The normal number of still pictures per unit of season of picture is 24 casings each second.

In the event that an individual sends delicate data over the uncertain channels of the framework then there might be an opportunity of hacking it, they can adjust the data and sends it over the net. (Model is military people sending delicate data over the net.)This issue has been addressed by the proposed framework.

B. Hash-Based Least Significant Bit Technique For Image Steganography (Hlsb)

Steganography manage the concealing restricted information or data inside a picture. In this paper, a hash based least huge piece (LSB) procedure has been proposed. A spatial space method where the privileged data is inserted in the LSB of the cover outlines. Eight pieces of the privileged data is isolated into 3,3,2 and inserted into the RGB pixel upsides of the cover outlines individually. A hash work is utilized to choose the situation of inclusion in LSB bits. The proposed strategy is analyzed in terms of both Peak to the signal ratio (PSNR) contrasted with the first cover picture just as the Mean Square Blunder (MSE) estimated between the first and steganographic documents found the middle value of over all picture outlines. Picture Devotion (IF) is likewise estimated and the outcomes show insignificant debasement of the steganographic picture record. The implemented method is contrasted and existing LSB based steganography and the outcomes are discovered to be empowering. A gauge of the implanting limit of the procedure in the test picture record alongside a utilization of the proposed strategy has additionally been introduced.

C. Image Steganography by LSB Substitution Using Different Polynomial Equations

Steganography is strategy and specialty of concealing a mysterious message in transporter record so the presence of the mysterious messages can't be known. During the most recent couple of many years, there have been an enormous number of papers that generally distributed by all unique examination. On the off chance that anybody knew the presence of the mysterious message with its transporter record then steganography is fizzled. This paper will talk about the different kinds Expressions of steganography are separated into "stegos" and "grafia" which each has signified "cover" and "stating" join the word become "covered composition" .

D. Image Steganography through LSB Based Hybrid Approach

Steganography can be examined on picture record and information is disguised by a scrambled arrangement. The widely recognized procedure is least huge Bit steganography (LSB) .Movement location method is perhaps the main errands in the picture handling frameworks. It assists with separating highly confidential data from scenes which is utilizing programmed picture observation like item following and so forth A ton of work has been done in this field and numerous strategies presented yet these all method has a few disadvantages and confronting testing like unexpected change in scene, nature of picture. Movement from nonstop picture can be distinguished through optical stream and foundation deduction . In optical stream, movement in picture is assessed by utilizing investigation. In foundation deduction, to discover movement in picture assessed foundation is contrasted and current casings.
The basic issue on the planet is the way where to securely communicate the privileged data and forestall the discovery of data.

E. Proposed System

In the proposed framework Conversations of steganography by and large use phrasing undifferentiated from and reliable with customary radio and interchanges innovation. Be that as it may, a few terms show up explicitly in programming and are effectively befuddled. These are the most significant ones to computerized steganographic frameworks:
In a bunch of documents, the records that are thought about prone to contain a payload are suspects. A speculate recognized through some sort of measurable examination can be alluded to as a competitor.
Recognizing actual steganography requires cautious actual assessment, including the utilization of amplification, designer synthetics and bright light. It is a tedious cycle with clear asset suggestions, even in nations that utilize numerous individuals to keep an eye on their kindred nationals. Nonetheless, it is possible to screen mail of certain presumed people or organizations, like penitentiaries or (POW) camps. There are an assortment of essential tests that should be possible to distinguish whether a mysterious message exists. This interaction isn't worried about the extraction of the message, which is an alternate cycle and a different advance. The most fundamental methodologies of steganalysis are visual or aural assaults, underlying assaults, and measurable assaults. These methodologies endeavor to identify the steganographic calculations that were utilized . These calculations range from unsophisticated to extremely complex, with early calculations being a lot simpler to distinguish because of measurable peculiarities that were available. The size of the message that is being covered up is a factor in the fact that it is so hard to recognize. The general size of the cover object plays a factor too. On the off chance that the cover object is little and the message is huge, this can mutilate the insights and make it simpler to distinguish. A bigger cover object with a little message diminishes the measurements and allows it a superior opportunity of going unseen. Steganalysis that objectives a specific calculation has much better accomplishment as it can enter in on the inconsistencies that are abandoned. This is on the grounds that the investigation can play out a focused on search to find known inclinations since it knows about the practices that it regularly shows. While examining a picture the most un-huge pieces of numerous pictures are really not arbitrary. The camera sensor, particularly lower end sensors are not the best quality and can present some arbitrary pieces. This can likewise be influenced by the document pressure done on the picture. Secret messages can be brought into the most un-huge pieces in a picture and afterward covered up. A steganography instrument can be utilized to disguise the mysterious message at all critical pieces yet it can present an irregular region that is excessively awesome. This space of wonderful randomization sticks out and can be recognized by contrasting the most un-huge pieces with the close to-least huge pieces on picture that hasn't been packed.

V. METHODOLOGY

A. General Perception and Required Process

There are many viewpoint to security and numerous applications. One such way of securing and protecting the information is cryptography. In such case, cryptography is the most essential medium for the securing of information, it isn't without help from anyone else adequate. There are some particular security pre knowledge information [3] for cryptography, which include confirmation, isolation/classification, and veracity Non-renouncement. The three kinds of calculations are depicted:

1) Secret-Key Cryptography (SKC): Implemented by a introverted key for both encryption and disentanglement
2) Public-Key Cryptography (PKC): Implemented by one key for encryption and another for disentanglement
3) Hash-Functions: Implemented by a arithmetical change to irrevocably "mess up" data.
a) convert space methods
b) extend range events
c) arithmetical method
d) deformation procedures
e) Cover age technique

Profit of utilize of AES computation

- Very protected.
- sensible price.
- Main uniqueness.
- litheness
- minimalism

B. Implementation Details

Here mainly three modules involved –

1) Crypto Module - AES Implementation Module
2) Security Module – Newly developed technique
3) Stego Module - DCT Techniques Implementation Module

These modules are design as reusable components and can work independently.

Retrieving Text

a) Retrieve the 7 characters from the picture.
b) Separate letter sets and digits from Key 2 with the assistance of Separator 2.
c) Add back the remainder of the letters in order from Key 2 to 7 characters recovered from the picture.
d) Reorganize the letters in order and digits with the assistance of the Key 1 to get back the first code text in hexadecimal structure.
e) Regenerate the first instant message from the code text with the assistance of AES calculation.

VI. IMPLEMENTATION

A. Tools Used

1) *MATLAB Software:* Matlab software is a high level programming language platform which uses mathematical expressions and matrices and performs operations on communication systems which was invented by mathworks. Applications of matlab is not only limited to control systems but it is used widely used to plot data in histograms pie charts, to calculate efficiency and noise in a communication channel it interfaces with C ,C++ and java by utilising with mathematical and numerous approximations. It is easy to use matlab from basic beginner to a professional and who wants to note the estimations of a system to know different application and to calculate various methodologies.

2) *MATLAB's Employing of Processing Calculations:* Matlab finds most of the application in computational mathematics. so it's new numerous application and approximation it is capable of performing are given below

Ø ·Managing matrices and multi dimensional arrays
Ø·Mapping and Sketching in two and three dimensions
Ø ·Algebraic calculations and linear algebra
Ø ·Direct and indirect functions
Ø ·Statistical analysis
Ø ·Data manipulation
Ø ·Calculus and Differential calculations
Ø ·Numerical Approximations
Ø ·Integrational analysis
Ø ·Transformation

3) *Features of MATLAB*

MATLAB has its basic features which are shown as follows

Ø It is an indisputable language for trigonometric analysis,Characterisation and approach enhancement.
Ø It furthermore provides an intuitive climate to recapitulate scrutiny, plan and critical thinking.
Ø It provides enormous library of numerical variables for undeviating irregular based mathematics,Fourier transforms, distinguishing, smooth running, algebraic and conveying normal differential conditions.

VII. OUTPUT PARAMETER

The whole arrangement comprises of two stages:

- Concealing information in Image (Encryption)
- Recovery of unique data (Decryption)

1) *Security:* Security is the basic goal of the proposed model. To make sure that the receiver receives the information without knowing it to the third party the key is used so that even if they identify that there is a message they cannot disclose it . Both private and public key are generated to increase the security so that the intended person can open the message .

2) *Design Description*

The steps which are to be designed are as follows:

- Encoding step
- Decoding step

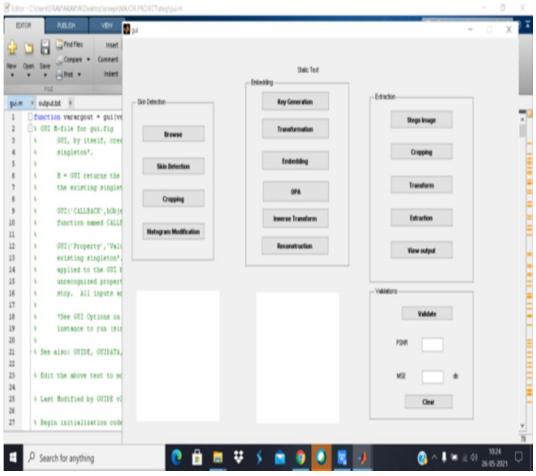
3) *Step 1: Encoding Process*

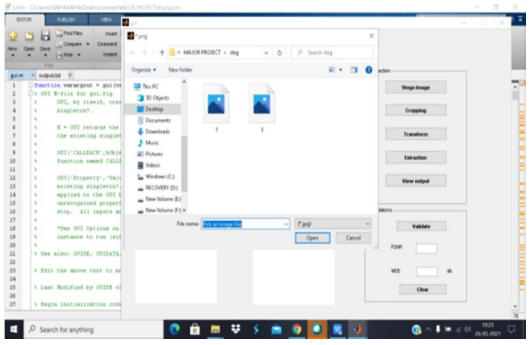
The means engaged with encoding measure are:

a) Separating outlines in the picture
b) Encoding information utilizing Feistel network calculation
c) Installing text inside picture outlines

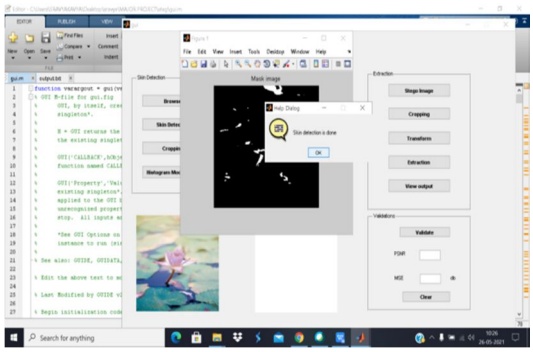
A. *Skin Detection*

1) *Browse:* The basic function is we browse an image directly from where ever we want to hide our message. The file can be an image or audio or video file but most steganographers use image files to hide the messages because of their simplicity and ease of hiding the data. In future we can also apply these techniques to complex files with certain improvements.Whenever you've determined the function you need, a basic double tap or press the keystroke is everything needful to add the capacity at the mark.





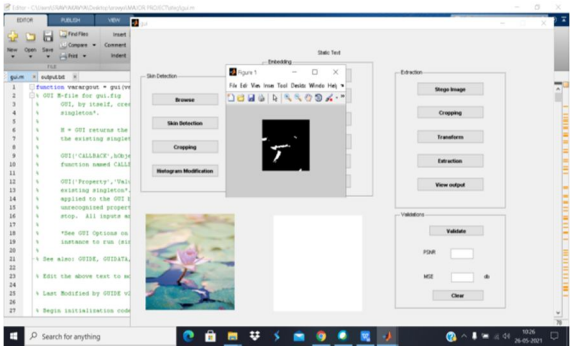
2) Skin Detection



The skin detection has the following steps:

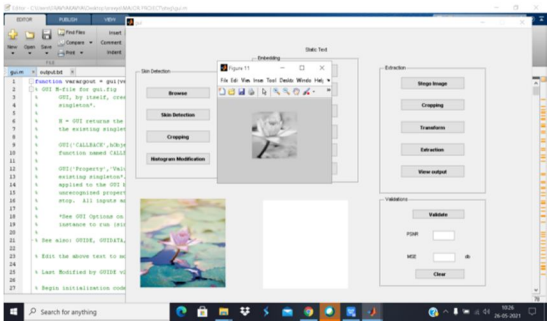
a) Step1: Extract the pictures from internet or capture through a camera.
b) Step2: Identify the pre-owned channel for resizing.
c) Step3: Perform the resizing technique with the removed picture, picture width/2, and picture tallness/2 as contentions.
d) Step4: Apply the skin shading location on the yield picture subsequent to resizing.
e) Step5: Record the CPU season of the recognition interaction for both the work of art and resized methods. Ordinarily utilized skin location calculations can separate skin locales from pictures precisely and dependably, yet they regularly set aside a long CPU effort to complete the identification process.The resizing calculation can be considered as quick skin region finder method.

3) Cropping



Cropping is a technique where the cover picture is divided into specific group of outputs with definite mysterious directions . Partitions the mysterious instant message into leaves behind same cover picture crops amount. Implanted every mysterious instant communication into a picture by concealed abstraction utilizing the LSB method .

4) Histogram Modification: To modify pixel values to accommodate more data and to exploit redundancy and noise. It is converted to gray scale to process the design which is shown in the given figure



B. Embedding

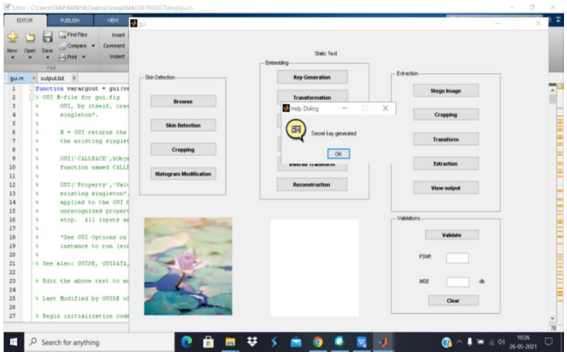
1) Key Generation

Key Generation is the important criterea as to provide a double layer security . Tgere are two types of keys

a) Public Key

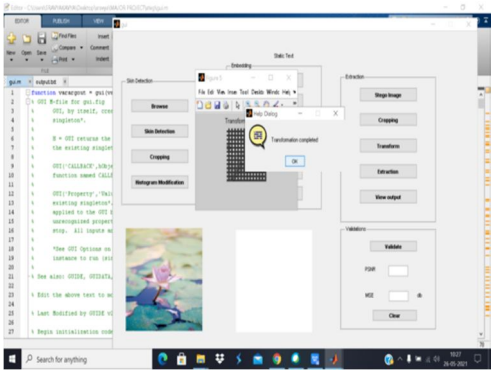
b) Private Key

Both public key and private ki will be generated at the sender and the receiver side. These keys are related to each other's mathematically. Most used RSA algorithms are used to generate these keys and the process of transmission of them. The receiver will send his public key to the transmitter which is visible to everyone who purchases it. the transmitter will send his private key to the receiver which can be opened by the receiver only. In this way the third person can have access to the private key we can not disclose the message message.



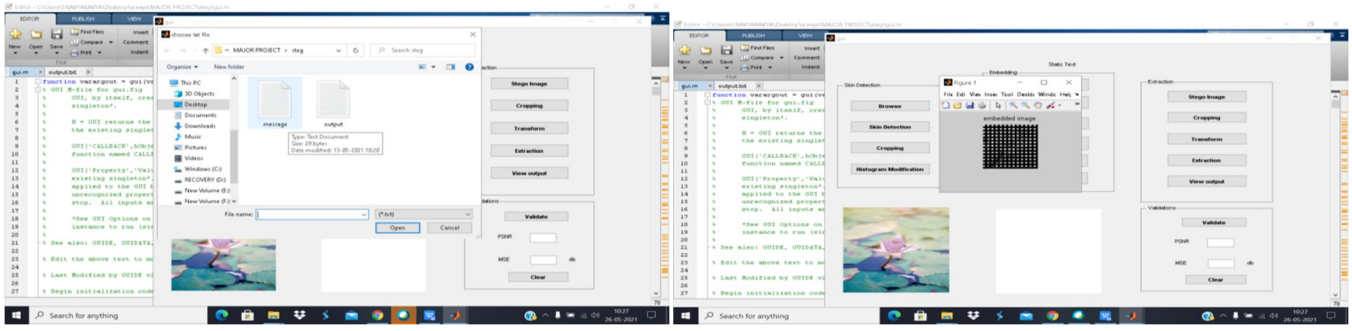
2) Transformation

Transformation is the process of converting from image to pixels. The grid lines shown are the output of the transformation technique .



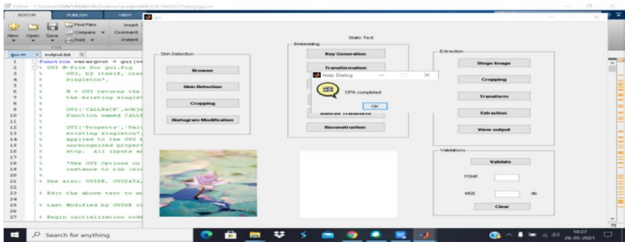
3) Embedding

As the name suggests we embed the message in the histogram modified image as shown in the figure

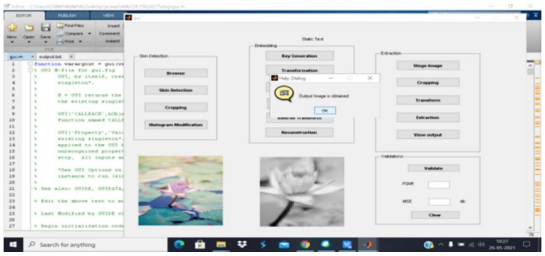


4) OPA

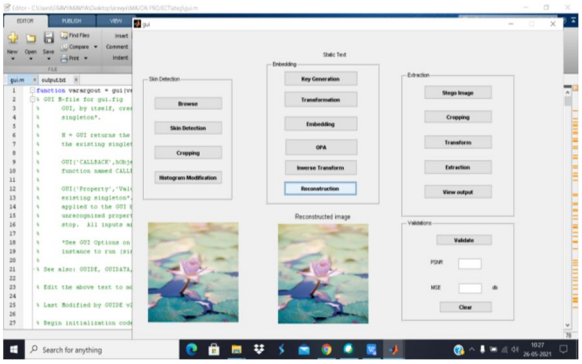
Optimal pixel adjustment is an adjustment technique which is very important because
when we are doing modifications the pixel values get disturbed so to format them and adjust them we use OPA



5) Inverse Transform

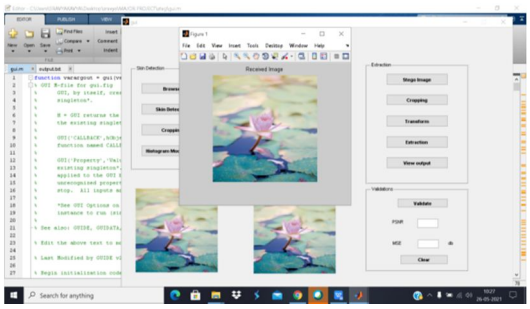


6) Reconstruction

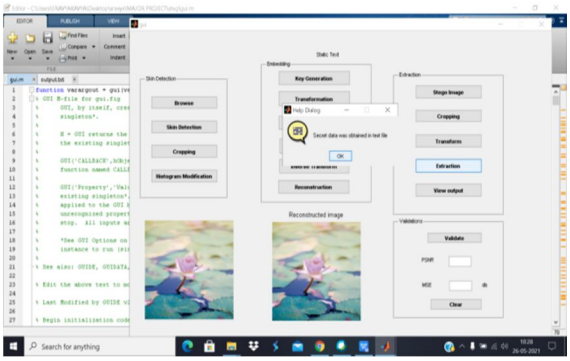


C. Extraction

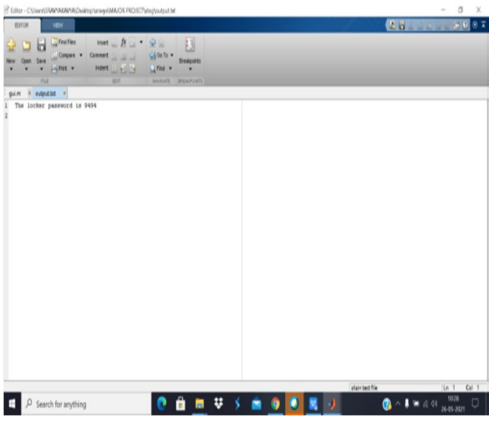
1) Stego Image: Stego image is the combination of the cover image which is an ordinary file consisting of text or audio or video files and the embedded secret message . There is no much difference between a stego and a original message but the size of the file changes.



2) *Extraction:* Extraction is the process of decryption where the main aim is to extract the the hidden message from the stego image. The output after the process of extraction is shown in the below figure



3) *Output:* In the below picture we can observe the output message we sent to the receiver . in our document we have two folders one is message and the other is output folder . The output folder is automatically updated with the secret message we have sent.



D. PSNR

PSNR which manifests an indispensable distinctive component which needs to be contemplated in any broadcasting system. It impersonates a significant role in modifying the attributes of the picture after it is encrypted with the message which stands for signal to the noise ratio. It is a ratio of output signal power obtained to the noise power at the receiver. It can be easily and more simply calculated by using the mean square error. By using MSE the error can be removed to a greater extent compared to the normal linear errors. If we consider a image I with m*n dimension and considering the noise factor as K; then MSE can be determined as below:

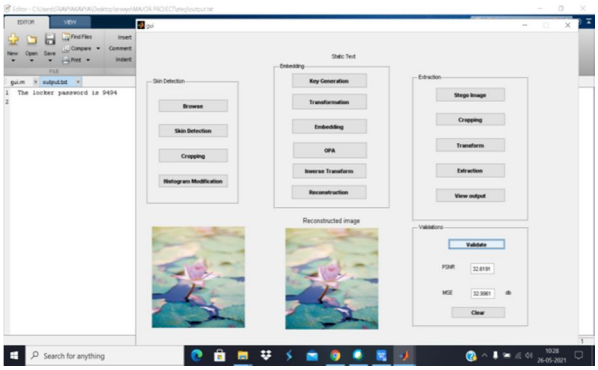
$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

E. MSE

MSE is a well familiar image compression technique which is used to compact the image by securing to maintain acceptable status of the image by diminishing the magnitude of storage to a conclusive level. This metric will not only reduce the storage but also keeps a check to curtail the cost and the transference time to construct an image without any deterioration of its facet. Mostly we will appertain this algorithm to two dimensional grayscale limits from a payload tool and we operate a transformation technique called "discrete wavelet transform" DWT which is then followed by "bit plane encoder" BPE to simulate and produce a bit stream to give compression and decompression. Advantage of this method is it can be easily pertinent to both lossless as well as lossy grayscale files. This algorithm is form in enacted in very numerous levels .The last stage is the decompression stage is perform in a contrasting way and decompression stage imparts the output image which is very near to the original image and finally it produces original image.



PSNR and MSE values

VIII. CONCLUSION

Steganography is the best data hiding technique used for securely sharing information. Today's world demands a data hiding technique which provides better storing characteristics . We have been using steganography and Cryptography individually. In this we are using a technique by combining both these techniques by providing a two layer security of data hiding. This technique envisages every dimension and provides a double layer protection by changing the format of the secret message and also hiding it under a cover that does not reveal in the first place that there is a message. In this we are applying LSB combined with RSA algorithm for data hiding. This will help the future investigators to provide more improved algorithms for better data hiding. PSNR value is used for determining the quality of the image after the data is encrypted, gives output or the efficiency of the image. The more PSNR the higher the quality of the image. We are also using the mean square error to check the quality of the image. The lesser the message the better is the quality of the image. So there should be a tradeoff between PSNR and MSE for image quality so that there will be very less difference between output image and the actual original image.

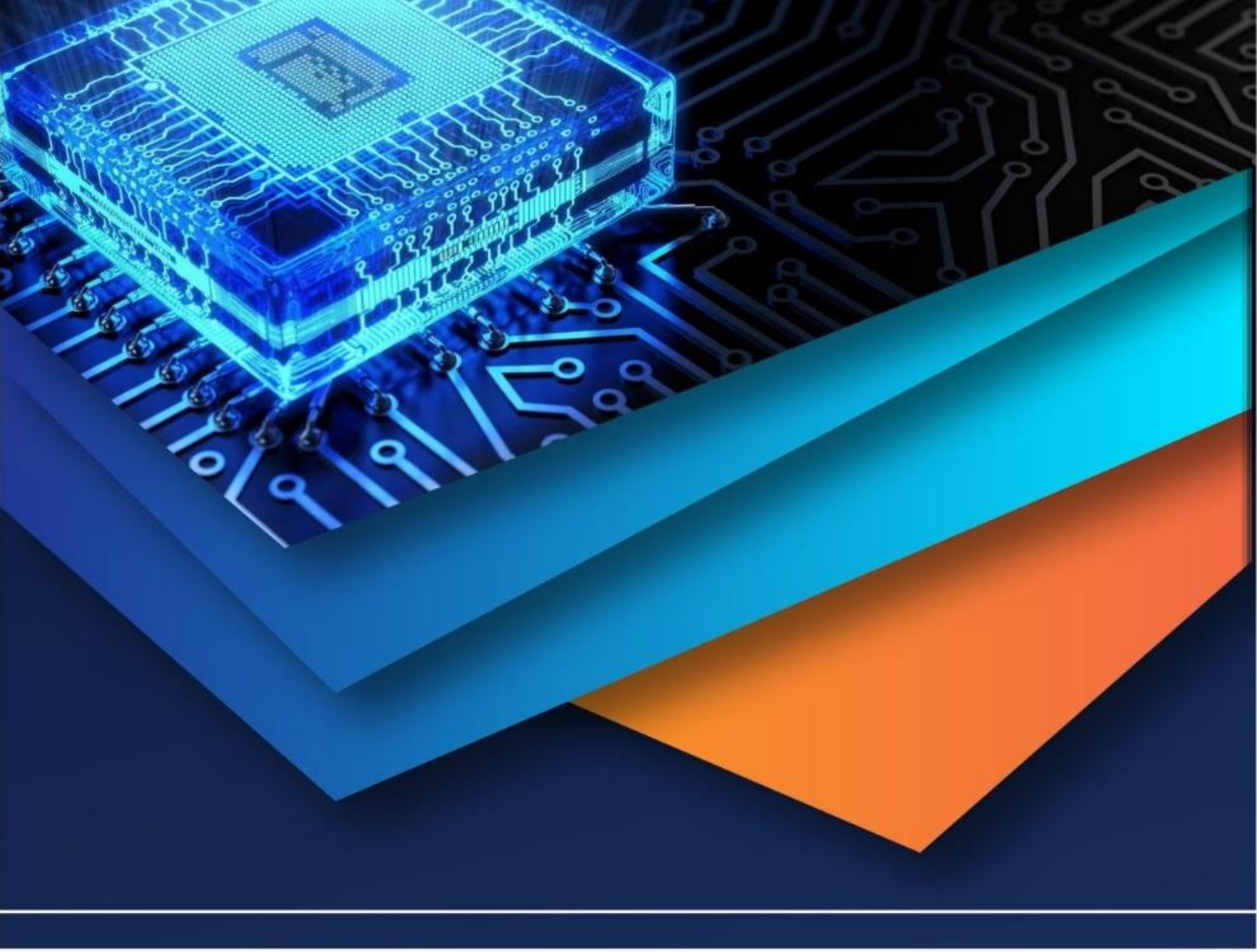
IX. ACKNOWLEDGEMENT

We would like to express sincere thanks and gratitude to our mentors Dr.chatopadhyay, Dr.Sruthi Bhargava for their encouragement and technical interaction.

REFERENCES

[1] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique for picture Steganography (HLSB"), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1,No2, April 2012.
[2] A. Swathi and Dr. S.A.K. Jilani, "picture Steganography by LSB Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 5, September 2012.
[3] Ronak Doshi, Pratik Jain and Lalit Gupta, "Steganography and Its Applications in Security",International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 6, November-December 2012.
[4] Rohit G Bal and Dr. P. Ezhilarasu, "An Efficient Safe and Secured picture Steganography utilizing Shadow Derivation", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.
[5] Hamdy M. Kelash, Osama F. Abdel Wahab, Osama A. Elshakankiry and Hala S. El-sayed, "Use of SteganographicTechniques inimage Sequences", International Journal of Computing and Network Technology, Sys. 2, No. 1 Pg. 17-24, January 2014.
[6] Hemant Gupta and Setu Chaturvedi, "picture Steganography through LSB Based Hybrid Approach", International Journal of Computer Science and Network Security, Vol. 14, No. 3, March 2014.

[7] Anwar H. Ibrahim and Waleed M. Ibrahim, "Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time",International Journal of Information Technology and Computer Science (IJITCS), Vol. 7, No. 3, February 2013.
[8] Krati vyas and B. L. Buddy, "A Proposed Method in Image Steganography to improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 3, Issue 1, January 2014.
[9] Deepak Kumar Sharma and Astha Gautam, "An Approach to shroud Data in picture utilizing Steganography",International Journal of Research in Engineering and Technology (IJRET), Vol. 3, Issue 4, April 2014.
[10] Vipula Madhukar Wajgade and Dr. Suresh Kumar, "Improving Data Security utilizing picture Steganography", International Journal of Emerging Technology and Advanced Engineering (IJETAC), Vol. 3, Issue 4, April 2013.
[11] Ms. Fameela. K. A, Mrs. Najiya. An and Mrs. Reshma. V. K, "Review on Reversible Data



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY