

SECRET COMMUNICATION USING CRYPTOGRAPHY AND STEGANOGRAPHY USING IMAGE PROCESSING

Group Member Names

17BCI0189 – Mrinal Kumar Mishra

18BCE0196 – Mohd Umar

18BCE0281- Anish Aggarwal

18BCE0298- K Nishanth Reddy

18BCE2279- Ashutosh Singh

Faculty Name

Dr. CHIRANJI LAL CHOWDHARY

Associate Professor, CITE, VIT Vellore

Winter Semester

December 2019 - June 2020

Video Link:

<https://drive.google.com/drive/u/1/folders/1maOSmuHjcymgXY1j9QEVcNtG1JLAtAcjq>



Synopsis

With the advancement and development in the field of information sharing and communication in the recent decades, information security has become one of the main topics in communication systems. Everyday one or the other Vulnerability is exploited by a black hat hacker. This leaves fear among the heart of the people. Some hacking have been even on a worldwide scale such as the infraex in Russia, wannacry hack in 2017 in which the wannacry ransomware cryptoworm targeted the computers running on the Microsoft windows operating system by encrypting data and demanding ransom payments in the Bitcoin Cryptocurrency. Due to these issues Security of information has become a critical part in the communication channel. Security of a information mainly depend on strength of the keys in the Cryptographic and Steganographic processes. Cryptography in simple words is the method of ciphering the text, i.e. secret writing. On the other hand Steganography is hiding the text in an image, video or audio. In this project, techniques are used to implement both steganography and cryptography . The text is first encrypted using RSA algorithm, followed by hiding of that data in an image using a least significant bit steganographic algorithm. The project is further extended to show the changes in an image after steganographic conversion. The LSB plane of the image is compared before and after steganographic conversion and how the size of the file matter in this accord is also preyed into.

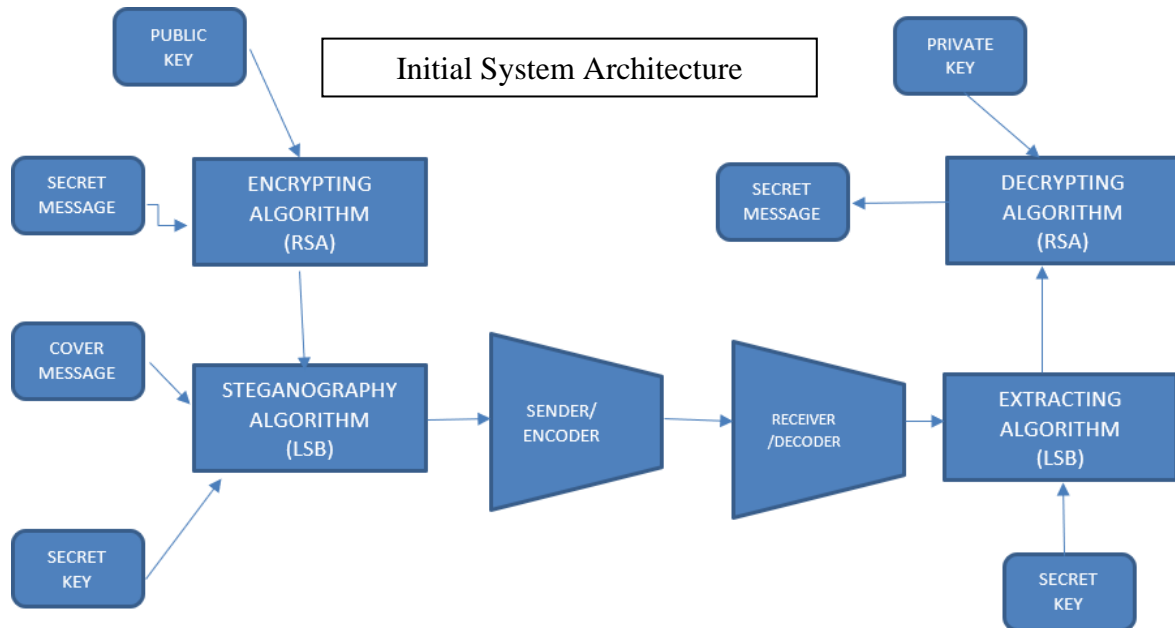
REVIEW 1

For Review 0, our team (Boi), brainstormed on the topic to choose for the project. The selection process was tiring and breath – taking. Many topics were introduced and rejected among ourselves cause we aimed at something good, which is not only bonny but also have a practical application in real life. So, our member Ashutosh came up with this idea of making the project on the topic of communication using cryptography and steganography. The topic was unknown to all but piqued everybody's inquisition. We researched about the topic and came up with all these in our Review 0:-

- We discussed with the faculty about the immensity and application of the topic.
- We found a number of research paper about the topic.
- We started analyzing the topic with the live examples like whatsapp, e-payment system like paytm, phonepay and more.
- We discussed the outline for the project and the phases and work division among the members.
- We finalized the algorithms to be used for cryptography and steganography.

REVIEW 2

Until the Review 0 everything was finalized only thing left to do was to give life to the project. We decided our project architecture, which is given below:-

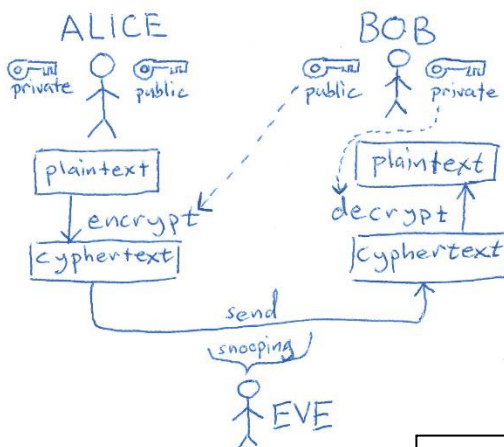


- LSB algorithm was implemented and the results were discussed and program was updated again and again until everyone agreed with the output.
- Mrinal came up with the idea of using RSA algorithm for cryptography because of its wide domain of applicability, ease of use and functions.

```

1 candidate_image = imread('ae.jpg'); % to load/read image
2 candidate_image = rgb2gray(candidate_image);
3 M = 'hideMessage.txt';
4 secret = fopen(M,'rb'); %open source file
5 % rb is used for opening a non- text file
6 [M,L] = fread(secret,'uint1'); %read secret file as binary
7 %L is the length of the secret file
8 [n,m] = size(candidate_image); %n is rows, m is columns*3
9 m = m/3;
10 %m*n is the max size of save secret
11 if (m*n*3 < L)
12     msg = msgbox('your picture is too small','size error');
13     pause(1);
14     if (ishandle(msg)) %returns true for graphic handles
15         % handle refers to a specific instance of a graphic object.
16         close(msg);
17     end
18 end
19 latest_data = candidate_image;
20 count=1;
21
22 for i=1:m %width
23     for j=1:n %height
24         for k=1:1 %RGB
25             latest_data(i,j,k) = candidate_image(i,j,k) - mod(candidate_image(i,j,k),2) + M(count,1);
26             if count==L
27                 break;
28             end
29             count= count+1;
30         end
31     end
32     if count==L
33         break;
34     end
35 end
  
```

LSB ALGORITHM



RSA ALGO. WORKING

REVIEW 3**TABLE OF CONTENTS OF PROJECT**

Group Member Names	1
Faculty Name.....	1
Video Link	1
REVIEW 1.....	3
REVIEW 2.....	4
REVIEW 3.....	5
TABLE OF CONTENTS OF PROJECT	5
INTRODUCTION.....	6
MOTIVATION.....	6
CONTRIBUTION	7
ORGANIZATION OF REPORT	7
LITERATURE SURVEY.....	8
BACKGROUND OF YOUR PROJECT WORK	9
PROPOSED WORK.....	9
Block Diagram	9
System Architecture.....	10
Evaluation and Results Analysis	10
Tabular Comparison with Existing Work.....	11
Overall Discussion	14
CONCLUSION	14
REFERENCES.....	14
Appendix for Individual Contribution Details in Group	15

INTRODUCTION

As digital information and data are transferred over the internet and securing sensitive messages need to discover and developed more often than ever before, new technologies for protecting and securing the sensitive messages needs to realize and develop. Because cryptography and steganography methods always exposed to attacks by Steganalysis, so we constantly need to develop and look for new modes. Cryptography and Steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way, which hides the existence of communication. On the other hand, cryptography is the enciphering and deciphering of data and information with a secret code so it cannot be understood. The Steganography hides the message so it cannot be seen.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key, both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message, for instance, might provoke suspicion on the part of the recipient while an invisible message created with steganographic methods will not. However, steganography can be useful when the use of cryptography is illegal. Where cryptography and strong encryption are barred, steganography can avoid such policies to pass the message secretly. Steganography can be broadly classified into four categories namely audio/video, image, text and protocol, based on the covering medium.

However, steganography and cryptography differ in the way they are judged. Cryptography fails when the “enemy” is able to access the content of the cipher message, while steganography fails when the “enemy” detects that there is a secret message present in the steganographic medium. However the combination of these two methods will enhance the security of the data embedded. Therefore the transmission system communication comprises of two stages. The first stage involves encrypting the secret message. In the second stage, the encrypted message is covered by using steganography. The blend of steganography with cryptography thereby ensures secret data communication; as a successful attack would involve hidden data inversion and data extraction. Thus breaching becomes harder since it requires recognition of carrier that conceals the secret message before its extraction and deciphering. This combined will satisfy the requirements such as capacity, security, and robustness for secure data transmission over an open channel. Although many different carrier file formats can be used, digital images are the most popular because of their frequency on the Internet. Image steganography has its own advantages and is most popular among the others as it has better payload capacity and imperceptibility. The aim of this project is to describe a method for integrating together cryptography and steganography through media such as image. In this project, the secret message is embedded within the image called cover-image. Cover-image carrying embedded secret data is referred to as stego-image. Stego-image is sent over the network towards the receiver end. Receiver receives the image, uncovers it followed by decryption to get the intended message.

MOTIVATION

The primary reason for selecting communication using steganography and cryptography among the list of possible topics was due to the unfamiliarity of the words that triggered an interest in the

subject. Another reason is the data security that it provides. I being a very paranoid person rarely puts my trust on unknow and if come it private matter things become more difficult. One of the other reason being that even if a hacker or an intruder gets access to our multimedia data, then also he can't access the information, that is the hacker has done the difficult part of hacking in getting access to the data but the actual data after being under his nose he can't do anything. This aspect makes the project more interesting.

CONTRIBUTION

Our aim has to develop a system to not just deepen the knowledge about the subject but to make it as practical as possible. For the purpose every member of the group was enthusiastic and the team leader (Anish) divided the work finely according to the interest of the members. There was collaboration among the members the project modules were not completely independent. The inter- dependencies of the individual project were clear. Communication between Mrinal and Umar was inevitable as both of them were working on the Encryption and Decryption part.

Whereas the rest of team was working on Steganography and bit plane slicing. The individual break down of the work is as follows:-

- Mrinal – Was assigned with choosing the right algorithm for encryption. He decided to go with RSA algorithm. All the research of RSA and coding was handled by him. Later he took part in report preparation.
- Umar – As a frontend developer, he did his part by making GUI. He also did the coding for encryption and decryption function. Also played an irreplaceable role in designing the ppt for the project.
- Anish – The steganography part was handled by him including the codes and the choice of algorithm. Later did a great work in video editing and project management.
- Nishanth – Odd one of all. Initially there were some communication disparities between us due to language, but as time passed the team capabilities rose and by the end there was no feeling of intruders among us. As for work he coded for bit plane slicing and played a major role in selecting algorithm by comparing their merits, demerits and feasibility. He with Umar, made the ppt too.
- Ashutosh – Gave the idea for showing the effects on LSB and helped Nishanth for the same. He was also the head for code optimization of the overall code.

ORGANIZATION OF REPORT

The purpose of this report is to inform the reader about image steganography and cryptography. How one uses it in its day to day life and still knows so little about it. The report tells about the project done by our team, which is to implement the steganography and cryptography. The project shows the use of ease and vastness of algorithms in this field.

LITERATURE SURVEY

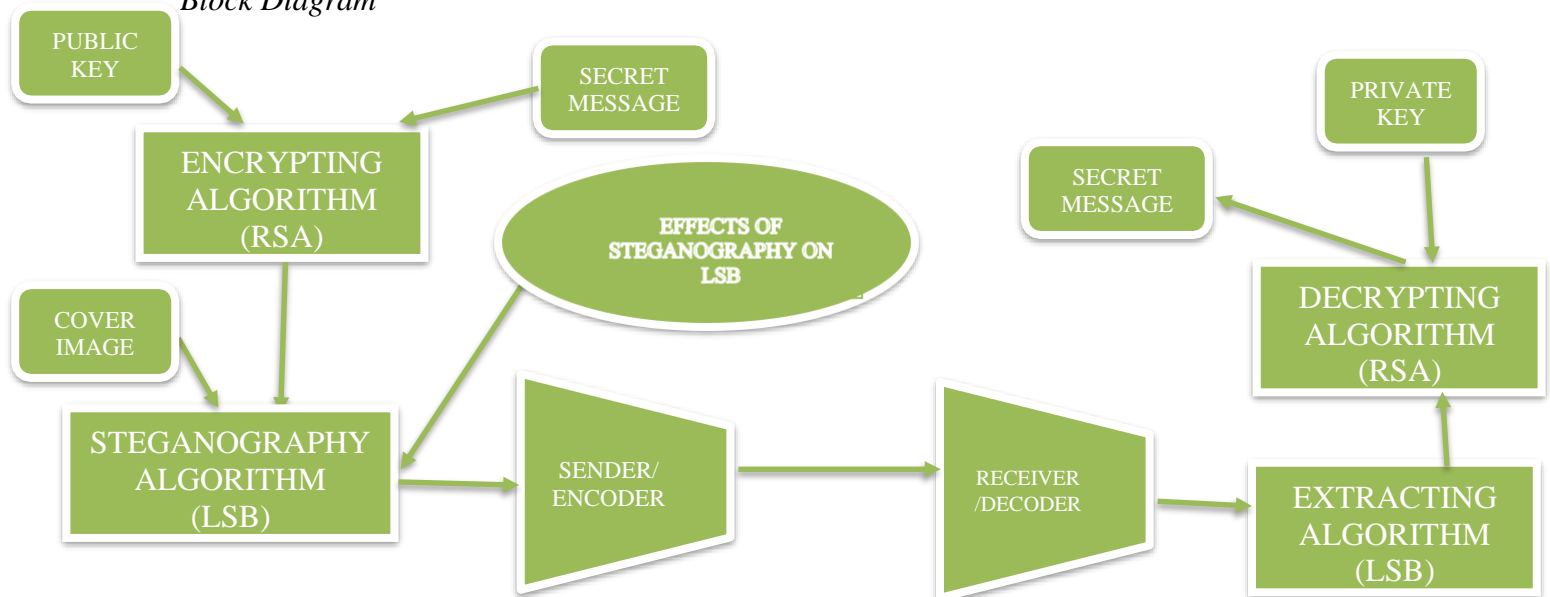
Reference	Methods Used	Evaluation	Merits and Demerits
http://www.iosrjournals.org/iosr-jce/papers/Vol13-issue5/A01350106.pdf?id=6593	Encryption using Blowfish Algorithm	Though the algorithm is very powerful and its complexity limits its application in the real world	Good performance and robust but, very high complexity makes it difficult for practical application
https://www.researchgate.net/publication/286679578_Secret_communication_using_Public_Key_steganography	Steganography using F5 algorithm followed by 1024bit key encryption	As the key is of 1024 bit, the security it provides on a next level. There is even no need of steganography with such high encrypted images	According to NIST, best cryptanalysis can break key with 768bit, so in today's time breaking key of 1024bit is infeasible.
https://pdfs.semanticscholar.org/b2cf/afab2318db09c719354c679c52539c465233.pdf	Used DES algorithm for encryption and LSB for steganography	The ease of implementation of the algorithm makes it possible to use it for local host but for a larger area there are many chances of exploiting the vulnerabilities	Though DES algorithm is good for eavesdrop by naked eye, but due to its lower complexity it can be easily decrypted.

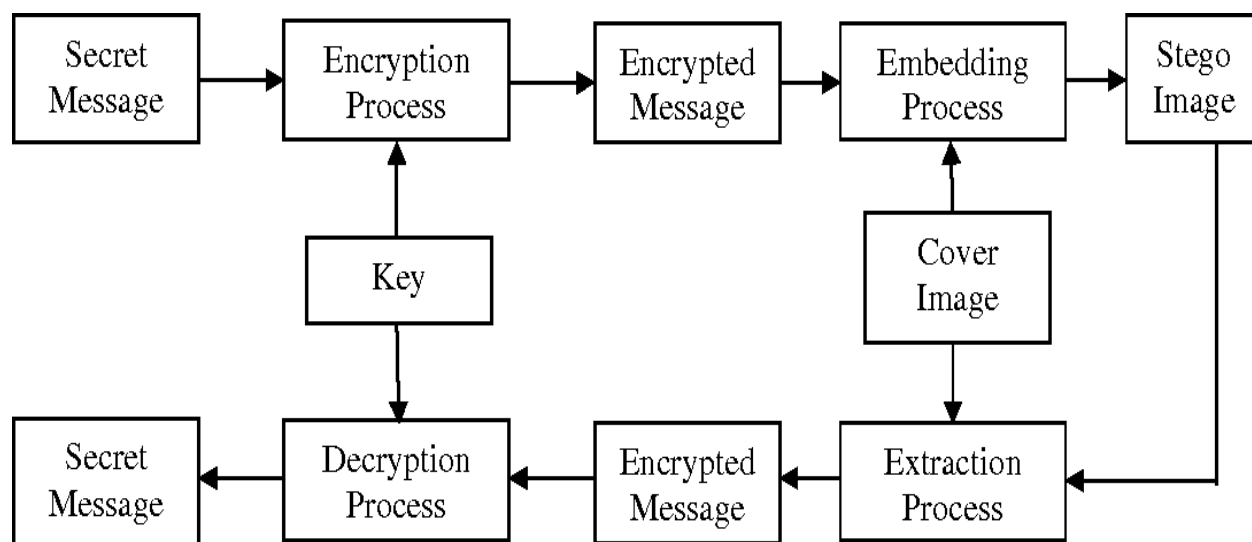
BACKGROUND OF YOUR PROJECT WORK

Cryptography is the method of encoding or scrambling secret messages whose meaning cannot be understood by others who try to intercept the message . The purpose of cryptography is to protect the secret message from unintended receiver or attacker. Unless the technique of the encoding system is known, the data cannot be retrieved. A Cryptographic algorithm is considered computationally secure if it cannot be broken with available resources . The technique for deciphering cipher messages is called cryptanalysis which signifies that the set of methods for obtaining the meaning of encrypted information. Successful cryptanalysis may recover the plaintext or the key by finding weaknesses in the cryptosystem that would lead to an attack from a third party . Steganography is the method of hiding confidential messages into digital media in a way that no one apart from the sender and intended receiver even realizes there is a hidden message inside the media . Steganography techniques are used to address digital rights, information security and conceal secrets. Most of the steganographic systems in the present days use images as cover media because digital images are mostly transmitted over Internet communication . Digital images often have a large amount of redundant data or noise present in them and this provides space to embed data and the modification in the image is not perceptible to a human eye . Steganalysis is a term closely related to steganography which is a method for detecting hidden messages in digital medium . Today advances in steganography are followed by advances in Steganalysis. Image based steganographic methods aims to make changes not detectable by the human eye. This feature is not enough because statistical methods can detect the changes in the image even if it is not visible .

PROPOSED WORK

Block Diagram



System Architecture*Evaluation and Results Analysis*

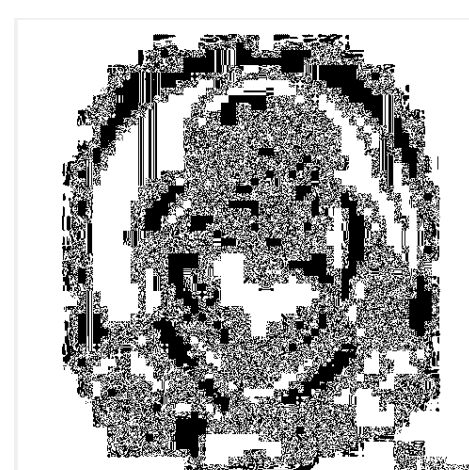
- Bit plane Slicing result



Original Grayscale Image

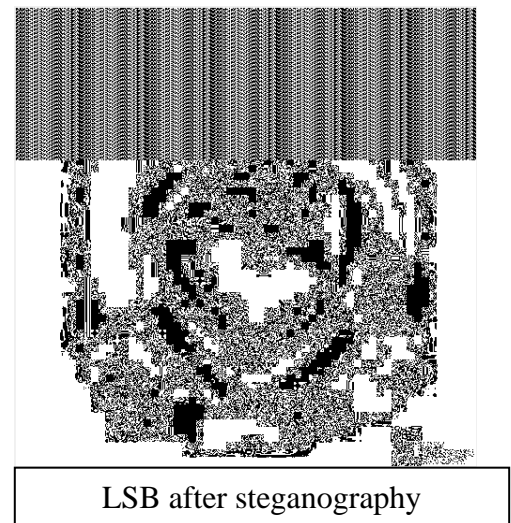
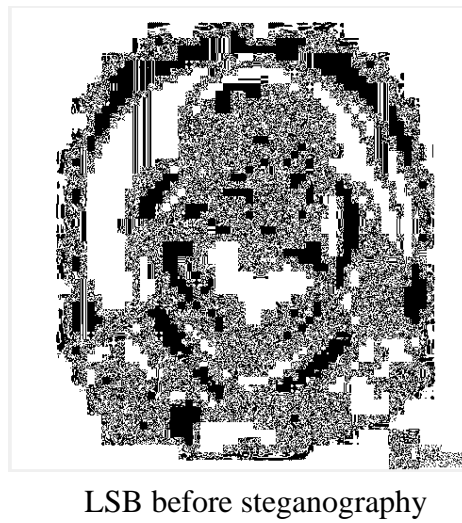


MSB plane of the image



LSB plane of the image

- Comparison of LSB of an image before and after Steganography.



- Image after steganography



- Image after encryption and decryption



Original Image

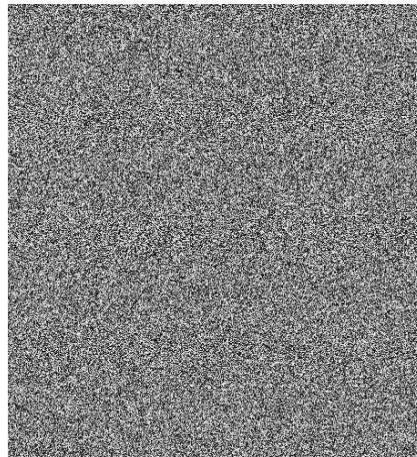


Image after encryption



Image after decryption

- Images of code

```

1 candidate_image = imread('minion.jpg'); % to load/read image
2 candidate_image = rgb2gray(candidate_image);
3 M = 'hideMessage.txt';
4 secret = fopen(M, 'rb'); % open source file
5 % rb is used for opening a non-text file
6 [M, L] = fread(secret, 'ubit1'); % read secret file as binary
7 % L is the length of the secret file
8 [n, m] = size(candidate_image); % n is rows, m is columns*3
9 m = m/3;
10 % m*n is the max size of save secret
11 if (m*n*3 < L)
12     msg = msgbox('your picture is too small', 'size error');
13     pause(1);
14     if (ishandle(msg)) % returns true for graphic handles
15         % handle refers to a specific instance of a graphic object.
16         close(msg);
17     end
18 end
19 latest_data = candidate_image;
20 count = 1;
21
22 for i = 1:m % width
23     for j = 1:n % height
24         for k = 1:3 % RGB
25             latest_data(i, j, k) = candidate_image(i, j, k) - mod(candidate_image(i, j, k), 2) + M(count, 1);
26             if count == L
27                 break;
28             end
29             count = count + 1;
30         end
31         if count == L
32             break;
33         end

```

Code for LSB image
Steganography

```
Editor - F:\STUDY\SEM 4\IP\ip_project\bit_plane_slicing.m
bit_plane_slicing.m  ImageEncryptionGui.m  imageProcess.m
1  p=imread('minion1_encrypted_image.jpg');
2  %p = rgb2gray(p);
3  %figure, imshow(p)
4  cd = double(p);
5
6  c0= mod(cd,2);
7  figure, imshow(c0);
8  c1= mod(floor(cd/2),2);
9  figure, imshow(c1);
10 c2= mod(floor(cd/4),2);
11 figure, imshow(c2);
12 c3= mod(floor(cd/8),2);
13 figure, imshow(c3);
14 c4= mod(floor(cd/16),2);
15 figure, imshow(c4);
16 c5= mod(floor(cd/32),2);
17 figure, imshow(c5);
18 c6= mod(floor(cd/64),2);
19 figure, imshow(c6);
20 c7= mod(floor(cd/128),2);
21 figure, imshow(c7);
22
23 combined_image= 2*(2*(2*(2*(2*(2*( (2*c7)+c6)+c5)+c4)+c3)+c2)+c1)+c0;
24 %figure, imshow(uint8(combined_image))
```

The screenshot shows the MATLAB R2018a interface. The 'Current Folder' window on the left displays a file tree with 'keyGen.m' selected. The 'Editor' window on the right shows the code for 'ImageEncryptionGui.m'. The code includes functions for GUI initialization, opening, and decryption. A red box highlights the 'keyGen.m' file in the file tree, and a red box highlights the 'Image Encryption code' text at the bottom right.

```

1 function varargout = ImageEncryptionGui(varargin)
2     gui_Singleton = 1;
3     gui_State = struct('gui_Name',       mfilename, ...
4                        'gui_Singleton',   gui_Singleton, ...
5                        'gui_OpeningFcn', @ImageEncryptionGui_OpeningFcn, ...
6                        'gui_OutputFcn',  @ImageEncryptionGui_OutputFcn, ...
7                        'gui_LayoutFcn',  @ImageEncryptionGui_OutputFcn, ...
8                        'gui_Callback',    []);
9
10    if nargin && ischar(varargin{1})
11        gui_State.gui_Callback = str2func(varargin{1});
12    end
13
14    if nargout
15        [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
16    else
17        gui_mainfcn(gui_State, varargin{:});
18    end
19
20 function ImageEncryptionGui_OpeningFcn(hObject, eventdata, handles, varargin)
21
22     handles.output = hObject;
23     axes(handles.axes4)
24     BackGr = imread('leaf.jpg');
25     imshow(BackGr);
26
27     guidata(hObject, handles);
28     clear all;
29     clc;
30     global img;
31     global DecImg;
32     global DecImg;
33

```

Image Encryption code

Bit – Plane slicing code

The screenshot shows the MATLAB Editor with the following code in `keyGen.m`:

```

1 function [key] = keyGen(n)
2     n = n*8;
3     % n = 2048*2048*16;
4     % n = 24 * 24 * 8;
5     bin_x = zeros(n,1,'uint8');
6     r = 3.9999998;
7     bin_x_N_Minus_1 = 0.300001;
8     x_N = 0;
9     tic
10    for ind = 2 : n
11        x_N = 1 - 2 * bin_x_N_Minus_1 * bin_x_N_Minus_1;
12        if (x_N > 0.0)
13            bin_x(ind-1) = 1;
14        end
15        bin_x_N_Minus_1 = x_N;
16    end
17    toc
18    % save bin_sec bin_x;
19    t = uint8(0);
20    key = zeros(n/8,1,'uint8');
21    for ind1 = 1 : n/8
22
23        for ind2 = 1 : 8
24            key(ind1) = key(ind1) + bin_x(ind2*ind1) * 2 ^ (ind2-1);
25        end
26    end
27 end

```

The script is saved in the current folder, and the function signature is shown as `keyGen(n)`.

Key Generation Code

Tabular Comparison with Existing Work

Our Work	Existing Work
<ul style="list-style-type: none"> • Easy to implement and maintain 	<ul style="list-style-type: none"> • Very complex and difficult to maintain
<ul style="list-style-type: none"> • Can be used on personal PCs. 	<ul style="list-style-type: none"> • Due to large complexity, it is not generally used on personal PCs.
<ul style="list-style-type: none"> • Easy to hack into 	<ul style="list-style-type: none"> • Very hard to hack
<ul style="list-style-type: none"> • Free of cost 	<ul style="list-style-type: none"> • Usually costly

Overall Discussion

Over the whole project we have analyzed many algorithms, literature reviews and way for image encryption and steganography. So from this we can conclude that though this is not the best method for the security of one's information and important files in all the situation but it can be used for a local host to give a extra layer of security to your document.

CONCLUSION

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. The proposed project is designed to combine the features of both cryptography and steganography, which will provide a higher level of security. It is better than the technique used separately. Simple LSB and RSA method together provide a pretty good security for the data.

REFERENCES

[1] <http://www.iosrjournals.org/iosr-ice/papers/Vol13-issue5/A01350106.pdf?id=6593>

Authors: Ms. Hemlata Sharma, Ms. Mithlesh Arya, Mr. Dinesh Goyal

Year of Publication: Issue 5 (Jul. - Aug. 2013)

Source Reference: www.iosrjournals.org

[2] <http://ijesc.org/upload/a5b07cc82388094760e7356f965aab53.Image%20Processing%20using%20Steganography.pdf>

Authors: Munesh Kumar¹, Gaurav Yadav², Ashish Kumar Keshari³, Sandhya Katiyar

Year of Publication: Issue April 2017

Source Reference: <http://ijesc.org/>


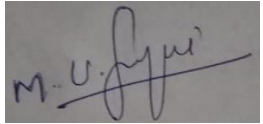
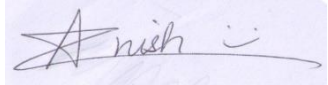
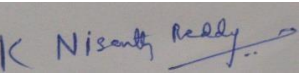
[3] https://www.researchgate.net/publication/322477779Combining_Cryptography_and_Steganography_for_Data_Hiding_in_Images

Authors: HAYFAA ABDULZAHRA, ROBIAH AHMAD, NORLIZA MOHD NOOR

Year of Publication: Issue May 2017

Source Reference: [researchgate.net/](https://www.researchgate.net/)

Appendix for Individual Contribution Details in Group

Sr No	Reg No	Role and Responsibility	Digital Signature
1	17BCI0189	LSA algorithm application, content selection and report preparation	
2	18BCE0196	Cryptography GUI, encryption and decryption, ppt	
3	18BCE0281	Steganography, video editing and project management.	
4	18BCE0298	Bit plane slicing and algorithm selection, ppt	
5	18BCE2279	Steganography effects on LSB, code optimization, report	