DATA HIDING METHODS

Report submitted to the SASTRA deemed to be

University as the requirement

of the course

EIE303: VIRTUAL INSTRUMENTATION

Submitted by

KASA SAI RANGA PHANI SHANKAR

(Reg.No:124006016**)**

DECEMBER 2022

SCHOOL OF **ELECTRICAL AND ELECTRONICS ENGINEERING**
THANJAVUR,
TAMIL NADU,
INDIA-**613401**

SASTRA

ENGINEERING · MANAGEMENT · LAW · SCIENCES · HUMANITIES · EDUCATION

DEEMED TO BE UNIVERSITY

(U/S 3 of the UGC Act,1956)

THINK MERIT | THINK TRANSPARENCY | THINK SASTRA

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

THANJAVUR-613401

Bona-fide Certificate

This is to certify that the project report titled "**DATA HIDING METHODS**" submitted as the requirements for the award of the degree of B.Tech. Electronics and Instrumentation Engineering to the SASTRA Deemed to be University, is a Bona-fide record of the work done by **Mr. KASA SAI RANGA PHANI SHANKAR** (Reg.No.124006016) during the 5th semester of the academic year 2021-22 in the **School of Electrical and Electronics Engineering,** under my supervision. This project report has not formed the basis for the award of any degree, diploma, associate ship, fellowship or other similar title to any candidate of any University.

Signature of Project Supervisor :

Name with Affiliation :

Date :

Project Viva-voce held on _____

Examiner 1 Examiner 2

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING
THANJAVUR-613401

Declaration

I declare that the project report titled "**DATA HIDING METHODS**" submitted by me is an original work done by me under the guidance of **PROF. Bagyalakshmi.G**, **School of Electrical and Electronics Engineering**, **SASTRA Deemed to be University** during the 5th semester of the academic year 2021-22, in the **School of Electrical and Electronics Engineering**. The work is original and wherever I have used materials from other sources, I have given due credit and cited them in the text of the project report. This project report has not formed the basis for the award of any degree, diploma, associate-ship, fellowship or other similar title to any candidate of any University.

Signature of the candidate(s) :

Name of the candidate(s) : **KASA SAI RANGA PHANI SHANKAR**

Date :

Acknowledgements

I would like to express my deepest appreciation to all those who aided me to complete this project and whose contribution is stimulating suggestions and encouragement, helped me to coordinate my project especially in writing this report.

I would like to extend my sincere gratitude to **Dr. S. Vaidhyasubramaniam**, Vice Chancellor, SASTRA Deemed to be University**, Dr. R. Chandramouli,** Registrar, SASTRA Deemed to be University, **Dr. S. Swaminathan**, Dean, Planning and Development, SASTRA Deemed to be University, **Dr. K. Thenmozhi**, Dean, EEE Department, School of Electrical and Electronics Engineering, SASTRA Deemed to be University, and **Dr.A.Krishnamoorthy**, Associate Dean, EIE Department, School of Electrical and Electronics Engineering, SASTRA Deemed to be University, for providing us with the opportunity.

I owe a debt of earnest gratitude towards my guide **PROF. Bagyalakshmi.G** /SEEE for her continued support and guidance throughout the course of our work. I also take immense pleasure in thanking her as the project coordinator for guiding us through various steps in submitting the project.

I am thankful to the guidance given by other supervisors, the panels in the project presentation that has aided me in improving my presentation skills and my parents for their constant support throughout the completion of my project.

ABSTRACT

Technology in Computers and the Internet have made a new milestone in the existence of data communication. Securing the data transfer over a transmission media has become of great importance. The data that is exchanged every day may become the victim of hackers. So we have to use certain Data Hiding Methods to deal with the issue.

Data encryption and decryption are used in data hiding techniques to protect data from hackers. The data is concealed using this technique to prevent hacking. The methods of data concealing that are the subject of this project include text-cryptography and image-steganography. While the goal of these two techniques is the same—to conceal the secret data—the process for doing so varies. In order for no one to decipher the secret information, it is jumbled using cryptographic techniques.

In text encryption, the text is concealed in a.txt file with unintelligible characters. Additionally, the methodology makes use of unique algorithms like FFT and IFFT. The FFT algorithm is used in encryption to extract unintelligible characters and vice versa. The text-decryption module is used on the receiver side to recover the original text. In order to disguise data, image-steganography repeats sequentially-placed bits in an image file that represent the same colour pixels. An image file that resembles the original image will be produced by employing this encrypted data in this outdated data and then incorporating it in the design.

This project employs an effective design to encrypt and decrypt any text or image file. The design of the method is implemented in LabVIEW software because it offers a number of benefits, including easy implementation, flexibility, modularity, an appealing user interface, and the ability to easily build any new technology.

Anti-forensic techniques such as steganography are used to conceal sensitive information beneath a cover medium. The method most frequently employed to conceal data is steganography.

The main moto of this project is to implement the Data Hiding Methods to hide contents safely and securely from being detected by unknown person or hackers.

Keywords: Encryption, Decryption,Cryptography, Steganography ,LaBVIEW

Table of Contents

LIST OF FIGURES

ABBREVIATIONS

ABBREVIATIONS	CLARIFICATIONS
LabVIEW	Laboratory Virtual Instrument Engineering Workbench
FFT	Fast Fourier Transform
IFFT	Inverse Fast Fourier Transform

CHAPTER 1

INTRODUCTION

The "Internet" is a vital component of daily living in the modern world. The internet's explosive expansion has greatly simplified people's daily lives. The most popular online shopping site, online bill payment, online money transfers, online ticket booking, online recharging, etc. are a few instances that show how to use the internet.

Social networking apps like Facebook, Twitter, Instagram, WhatsApp, and others are another feature that has a significant impact on our life. People are sharing their vital documents and information with one another as a result of this feature. Through the internet, people exchange secret and private information with one another. Private data transfers across the internet run the risk of being hacked. Security is therefore of the utmost importance while sending data through Internet.

Steganography is a widely used method of secure communication. It is used to conceal secret messages within a cover image in order to protect data from third parties. There are various methods for encrypting data to keep the message secret, one of which is cryptography. Message encryption and decryption were used in cryptography to provide security. Data information is hidden in cover information in the case of steganography. Steganography overcomes the disadvantage of cryptography in that the existence of the message is also not visible because in some communications encrypting the data is insufficient. Image steganography is used in this project. Image steganography employs both data and cover information in the form of images. It conceals the existence of the data media by concealing the data information in a cover media without making any visible changes to it. Steganography is primarily used to conceal the existence of data media in text, audio, video, image, and protocol media without making any visible changes to them. It makes use of image data as well as cover information. It conceals the data information

CHAPTER 2

REVIEW OF RELATED LITERATURE

2.1 ENCRYPTION AND DECRYPTION OF TEXT FILE USING LabVIEW

Year: 2018

Author's name: Balaji Tat, Surya Prasad Rao Borra, Geetha Devi Appari

Publication name: IJRECE VOL. 6 ISSUE 3

This paper explains about an efficient method used to encrypt any text file and decrypt it using Fast Fourier Transform and Inverse FFT algorithms respectively.

2.2 REVIEW OF IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES FOR 2D IMAGES

Year: Jan 2016

Author's name: Jalpa Shah and J. S. Dhobi

Publication name: International Journal of Engineering Technologies and Management and Research.

This journal says about that we can use grayscale image or any other parameters to hide the original image.

2.3 IMPLEMENTATION OF IMAGE STEGANOGRAPHY USING LabVIEW

Year: Feb-2018

Author's name: Shanthamma K, Sanket N Shettar, Senthilkumar S

Publication name: IJASET

This journal explains about the technique steganography which is used for hiding secret image within a cover image to hide the data from the unknown person.

CHAPTER 3

PROPOSED SCHEME

3.1. Text Cryptography

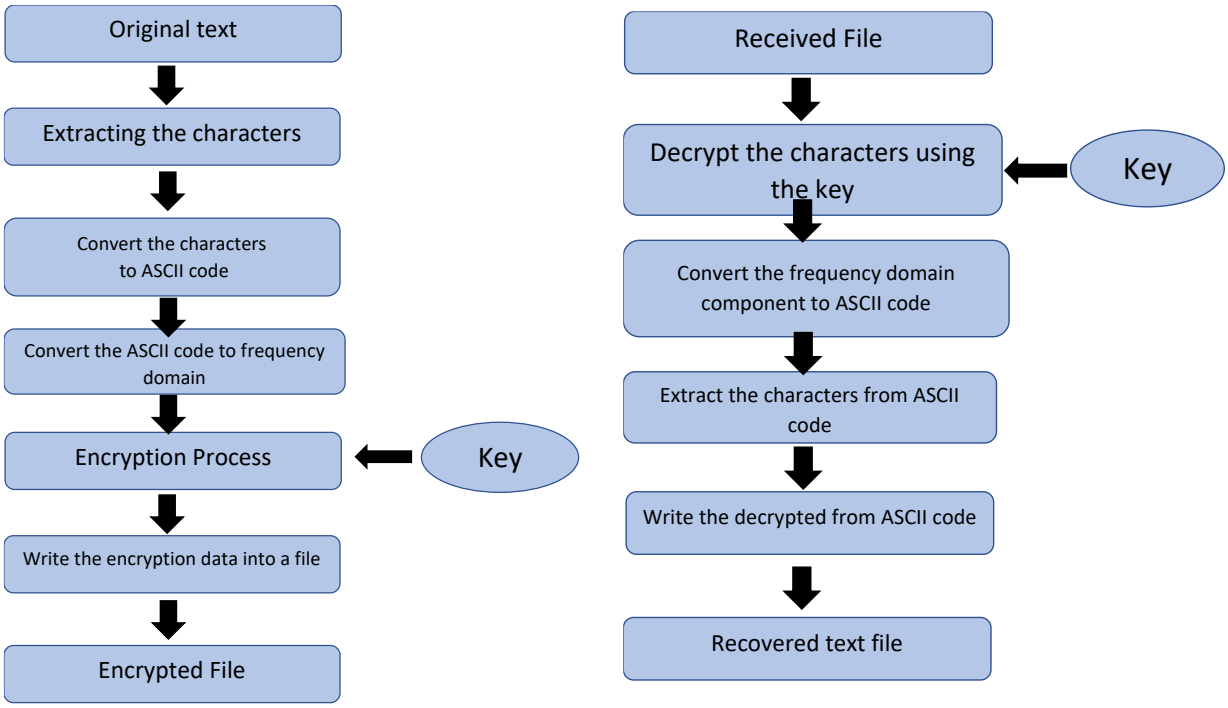

Fig. 3.1: Proposed algorithm for text cryptography

Process of encryption of text file in another .txt file:

- The Encryption module offers the ability to encrypt a text file, which renders it unreadable (or cypher text).
- First the text file is to be created for the encryption process.
- The location of this file is given as input.
- Every character of the data is extracted and converted into ASCII codes.

- The codes are then encrypted using the FFT algorithm.
- As a result, a series of complex numbers are generated.
- The required encrypted output is obtained after running the FFT algorithm.
- The encrypted output is saved and stored into a new transmitting file and the location of it will be displayed in the front panel too.

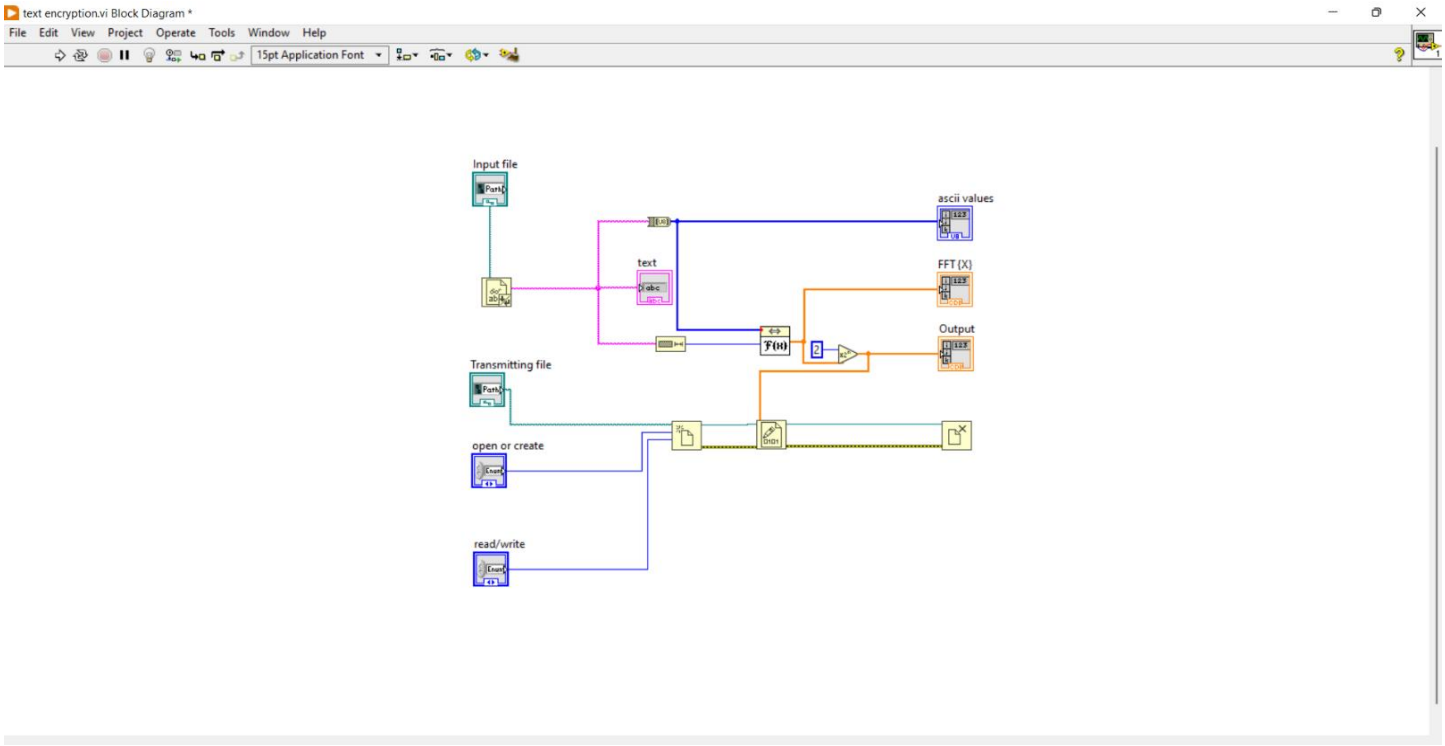

Fig 3.2: **Block diagram of text-encryption module**

To begin the process of encrypting a text file, the original file which has to be encrypted must first be located using the file path control. A series of characters make up the original text file in its entirety. The text file is initially read via the "read from text file" function, from which the string values are carried and transformed to an unsigned byte array, in order to convert the text file into ASCII character values as suggested by the algorithm (8-bit integer 0-255).

The ASCII values {X} obtained are passed to a function for determining the Fast Fourier Transform (FFT). The FFT{X} will have an array of complex numbers. This FFT{X} is made 4x and the output data is encrypted into a text file (i.e. transmitting file).

The file is opened using the "open/create/replace file" function once the transmitting file path location is specified as the control. The "write to binary file" function is now related to both the output data and the transmitting file. This causes the output data to be transformed into unintelligible cypher text in some way. The figures for the text and sending files are listed below.

Fig 3.2: Original text file

Fig 3.3: Transmitting file

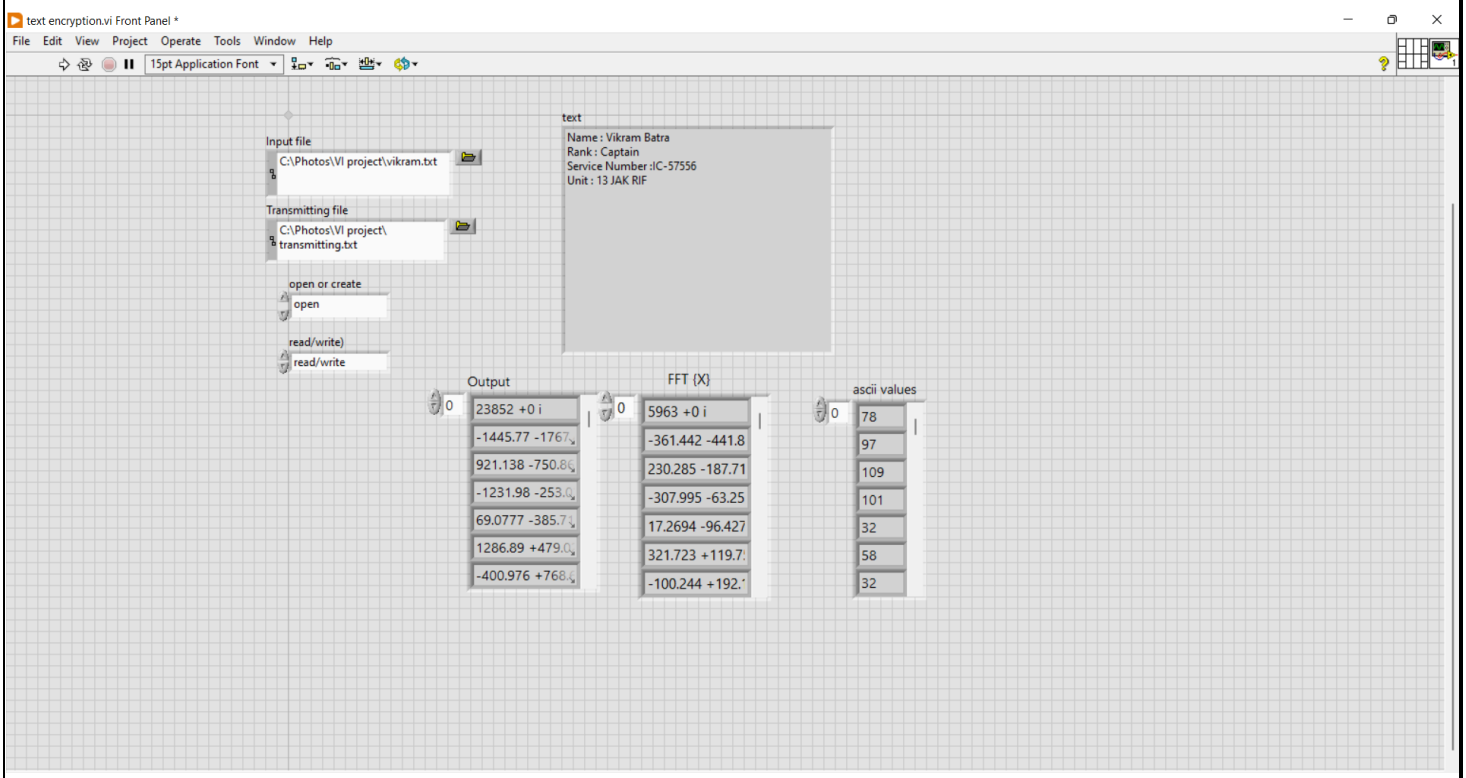

Fig 3.4: Front panel of the text-encryption

Process of decryption of the transmitting text file into the original text file:

- The application's decryption module, which receives encrypted text files from the encryption module, is another crucial component.
- In order to decrypt encrypted data or restore it to its original form, the user must first supply the file location of the transmitting text file containing the data.
- The following step is to extract all of the coded characters from the necessary file.
- The file is then subjected to IFFT algorithm.
- The result is the required decrypted output data.
- This is then displayed and saved to a different file location.

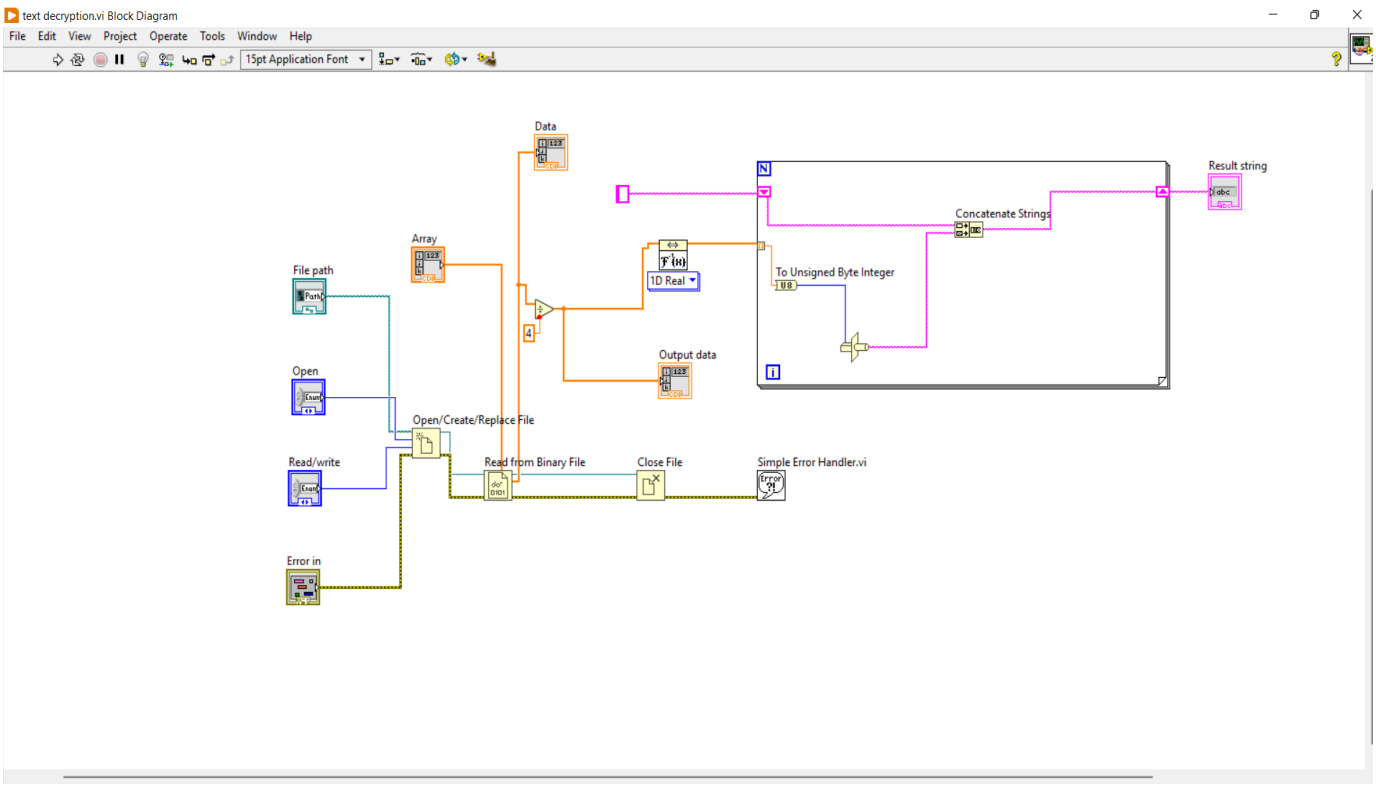

Fig3.5: **Block diagram for text-decryption**

For the decryption process, the transmitting file path location control is opened using the 'open/create/replace file' function. The transmitting text file has only unknown characters which are to be decoded, so the transmitting file is passed on for reading. The 'read from binary' function can assign the data type for the data which it will read and it has been given as complex double for the complex numbers that it will read.

Data representing complex values is displayed as an array and divided by four (4x in encryption). An array is also used to display this divided data. The resultant complex values are put via the Inverse Fast Fourier Transform (IFFT).

The resultant IFFT values are then supplied to a loop, where the "to unsigned byte integer" function transforms them into unsigned 8-bit integers (0–255). The numbers are now flattened and unflatten before being cast to a string type data type using the "type cast" method. LabVIEW employs a temporary buffer when the function needs reinterpret data rather than transform it.

In order to combine many strings into a single output string, the "concatenate strings" function is utilised. On the front panel, it is noted that there is only one output string. The needed string type output is the final output that is obtained.

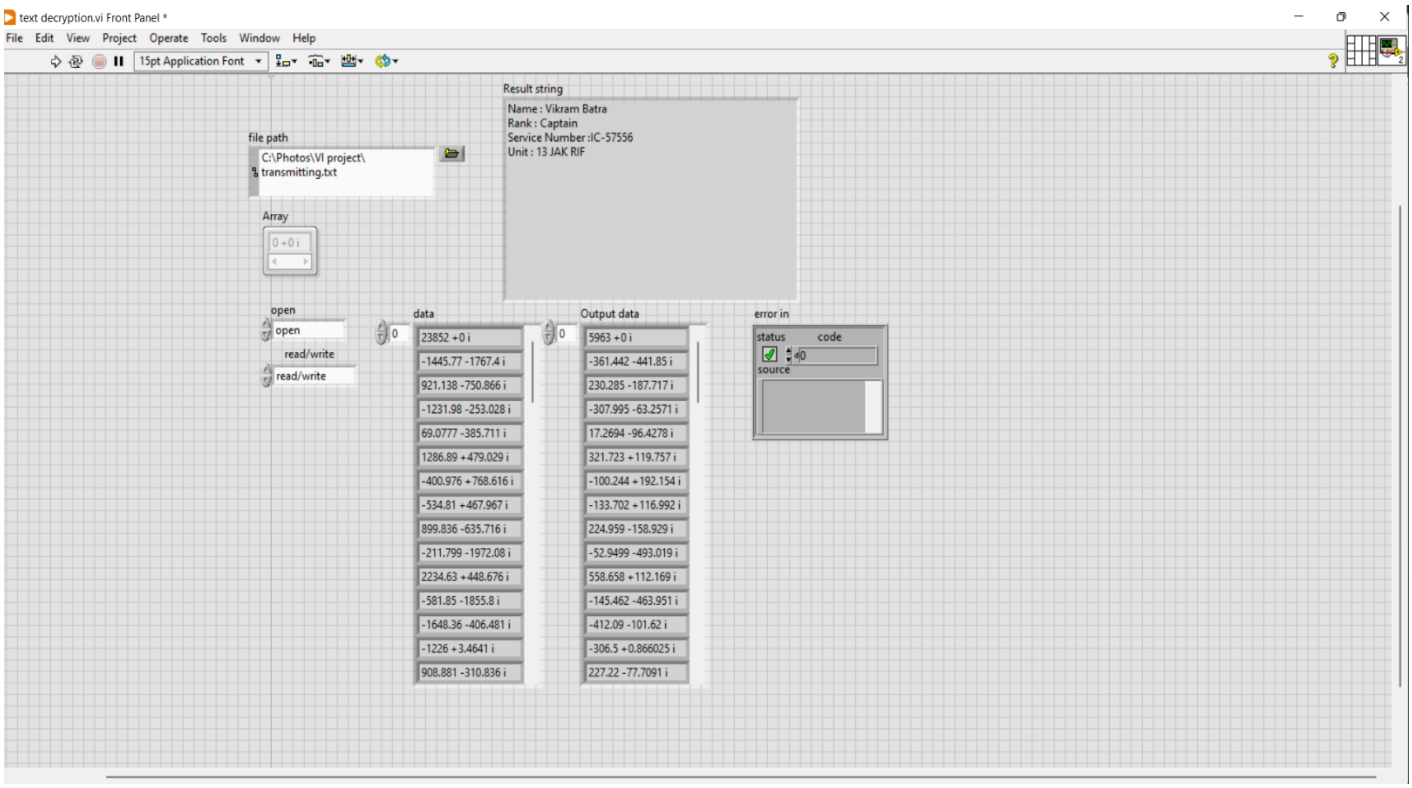

Fig 3.6: **Front panel of Text-Decryption module**

3.2. Image Steganography

The primary moto of this system is to encode the secret image inside the cover image and decode the obtained steago image to get the secret and cover image.

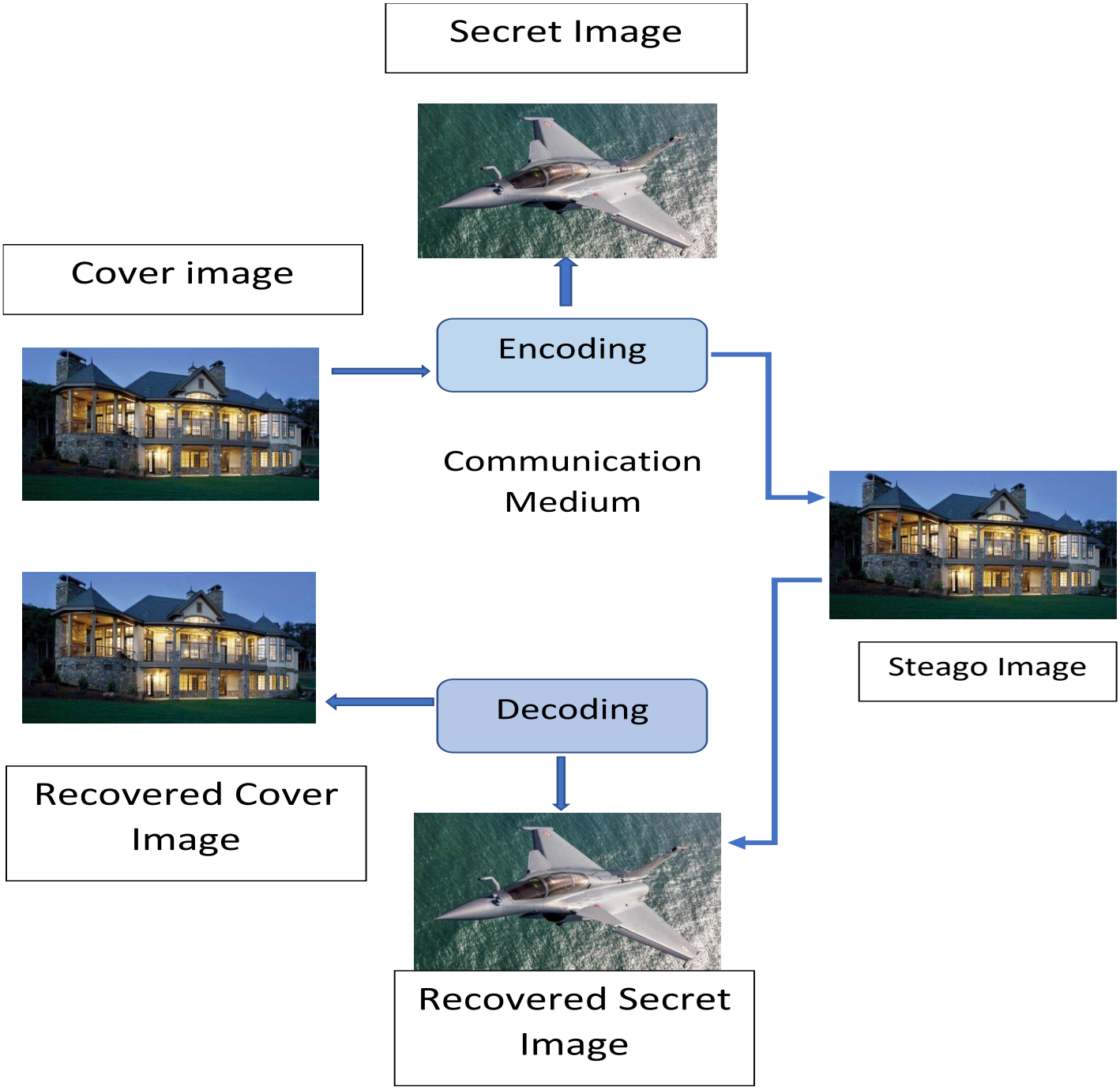

Fig. 3.7: Proposed flow diagram for image steganography

The cover image is initially selected for encoding from the PC's file location, and the pixels' values are extracted, followed by the RGB values of each pixel value. The cover image's 2D RGB array is transformed into a 1D array. Similar to this, the components of vision acquisition software are used to capture the data image, and the data image's pixel values are then retrieved. Additionally, the data image's 2D R, G, and B array is converted to a 1D array.

The column and row sizes of the data image are extracted and saved as global variables during the encoding process. Each RGB value of the Data Image is searched from the reshaped 1D RGB array of the Cover Image, and the index values are returned. R, G, and B index values are also converted into global variables.

The cover image used in the decoding process is the same as the cover image used in the image-encryption module. The RGB values of each pixel are extracted from the cover image, and the 2D RGB array of the data image is then converted to a 1D array. Each RGB element in the Data image is searched for in the Cover Image. For searching, the global variables are taken from the Image-encryption module. The global variables are used to extract the 2D RGB values of the data image, which are then combined with the RGB values to extract the Data Image.

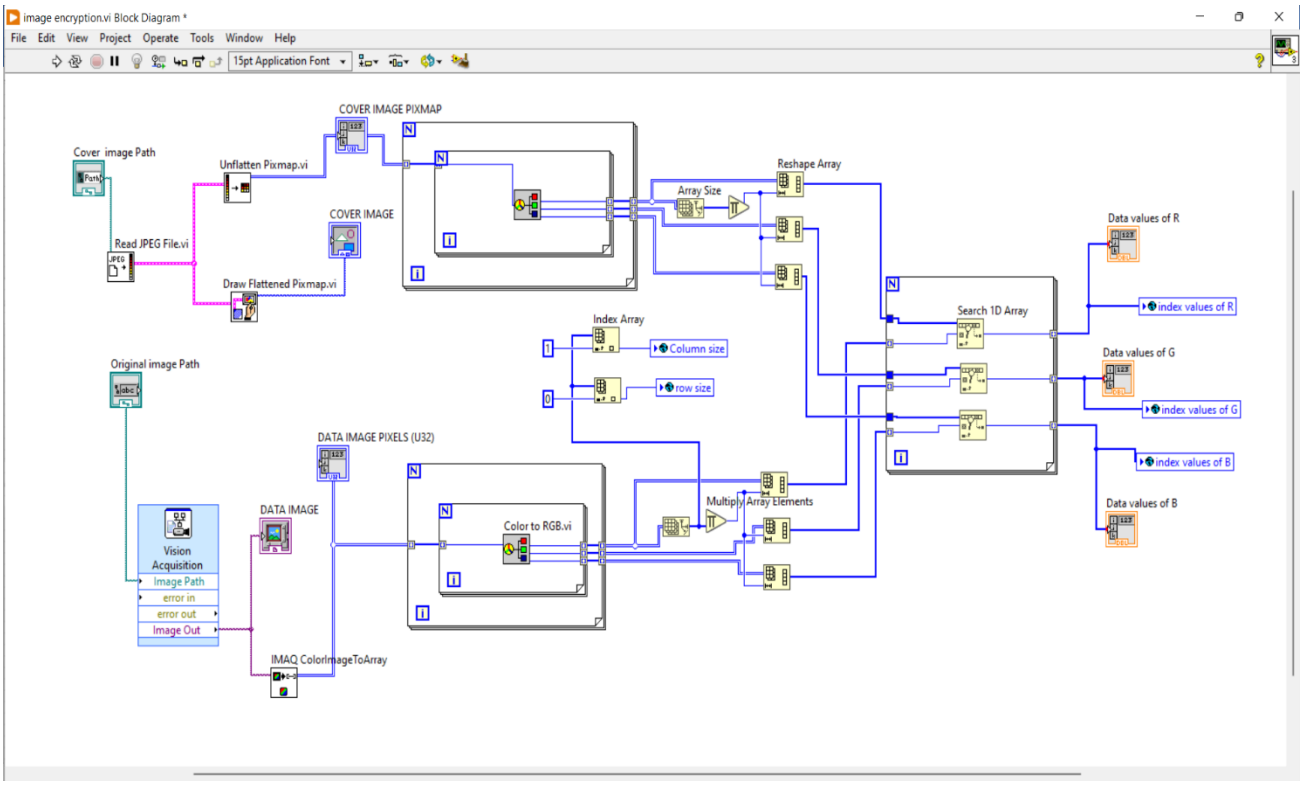

Fig 3.8: Block diagram of Image-encryption module

The Data and Cover images are first provided as input, with the Data image being used via vision acquisition and the Cover image being opened via the path location and displayed on the front panel.

As previously stated, the 'colour to RGB' function converts both the data image and the cover image into pixels, and both images are converted to RGB pixels arrays.

The 'Reshape array' function transforms this 2D RGB array into a 1D array. Because the operation must be repeated for all pixels, the loop structure is used.

Before reshaping the array, the 'global variable' function is introduced for the row and column size, which will later be used for decryption. In addition, the index values obtained by searching RGB elements in a 1D array are provided as global variables for decryption.

All the pixels values of the images and the RGB data from the data and cover image are indicated in the front panel with a display of the images.

Therefore, when two image inputs are given into the module the pixels will be broken and the pixel values will be reshaped for convenience and the index values obtained are stored in global variables for decryption module.

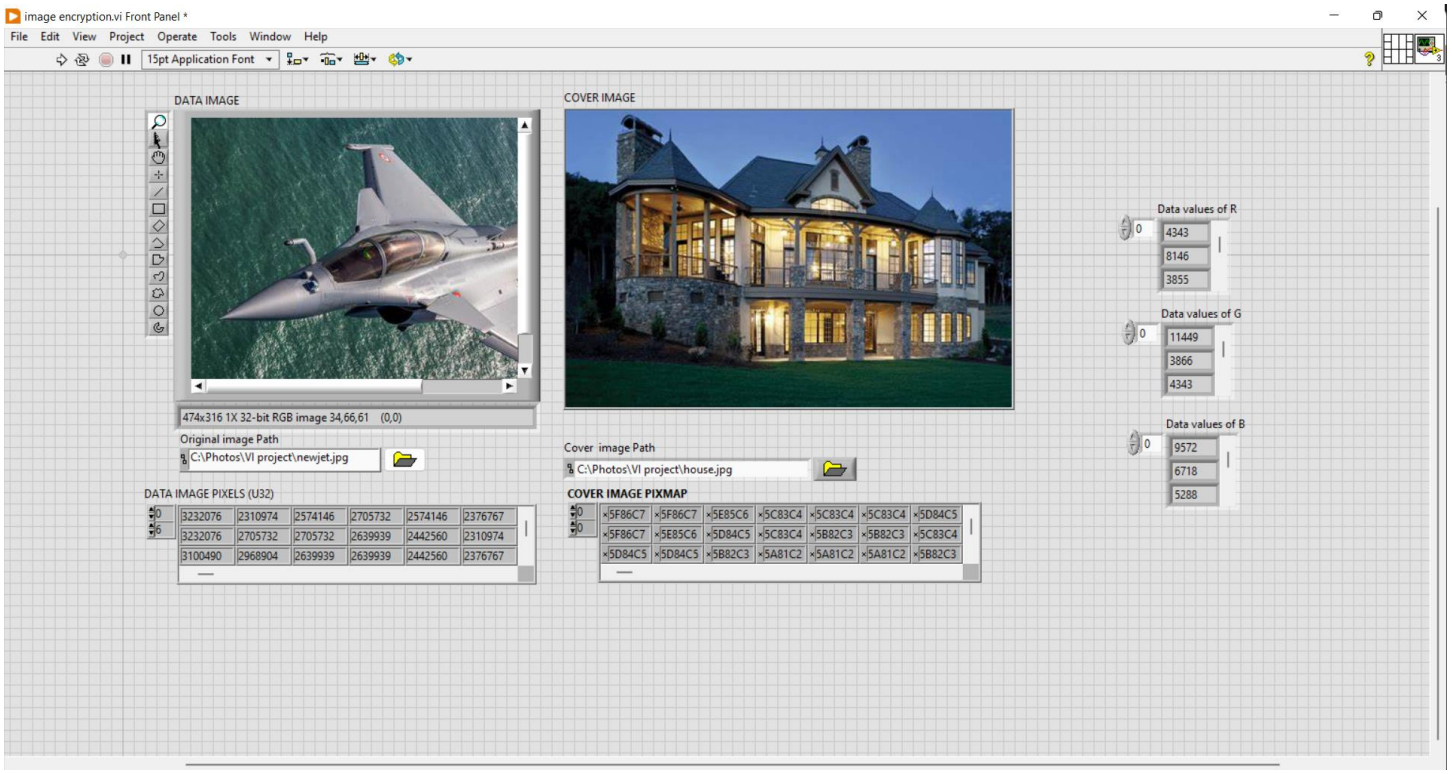

Fig. 3.9: Front panel of Image-encryption module

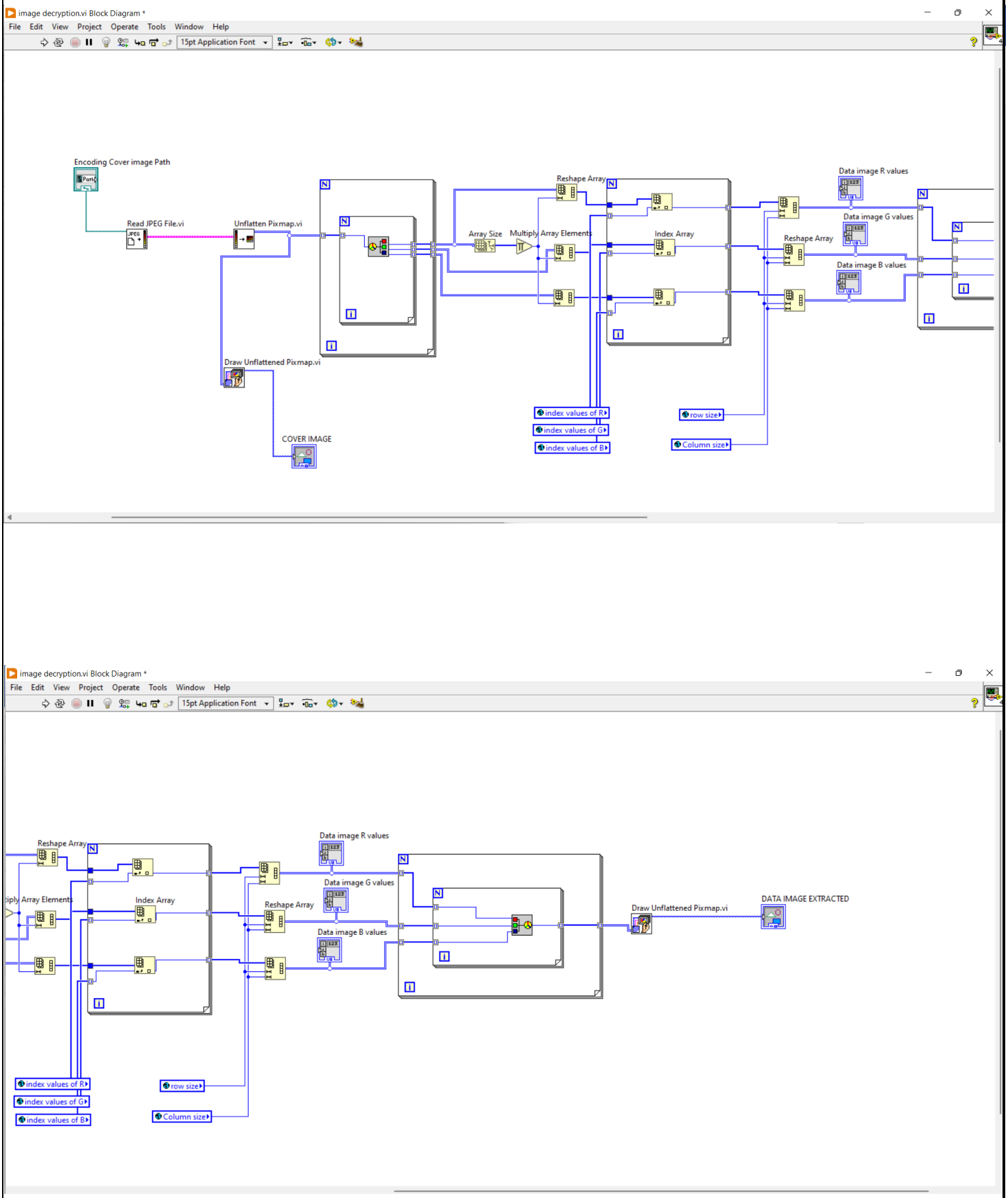

Fig. 3.10: Block diagram of Image-decryption module

Decoding is the opposite of encoding in that the hidden image is recovered from the cover image. During the decoding process, global variables known as secret shared keys are obtained. The array of Red, Green and Blue pixel values is provided by this key. Using these arrays, the entire image is searched, and the result is the data image. The shared secret key is a global variable obtained from the encryption module. The final data image received is generated from the cover image based on the location stored in the global variable.

In the decoding process, the global variables obtained from the encoding VI are used as the key for the decoder to extract the data image from the cover image. The same cover image is selected and used in the encoding process on the decoder's front panel. Global variables are used as the decoding process's key. The data image is extracted from the cover image using these global variables. The input is an encoded image, and the output is a data image. As a result, any third party cannot easily track the secret image.

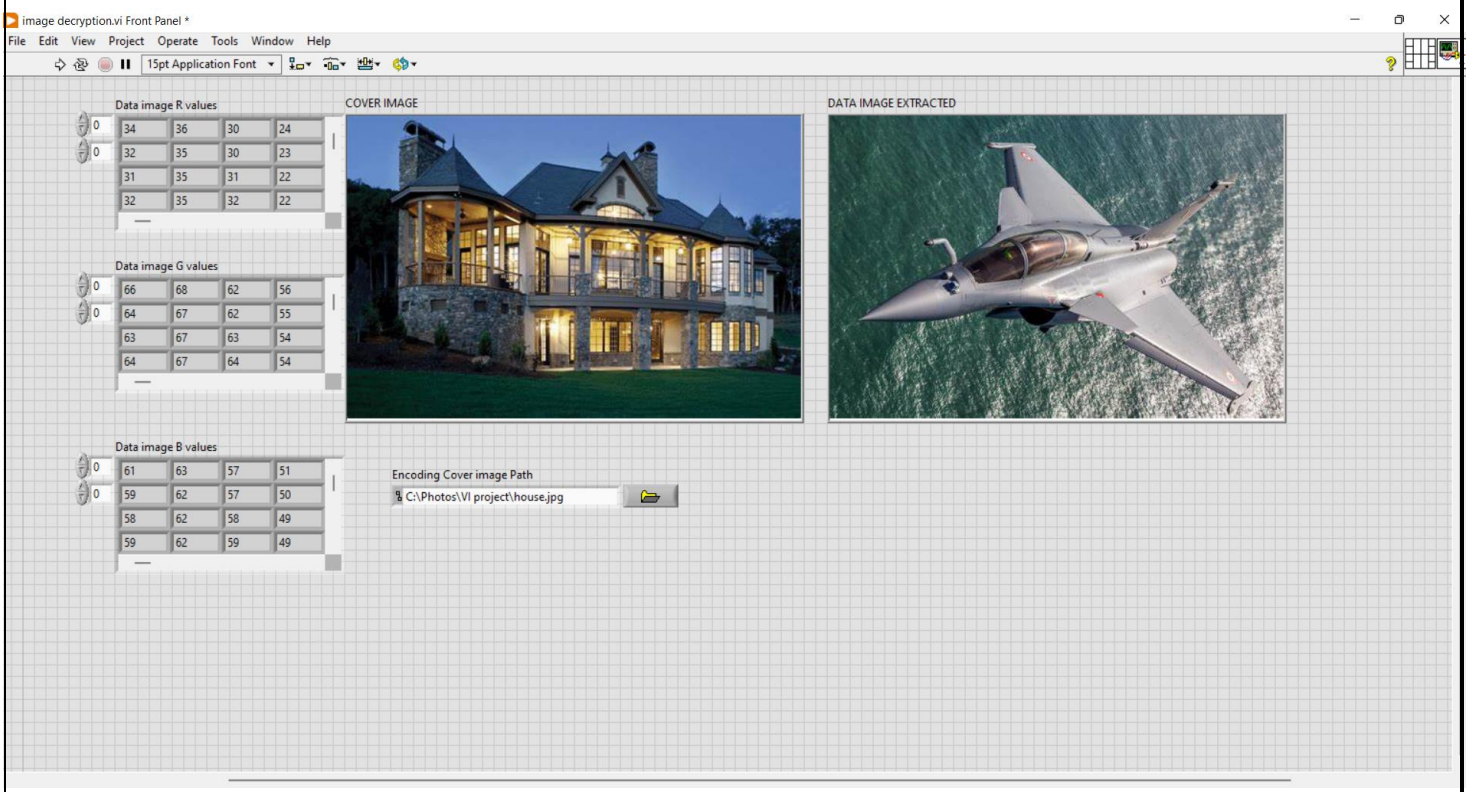

Fig 3.11.: Front panel of the Image-decryption module

CHAPTER 4

RESULTS AND DISCUSSION

The proposed model used cryptography and steganography data hiding techniques to encrypt and decrypt the text and image. The text is encrypted using the FFT algorithm into another text file containing non-readable secret characters, and that file is decrypted using the IFFT algorithm into the hidden string of data. Similarly, image steganography is accomplished by converting both the original and cover images into pixel arrays that will be used as secret keys in the form of global variables. These global variables are passed as keys to the decryption module during the cover image decryption process. The original file that was retrieved by the cover file was displayed on the front panels of both cryptography and steganography. Also, The front panels are made user-friendly and easy to operate. The whole operation is done in LabVIEW software with the required add-ons for the project.

Future work could include using video files to transport secret information and developing an application where the algorithm is applicable to text, audio, and video transmission The NI LabVIEW with Motion and Vision toolkit is available now and are useful for implementing the steganography algorithm. In addition, by utilising quantum computing computers, effective new algorithms and cypher texts can be used in cryptography.

CHAPTER 5

CONCLUSION

As a result, this application can be used in the military for transforming secret information between different Zones. The application has enormous potential for further development. The development is dependent on factors that ensure transmission security. The application can be customised to work with word documents and other file types.

Future work could include using video files to transport secret information and developing an application in which the algorithm can be applied for text, audio, and video transmission. The NI LabVIEW with Motion and Vision toolkit is useful for applying the steganography method. In addition, by utilising quantum computing computers, effective new algorithms and cypher texts can be used in cryptography.

CHAPTER 6

REFERENCES

[1] Kester, Q. A., & Danquah, P. (2012, October). A novel cryptographic key technique. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on (pp.70-73).

[2] Symmetric key Cryptography using two-way updated – Generalized Vernam Cipher method: TTSJA algorithm, International Journal of Computer Applications (IJCA, USA), Vol 42, No.1, March, Pg: 34 -39(2012)

[3] Satyaki Roy, Shalabh Agarwal, Asoke Nath, Navajit Maitra, and Joyshree Nath, "Ultra encryption algorithm (UEA): Bit level symmetric key cryptosystem with randomised bits and feedback mechanism," International Journal of Computer Applications (0975-8887) Volume 49-No.5, July 2012.

[4] Sruthi s, Athira vijay, Shejo jose, Athira v, Encryption & Decryption of Text file and Audio using LabVIEW, "2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum" pp. 462-466.

[5] Ultra Encryption Standard (UES) Version-I: Symmetric Key Cryptosystem Using Generalized Modified Vernam Cipher, Permutation, and Columnar Transposition, Satyaki Roy, Navajit Maitra, Joyshree Nath, Shalabh Agarwal, and Asoke Nath, Proceedings of the IEEE sponsored National Conference on Recent Advances in Communication, Control, and Computing Technology-RACCCT 2012, March 29-30, Surat, India, Page 81-88. (2012).

[6] Gang Hu, "Study of file encryption and decryption system using security key," in Chengdu, 2010 2nd International Conference on Computer Engineering and Technology, pp. V7121-V7-124.

[7] Md. Rashedul Islam, Ayasha Siddiqa, Palash Uddin, Ashis Kumar Mandal, and Md. Delowar Hossain: An Efficient Filtering-Based Approach Improving LSB Image Steganography Using Status Bit and AES Cryptography. 3rd International Conference on Informatics, Electronics, and Vision, May 23-24, Dhaka, Bangladesh, pp. 1-6 (2014).

[8] Lita, I.; Visan, D.A.; Cioc, I.B: LabVIEW application for movement detection using image acquisition and processing. IEEE 16th International Symposium onDesign and Technology in Electronic Packaging (SIITME), , pp. 225-228 (2010).

[9] Saket Kumar, Ajay Kumar Yadav, Ashutosh Gupta, Pradeep Kumar: RGB Image Steganography on Multiple Frame Video using LSB Technique. International Conference on Computer and Computational Sciences (ICCCS), pp. 226-231, Jan 26- 27, Noida (2015).

[10] RigDas, Themrichon Tuithung: A Novel Steganography Method for Image Based on Huffman Encoding. 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), pp. 14-18, March 30-31, Shillong (2012).

[11] Caixia Liu: The Development Trend of Evaluating Face- Recognition Technology. IEEE International Conference on Mechatronics and Control (ICMC), pp. 1540-1544, (2014).

[12] G. Prabhu Teja, S. Ravi: Face Recognition using Subspaces Techniques. IEEE International Conference onRecent Trends In Information Technology (ICRTIT), pp. 103-107, (2012).