**TOPIC OF THE PROJECT**

**SECRET CODE CONCEALER**

***Submitted in partial fulfilment of th*e *requirements for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

***in***

**INFORMATION TECHNOLOGY**

***by***

**Aayush Moolchandani Rishabh Singh Sahil Bansal Shivann Hangloo**

**35115603116 36115603116 40115603116 44215603116**

***Guided by***

**Mr. Devender Banga**

**Mentor**



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**AKHILESH DAS GUPTA INSTITUTE OF TECHNOLOGY AND MANAGEMENT**

**(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI)**

**NEW DELHI – 110053**

**AUG 2019**

**CANDIDATE’S DECLARATION**

It is hereby certified that the work which is being presented in the B. Tech Minor Project Report entitled **“SECRET CODE CONCEALER”** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** and submitted in the **Department of Information Technology** of **Dr. Akhilesh Das Gupta Institute Of Technology and Management, New Delhi (Affiliated to Guru Gobind Singh Indraprastha University, Delhi)** is an authentic record of our own work carried out during a period from **August 2019 to October 2019** under the guidance of **Mr. Devender Banga.**

The matter presented in the B. Tech Minor Project Report has been submitted by me for the award of any other degree of this or any other Institute.

**(Aayush Moolchandani) (Rishabh Singh) (Sahil Bansal) (Shivann Hangloo)**

**(35115603116) (3615603116) (40115603116) (44215603116)**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge. They are permitted to appear in the External Minor Project Examination.

**(Mr. Devender Banga) Prof. (Dr.) Prashant Singh**

**Assistant Professor Head, IT**

The B. Tech. Minor Project Viva-Voce Examination of Shivann Hangloo(44215603116), Sahil Bansal(40115603116), Aayush Moolchandani(35115603116), Rishabh Singh(36115603116),has been held on **……………………………….**

**Mr. Ankit Aggarwal (Signature of External Examiner)**

**Project Coordinator**

**Prof. (Dr.) Preety Verma Dhaka**

**Project Coordinator**

**ABSTRACT**

This project report tends to give an overview of secretly concealing the information meant for the receiver inside the image, its uses and techniques. It also attempts to identify the requirements of a good encryption and decryption software that can be used for the following task. The project is basically providing the techniques and physical application or software-based application of how the private or sensitive information could be hidden within something that appears to be nothing out to the usual. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding the respective information many encryption and decryption tools can be used of which some can be way more complex than the others all of them having their own respective strong and weak points. So, the basic objective behind the creation of this project is to provide the users with a sense of privacy and security while having a conversation online and not worrying about the fact that the information would somehow leak to the outside world.

**ACKNOWLEDGEMENT**

We express our deep gratitude to **Mr. Devender Banga,** Assistant Professor, Department of Information Technology for his valuable guidance and suggestion throughout our project work. We are thankful to **Prof. (Dr.) Preety Verma Dhaka**, Project Coordinator and **Mr. Ankit Aggarwal,** Project Coordinator for their valuable guidance.

We would like to extend our sincere thanks to **Dr. Prashant Singh, Head of the Department,** for his time to time suggestions to complete my project work.

**(Aayush Moolchandani) (Rishabh Singh) (Sahil Bansal) (Shivann Hangloo)**

**(35115603116) (3615603116) (40115603116) (44215603116)**

**TABLE OF CONTENTS**

CANDIDATE’S DECLARATION..................................................................i

ABSTRACT…………………..........................................................................ii

ACKNOWLEDGEMENT..............................................................................iii

LIST OF FIGURES...........................................................................................v

CHAPTER 1

1.1 OBJECTIVE 1

CHAPTER 2

2.1 INTRODUCTION 2

2.2 WHAT DOES THE PROJECT DO 3

2.3 PROBLEM STATEMENT 4

CHAPTER 3

3.1 TECHNOLOGIES USED 5

3.2 SOFTWARE DETAILS 6

3.3 ALGORITHMS USED

3.3.1 LSB ALGORITHM 7

3.3.2 AES ALGORITHM 7

3.3.3 TRIPLE DES ALGORITHM 8

3.4 SITE PLAN FOR ENCODING 9

3.5 SITE PLAN FOR DECODING 10

CHAPTER 4

4.1 RESULT ANALYSIS (SCREENSHOTS) 11

CONCLUSION 27

REFERENCES 28

**LIST OF FIGURES**

Figure 2.1 Secret Code Concealer Module.........................................................3

Figure 3.1 LSB Algorithm..................................................................................7

Figure 3.2 AES Algorithm..................................................................................8

Figure 3.3 Triple DES Algorithm........................................................................8

Figure 3.4 Site Plan For Encoding.......................................................................9

Figure 3.5 Site Plan For Decoding......................................................................10

Figure 4.1 Starting of Secret Code Concealer.......................................................11

Figure 4.2 Select from the following algorithms...................................................12

Figure 4.3 Click on open file to select cover image...............................................12

Figure 4.4 Select cover image................................................................................13

Figure 4.5 Enter message to hide............................................................................13

Figure 4.6 Click encode and save it as stego..........................................................14

Figure 4.7 Encoding Time.......................................................................................14

Figure 4.8 Select stego image for decoding............................................................15

Figure 4.9 Stego image is selected..........................................................................15

Figure 4.10 Time taken in decoding.........................................................................16

Figure 4.11 Hidden message is decoded...................................................................16

Figure 4.12 Click on open file to select cover image................................................17

Figure 4.13 Select cover image..................................................................................17

Figure 4.14 Enter message to hide.............................................................................18

Figure 4.15 Encrypt the entered message...................................................................18

Figure 4.16 Click encode and save it as stego............................................................19

Figure 4.17 Encoding Time............................................................................... ........19

Figure 4.18 Select stego image for decoding..............................................................20

Figure 4.19 Stego image is selected............................................................................20

Figure 4.20 Time taken in decoding............................................................................21

Figure 4.21 Hidden message is decoded......................................................................21

Figure 4.22 Click on open file to select cover image...................................................22

Figure 4.23 Select cover image.....................................................................................22

Figure 4.24 Enter message to hide.................................................................................23

Figure 4.25 Encrypt the entered message......................................................................23

Figure 4.26 Click encode and save it as stego...............................................................24

Figure 4.27 Encoding Time...........................................................................................24

Figure 4.28 Select stego image for decoding.................................................................25

Figure 4.29 Stego image is selected...............................................................................25

Figure 4.30 Time taken in decoding...............................................................................26

Figure 4.31 Hidden message is decoded........................................................................26

**CHAPTER: 1**

**1.1 Objective**

The main objective of this project named “Secret Code Concealer” is to hide the fact that communication is taking place, by hiding information in another information. This project is developed for hiding information in any image file. The scope of the project is implementation of encryption and decryption tools for hiding information which may include any type of information file and image file and the path where the user wants to save image and the extruded file.

For hiding this secret information many encryption and decryption techniques are available some are complex than others and all of them have their respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. The basic usage of this is to hide the private information and maintain the privacy so that the message could only be decrypted by the intended user and not the general public.

The techniques used for hiding the digital media in some other digital media is done by three different encryption and decryption algorithms which are as follows:

* LSB (Least Significant Bit)
* AES (Advanced Encryption Standard)
* Triple DES (Data Encryption Standard)

Now what we are trying to do here is create an informative application by comparing the execution time of all the three algorithms and provide the user with the best and the most effective algorithm to use for concealing their message in a digital media in the least effective time so as to save their time.

This learning and simulation tool will be used further ahead for hiding the secret data inside files will not be visible to the naked eye unless the decryption of the data is done to retrieve the information meant for the rightful receiver. Being a simulation tool it also acts as a learning tool by providing the user with information regarding the working of all the three algorithms and their proficiency in the real world usage by calculating the exact execution time for each algorithm of which the user can then choose the best algorithm to encrypt their data.

**CHAPTER: 2**

* 1. **Introduction**

The goal of this project is covert communication. So, a fundamental requirement of this system is that the hider message carried by the media file or the image file in our case should not be sensible to human beings. What we basically aim at doing is to covertly provide the information to the intended receiver by first encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by the government to limit uses of encryption, the role of this project will gain subsequent prominence.

What this project is intended for is to hide the secret message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

The main thing to be taken care of is that the graphic or audio files which are to be altered do not lose their overall viability for the viewer and the listener. With audio bits of file that contain sound not audible to the human ear can be used. But since we are encrypting the image files only the possible ways include the removal of redundant bits of colour from the image and still produce a picture that looks intact to human eye and is difficult to discern from the original media file.

It is in those bits that the data will be hidden from the general public and by keeping in mind the security risks the data will be provide to the user in form of these bits hidden in the media file which would later be decrypted and would make perfect sense.

The other goal of this project is to avoid drawing suspicion to the existence of the hidden message. This approach of hiding technique has recently become important in a number of application areas. We are going to explore the techniques of hiding data using encryption module of this project and the extraction techniques of getting secret data using the decryption module.

**2.2 What does the project do?**

* Hiding a secret data in cover image .
* Encrypting the same message, so as to support more secure communication.
* The decoding of the message, decryption and source message retrieval are also supported by the project.

**SENDER**

(Image, text file)

**Encoding Algorithm**

**Carrier image**

**Secret Code Concealer**

**Module**

**Decoding Algorithm**

**Plain text**

**RECEIVER**

**Figure 2.1 :- Secret Code Concealer Module**

**2.3 Problem Statement**

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hiding messages physically. One disadvantage of this linguistic form of hiding the messages is that only if the users have enough knowledge about linguistry then only are, they able to encode the messages and even the receiver needs to be aware of the decoding techniques without which the message just seems to be a usual message.

In recent years, everything is trending towards digitization. And with the development of internet technology, digital media can be transmitted conveniently over the network. The problem here arises if the user wants a covert communication just to feel safe about sharing his/her content to the receiver which can be done by the technique of secretly hiding the messages in the digital media files such as images and then transmitted through the internet rapidly.

What we are trying to create here involves the hiding of private or sensitive data to be sent over the internet and hope that even there is a leak of information by any means then it may cause no harm to the user as the image may seem casual to the normal eye until and unless you know how to decode it.

The fact that we are hiding the information in some other information may provide the user with a sense of safety and security. In this growing digital market where digital media plays an important role in our day to day life where millions of images are transmitted daily on the internet the user may be able to covertly conduct a conversation with the required party without worrying about any leak of information. Many digital file formats can be used, but digital images being the most popular due to their frequency on the internet can be preferred for the sharing of information.

There may be a lot of techniques for hiding the secret information or message of which some may be way more complex than others but each one having their own respective strong and weak points. So, we prepare this application, to make the information hiding more simple and user friendly.

**CHAPTER: 3**

**3.1 Technologies Used**

**C #**

C# is a general-purpose, modern and object-oriented programming language pronounced as **“C sharp”**. It was developed by Microsoft led by Anders Hejlsberg and his team within the .Net initiative and was approved by European Computer Manufacturers Association (ECMA) and International Standards Organization (ISO).

C# is among the languages for Common Language Infrastructure and the current version of C# is version 7.2. C# is a lot similar to Java syntactically and is easy for the users who have knowledge of C, C++ or Java.

C# has many other reasons for being popular and in demand. Few of the reasons are mentioned below:

* **Easy to start:** C# is a high-level language so it is closer to other popular programming languages like C, C++, and Java and thus becomes easy to learn for anyone.
* **Widely used for developing Desktop and Web Application:**  
  C# is widely used for developing web applications and Desktop applications. It is one of the most popular languages that is used in professional desktop. If anyone want to create Microsoft apps, C# is the go-to language.
* **Community:** The larger the community the better it is as new tools and software’s will be developing to make it better. C# has a large community so the developments are done to make it exist in system and not become extinct.
* **GameDevelopment:**  
  C# is widely used in game development and will continue to dominate. C# integrate with Microsoft and thus has a large target audience. The C# features such as Automatic Garbage Collection, interfaces, object oriented etc. makes C# a popular game developing language.

**.NET FRAMEWORK**

The .NET framework is a software development framework from Microsoft. It provides a controlled programming environment where software can be developed, installed and executed on Windows-based operating systems. So this is a framework designed for Microsoft Windows.  
  
The principal design features are:

* **Interoperability**: This allows for .NET-developed programs to access functionalities in programs developed outside .NET.
* **Common Runtime Engine**: Also known as the common language runtime, this allows programs developed in .NET to exhibit common behaviour in memory usage, exception handling and security.
* **Language Independence**: Common language infrastructure specifications (CLI) allow for the exchange of data types between two programs developed in different languages.
* **Base Class Library**: A library of code for most common functions--used by programmers to avoid repetitive rewriting of code.
* **Ease of Deployment**: There are tools to ensure the ease of installing programs without interfering with previously installed applications.
* **Security**: Programs developed in .NET are based on a common security model.

**3.2 Software Details**

**VISUAL STUDIO**

Microsoft Visual Studio is an integrated development environment from Microsoft. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps. Visual Studio IDE is a full-featured development platform for multiple operating systems as well as the web and the cloud. It allows users to smoothly navigate the interface so they can write their code speedily and accurately. Visual Studio IDE also serves as a testing interface. Languages which can be used in Visual Studio are C++ and C#.

It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight.

Additional components and tools of Visual Studio Code includes a small download by design and only includes the minimum number of components shared across most development workflows. Basic functionality like the editor, file management, window management, and preference settings are included.

There are three editions of Visual Studio IDE which are as follows:

* Community
* Professional
* Enterprise

It is not a language-specific IDE as you can use this to write code in C#, C++, VB (Visual Basic), Python, JavaScript, and many more languages. It provides support for 36 different programming languages. It is available for Windows as well as for macOS.

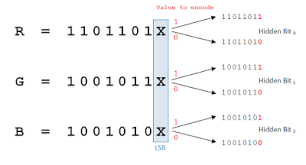
**3.3 Algorithms Used**

**3.3.1 LSB Algorithm**

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit in other words, the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message.

When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types.

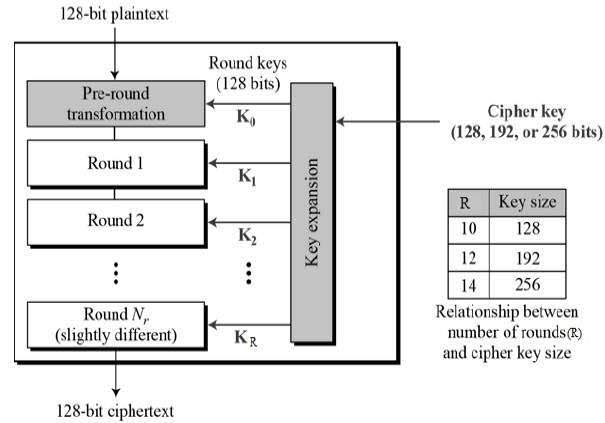


**Figure 3.1 :- LSB Algorithm**

**3.3.2 AES Algorithm**

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

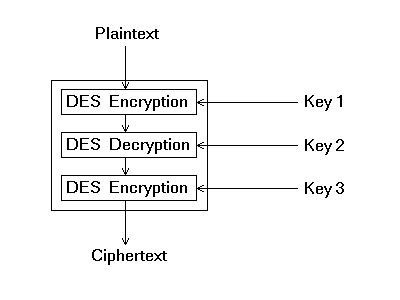


**Figure 3.2 :- AES Algorithm**

**3.3.3 TripleDES Algorithm**

Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryptor, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.



**Figure 3.3 :- Triple DES Algorithm**

**3.4 Site Plan for Encoding**

**Figure 3.4 :- Site Plan For Encoding**

Encode

Encode

Encrypt The Text Message

Encrypt The Text Message

Encode

Write Text Message to Hide

Write Text Message to Hide

Write Text Message to Hide

Select Cover Image

Select Cover Image

Select Cover Image

Advanced Encryption Standard

(AES)

Least Significant Bit

(LSB)

Triple Data Encryption Standard

(Triple DES)

**Start Application**

**3.5 Site Plan for Decoding**

**Start Application**

Select Encrypted Image

Text Message

Decode

Advanced Encryption Standard

(AES)

Least Significant Bit

(LSB)

Triple Data Encryption Standard

(Triple DES)

**Figure 3.5 :- Site Plan For Decoding**

**CHAPTER: 4**

**4.1 Result Analysis (Screenshots)**

Start the application, Secret Code Concealer



Figure 4.1 :-Starting of Secret Code Concealer

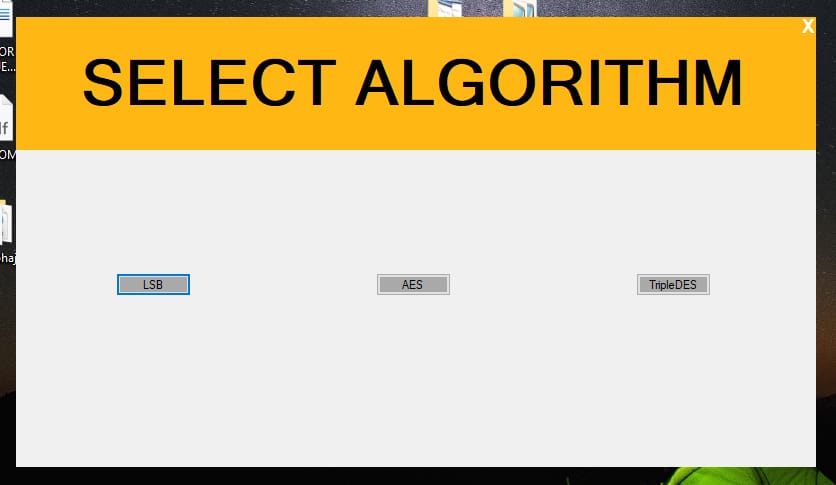


Figure 4.2 :-Select from the following algorithms

On selecting LSB Algorithm

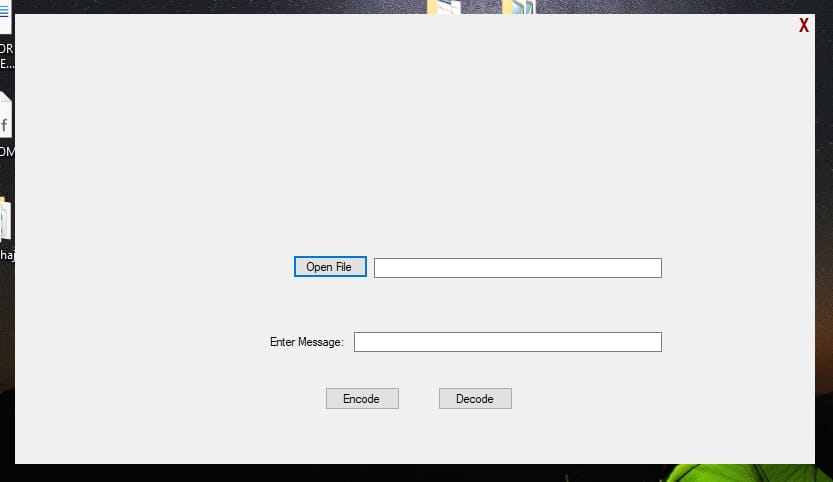


Figure 4.3 :-Click on open file to select cover image

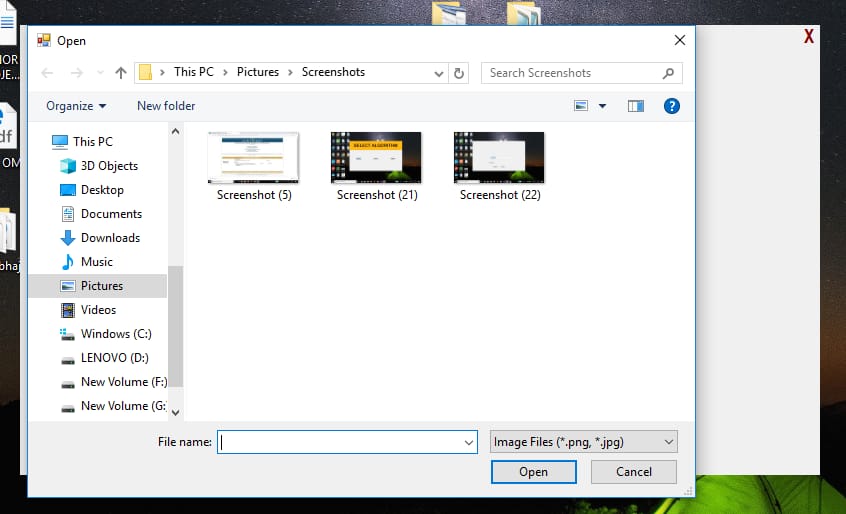


Figure 4.4 :-Select cover image

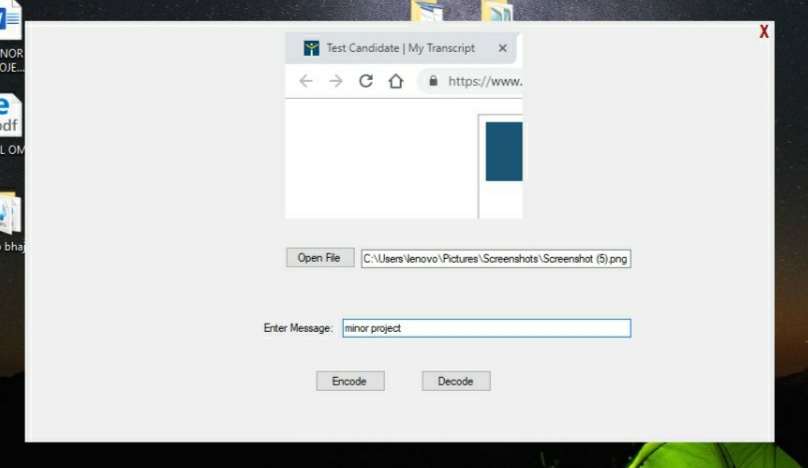


Figure 4.5 :-Enter message to hide

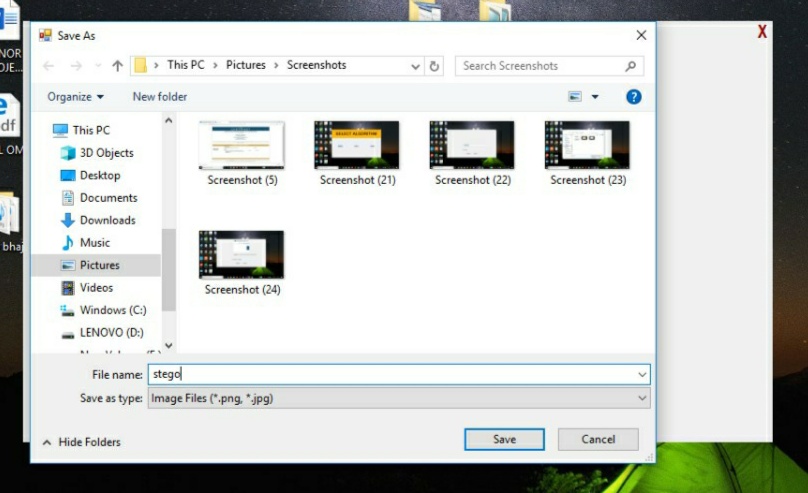


Figure 4.6 :-Click encode and save it as stego

Time taken in encoding

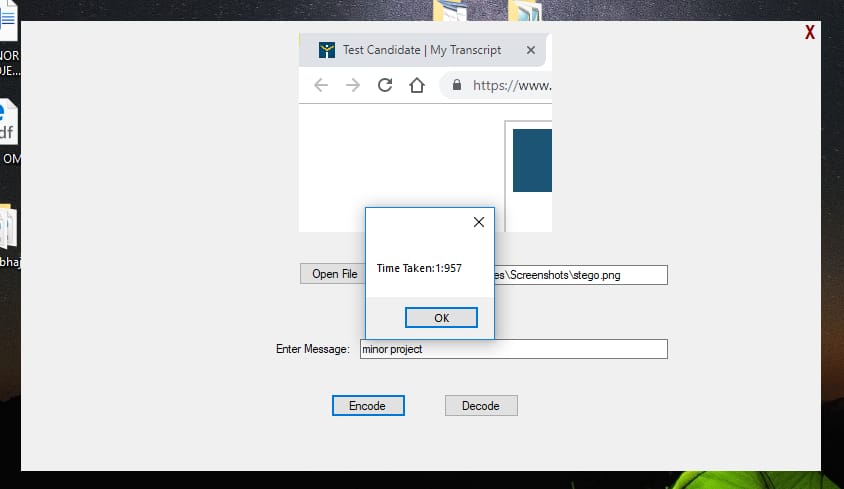


Figure 4.7 :- Encoding Time

Open LSB again for decoding

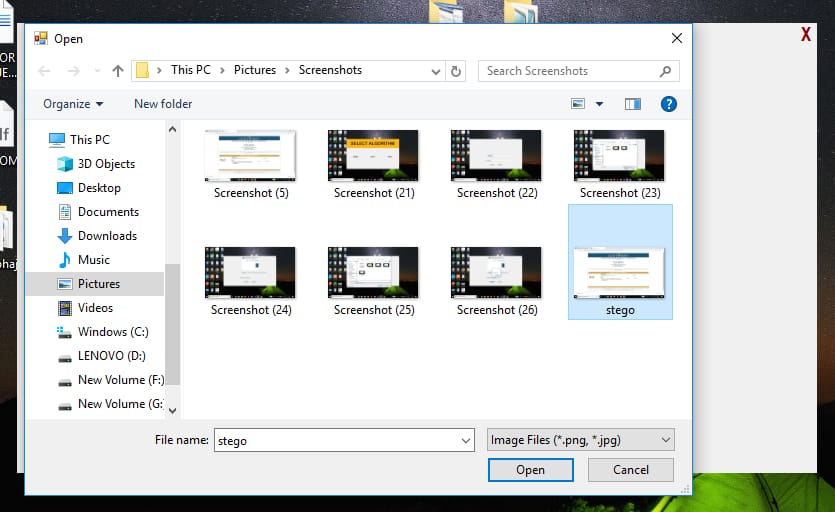


Figure 4.8 :-Select stego image for decoding

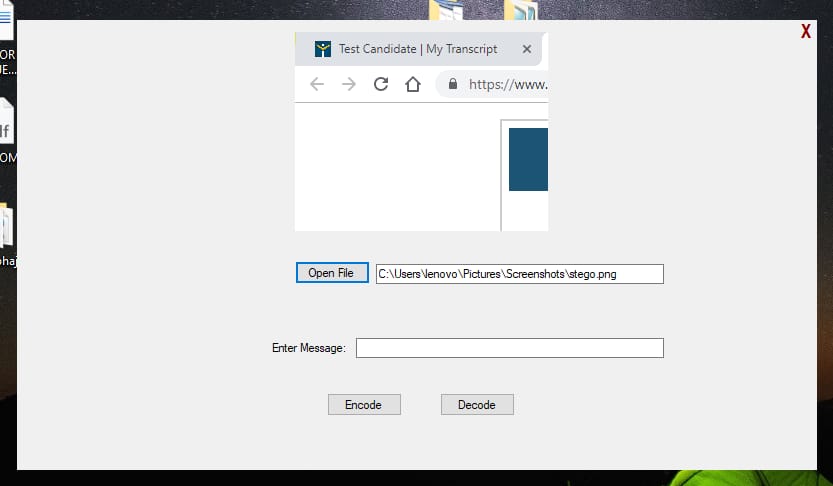


Figure 4.9 :-Stego image is selected

Click decode

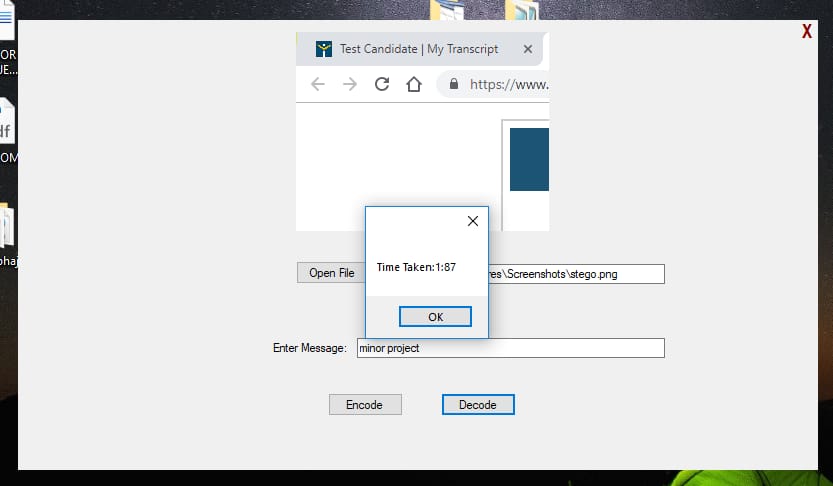


Figure 4.10 :-Time taken in decoding

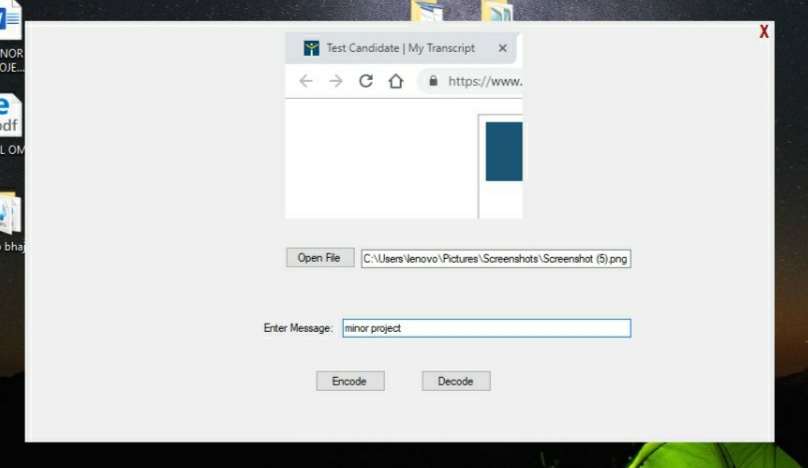


Figure 4.11 :-Hidden message is decoded

On selecting AES Algorithm

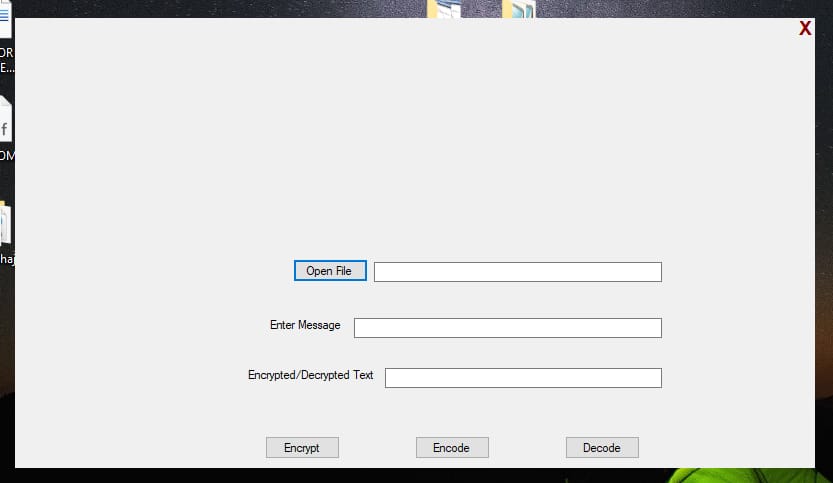


Figure 4.12 :-Click on open file to select cover image

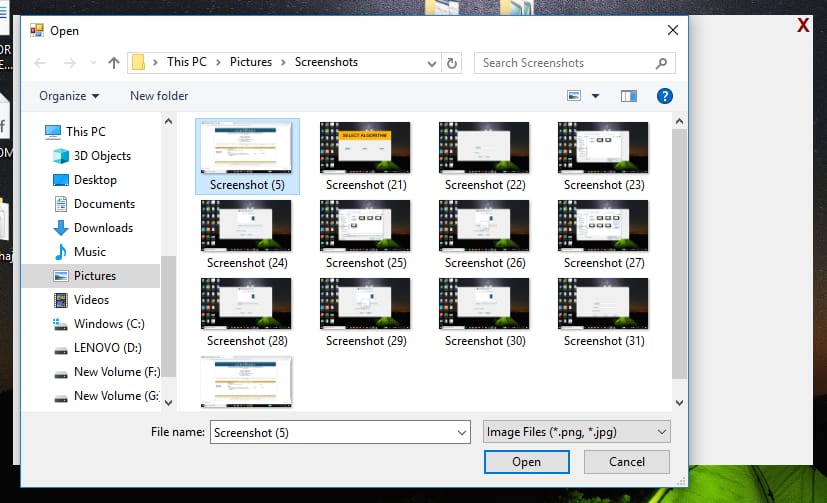


Figure 4.13 :-Select cover image

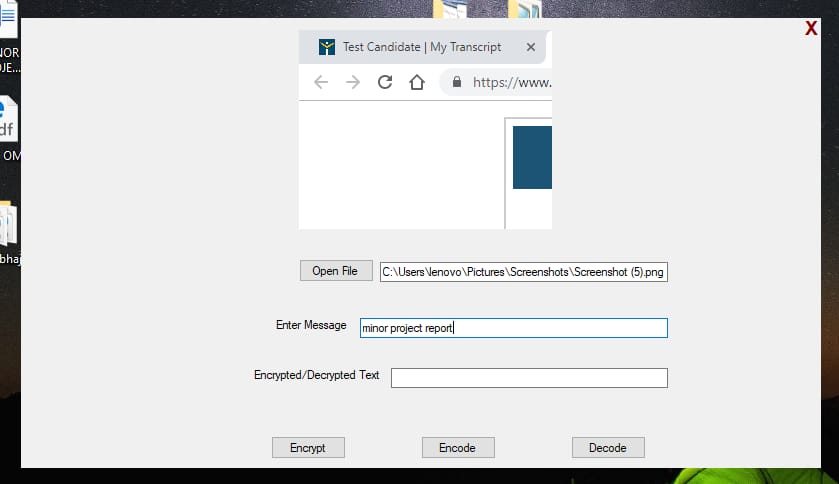


Figure 4.14 :-Enter message to hide

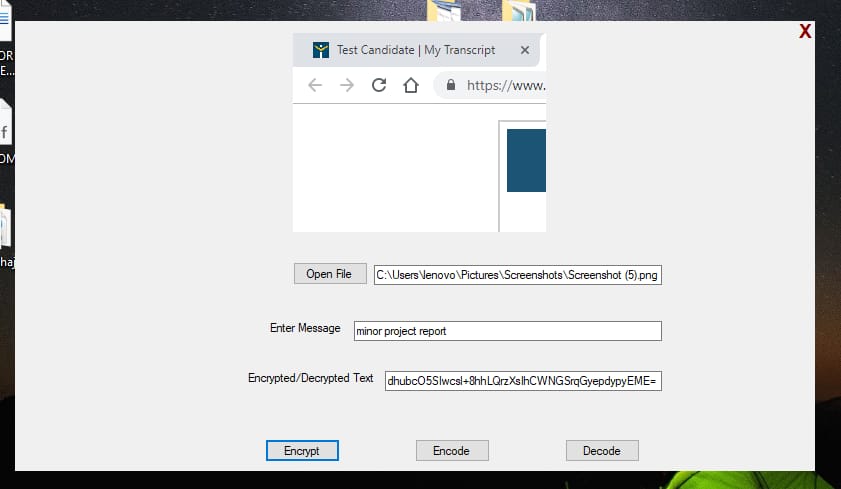


Figure 4.15 :-Encrypt the entered message

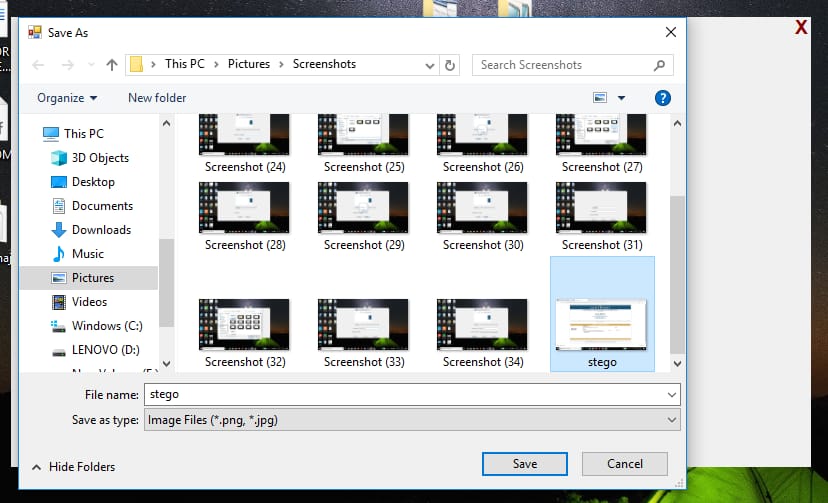


Figure 4.16 :-Click encode and save it as stego

Time taken in encoding

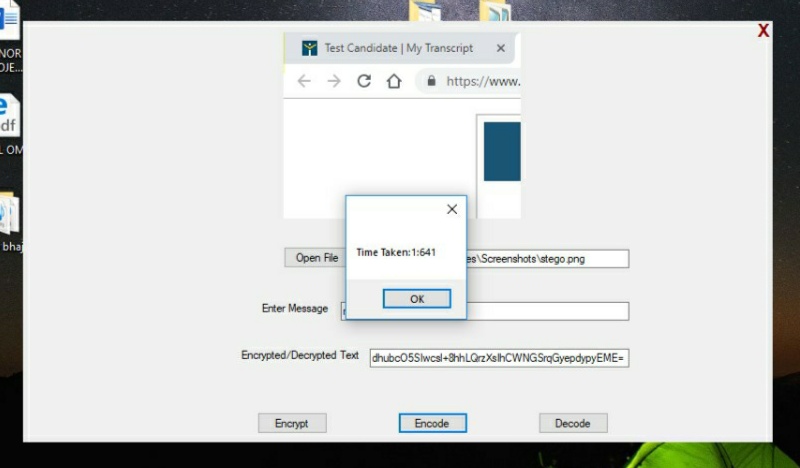


Figure 4.17 :- Encoding Time

Open AES again for decoding

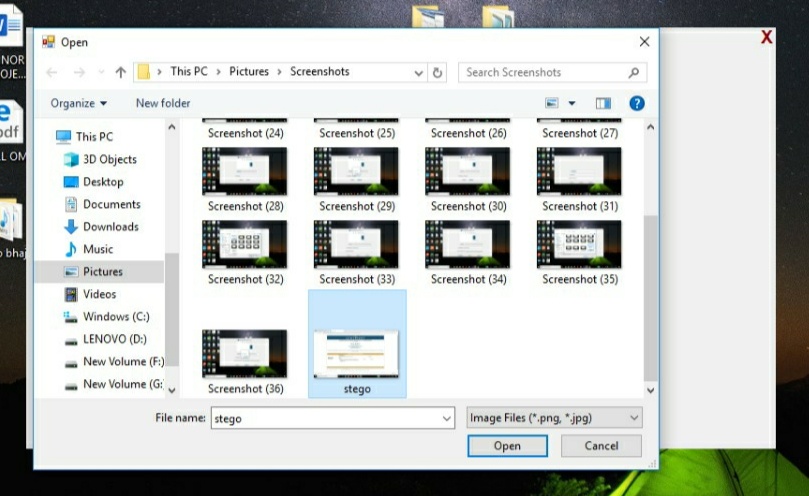


Figure 4.18 :-Select stego image for decoding

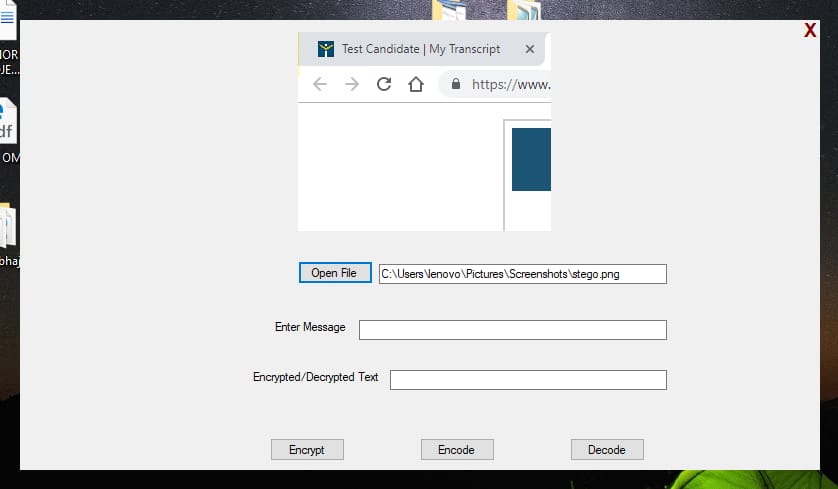


Figure 4.19 :-Stego image is selected

Click decode

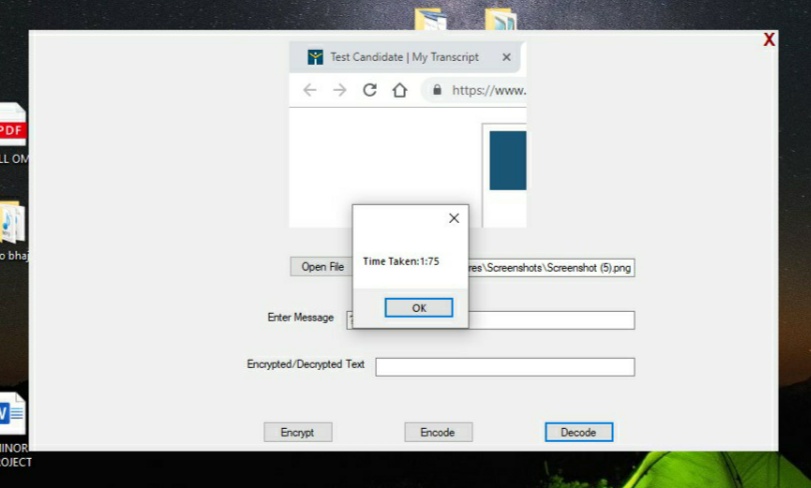


Figure 4.20 :-Time taken in decoding

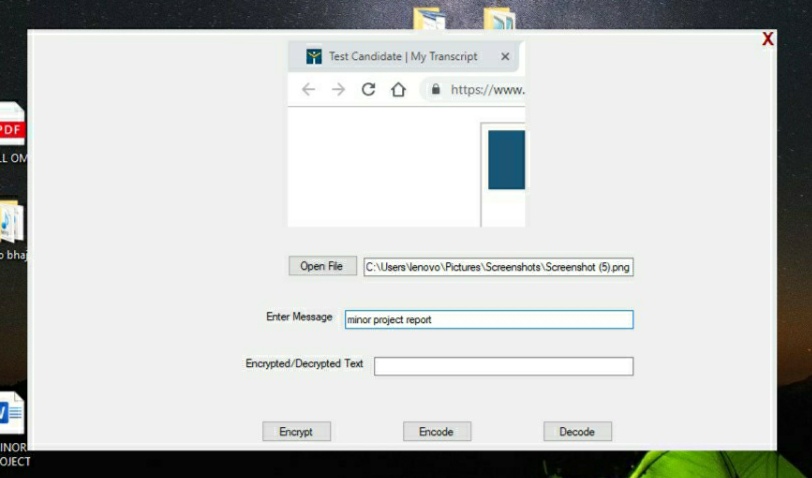


Figure 4.21 :-Hidden message is decoded

On selecting Triple DES Algorithm

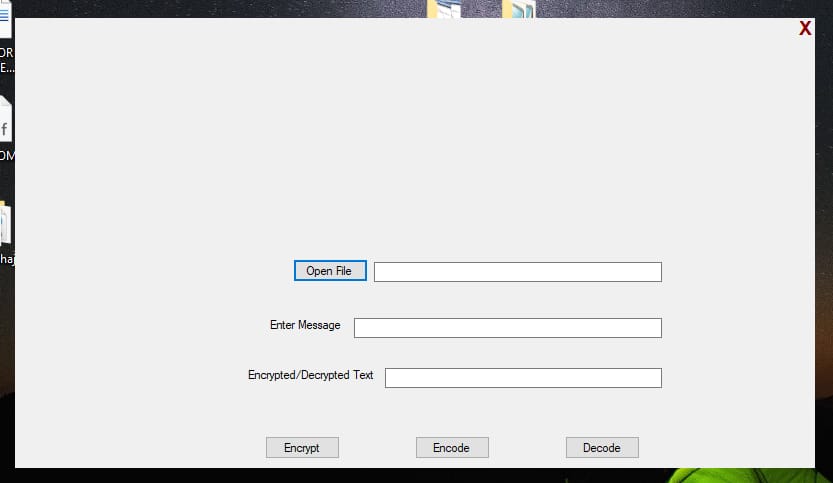


Figure 4.22 :-Click on open file to select cover image

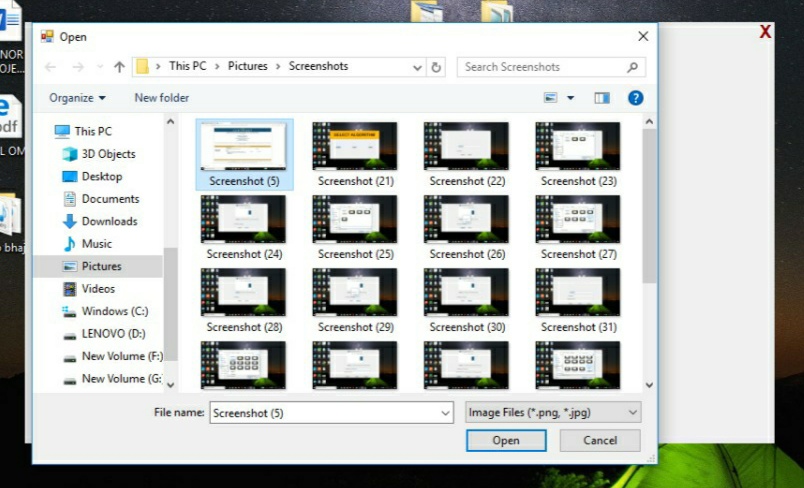


Figure 4.23 :-Select cover image

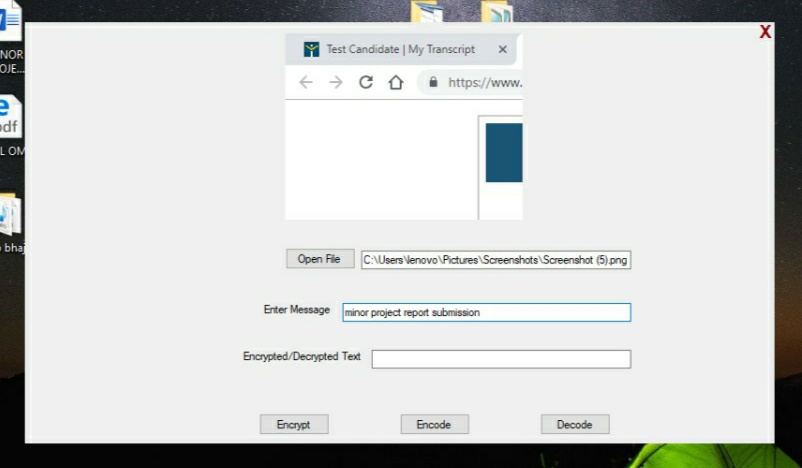


Figure 4.24 :-Enter message to hide

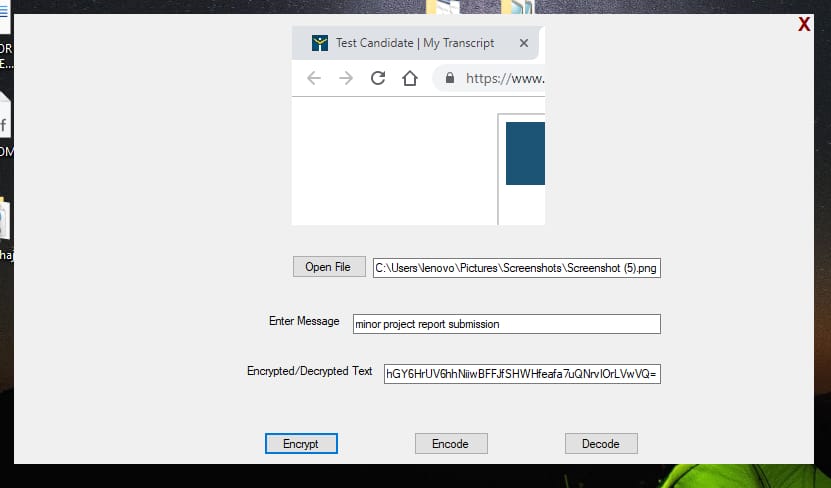


Figure 4.25 :-Encrypt the entered message

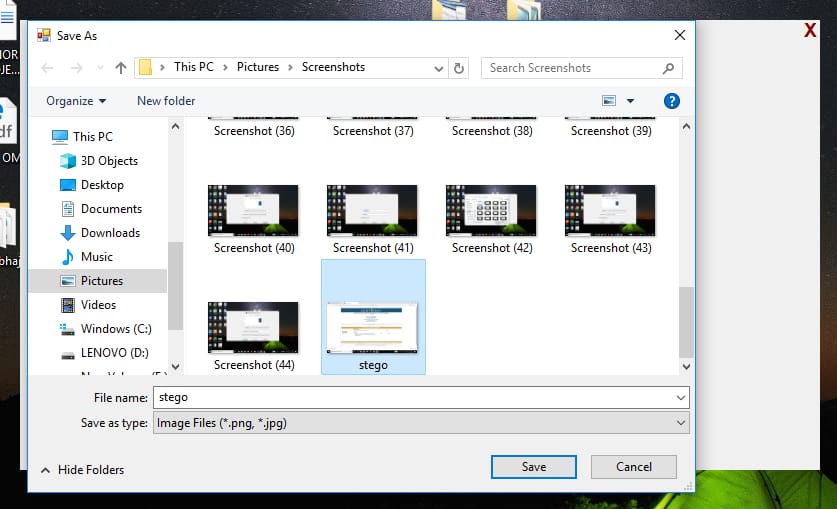


Figure 4.26 :-Click encode and save it as stego

Time taken in encoding

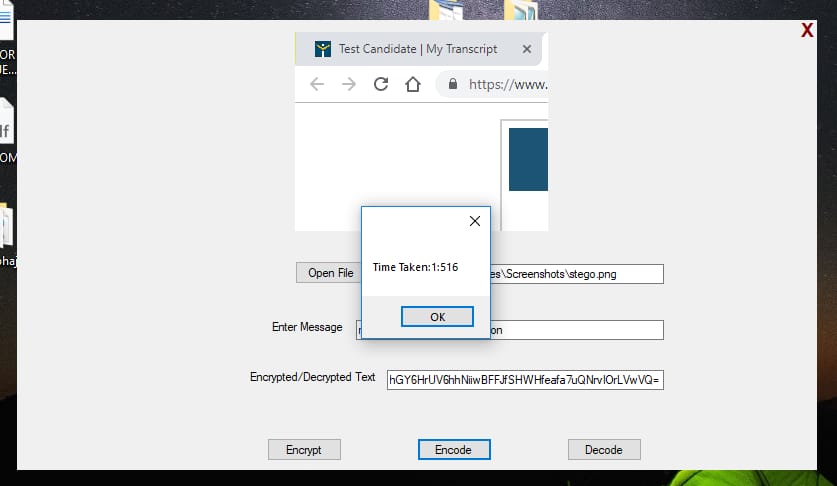


Figure 4.27 :- Encoding Time

Open Triple DES again for decoding

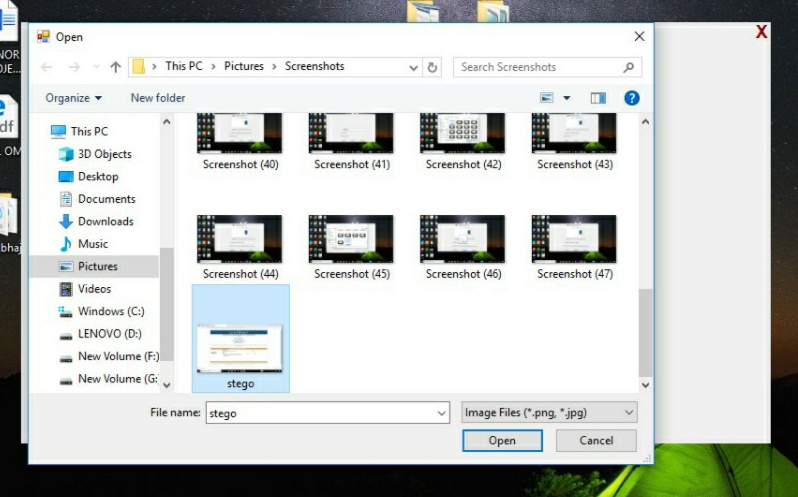


Figure 4.28 :-Select stego image for decoding

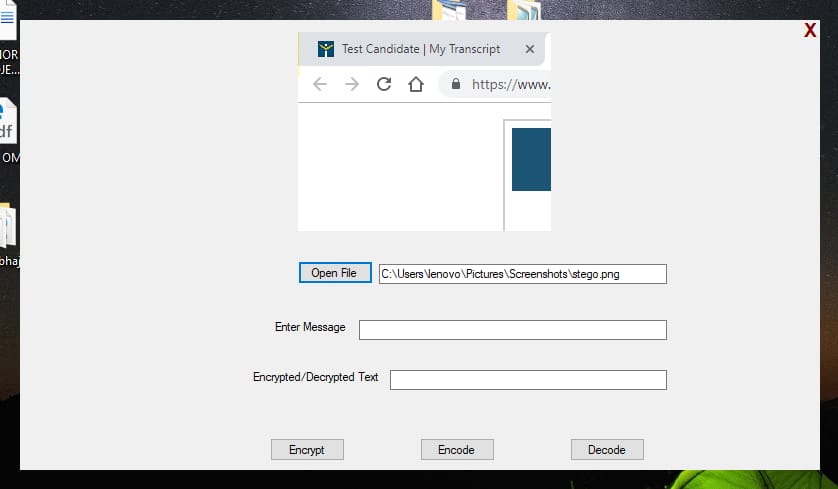


Figure 4.29 :-Stego image is selected

Click decode

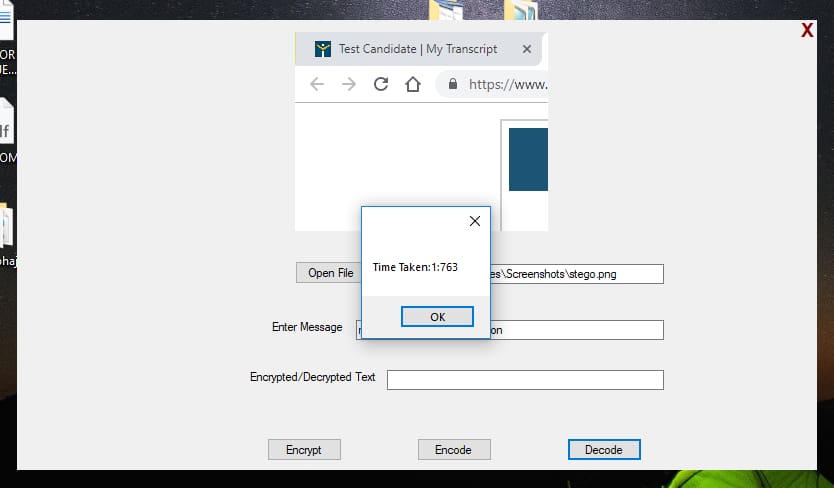
****

Figure 4.30 :-Time taken in decoding

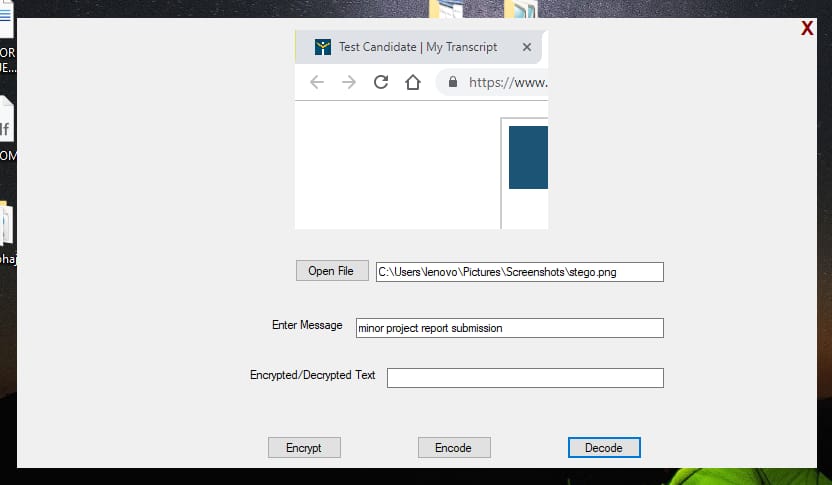
****

Figure 4.31 :-Hidden message is decoded

**CONCLUSION**

This project mainly focuses on the different encryption and decryption mechanisms acting as a learning and simulation tool, making the user aware of which algorithm is best suited for a more secure communication or much faster and efficient communication by hiding the messages inside the digital media.

We learned that the algorithms we used had varying encryption and decryption timings and the most efficient and faster of them all was the LSB algorithm as it was simply encoding the message and decoding it. It was further followed by the AES algorithm which was first encrypting the text to be hidden and then encoding it inside the media file. Finally the algorithm which took the most time for the whole encryption and decryption process was Triple DES. Although the expected outcome was believed to give the result as above but the final outcome had a varying result as LSB took the most amount of time even if same message was setup to be encrypted followed by AES and Triple DES which took the least time as compared to the LSB algorithm.

So we learned that LSB being simpler in mechanism is not faster algorithm as expected as AES and Triple DES is and thus it is totally upto the user to choose between security and easy accessibility and efficient use of an algorithm.

**REFERENCES**

[1] <https://www.cybrary.it/0p3n/hide-secret-message-inside-image-using-lsb-steganography/>

[2] <https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm>

[3] <https://www.commonlounge.com/discussion/5c7c2828bf6b4724b806a9013a5a4b99>