International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-3, May 2020
https://doi.org/10.21276/ijircst.2020.8.3.13
www.ijircst.org

Two Step Verification and Data Security through TheNetwork

Soumyadeep Das, Vishal Rohilla, Dr. Meenu Vijarania, Dr. Yojna Arora

ABSTRACT- Our project is basically a web based application that engages in security and the transmission of data through the network. As we know that security is now become a necessity in each and everyone's life as there might be people who want to access your secret data for wrong purposes.So our system deals with the security issue by implementing steganography into our system. Steganography basically helps to hide secret messages and information embedded in a photograph or a video. This technique helps to prevent any third party user from accessing the secret message. In our project we are also using an encryption technique that is the "Tiny Encryption Algorithm". Encryption also plays an important role in keeping the data from unauthorized people in real time environment such that the data is safe. After encryption, the file is implemented with steganography and is then transmitted through the network to the receiver. The receiver should have the same application to de-embed the file and then decrypt the same file to extract the original file. The goal of our project is to design a tool for providing security to the system during transmission of data through the network for the likes of military forces that have an essential need for communication for vehicle control, surveillance signal processing and is even more imperative in times of a war.

KEYWORDS- Data Transmission, Security, Steganography, Tiny Encryption Algorithm.

Manuscript received May 16, 2020

Soumyadeep Das, Department of Computer Science and Engineering, Amity University Haryana, Gurugram, India, 9717137840 (email: dassoumyadeep87@gmail.com)

Vishal Rohilla, Department of Computer Science and Engineering, Amity University Haryana, Gurugram, India

Dr. Meenu Vijarania, Department of Computer Science and Engineering, Amity University Haryana, Gurugram,India

Dr. Yojna Arora, Department of Computer Science and Engineering, Amity University Haryana, Gurugram, India

I. INTRODUCTION

Our project mainly is designed to transmit a file from sender to receiver in a secured manner. The sender firstly chooses the data that he/she wants to send and encrypts it using "Tiny Encryption Algorithm". This algorithm has been used because it requires less memory. It uses only simple operations, therefore it is easy to implement [4]. While encryption of the data, a key is entered by the sender. The purpose of the key file is to provide security to the system as it is known only to the sender and the receiver. The encrypted data will embed with a video file by using the concept of steganography [12]. While applying steganography, it will read the video and the encrypted file. So if someone tries to open the file, only a video file will be visible to them. Then this video file is sent to the network [24]. After the receiver receives the video file through the network then the receiver will start to de-embed the encrypted data from the received video file. The decryption only takes place when the receiver enters the proper key. Thus the data is transferred from sender to receiver in a secured manner [5].

II. LITERATURE REVIEW

Cryptography is a method to exchange data in a secret form, which means, that only the recipients can interpret or understand the data and its relevance and that no one else is able to access that data [1][3]. According to the etymology of cryptography, kryptos means hidden and graphein means to write [2][3]. Justifying this, the original data is encoded into a scramble code, which is difficult to understand by any third person, and the extent of this difficulty characterizes the level of security and therefore, the efficiency of the cryptography technique [2][3]. TEA has proven to be a highly accurate and efficient symmetric cryptographic algorithm, which is therefore, widely used for data abstraction, these days. Not only one, but there are several studies which evident the use of TEA as an efficient cryptography algorithm. The first use of TEA as an encryption and decryption algorithm was seen in a study by Wheeler and Needham where they applied a fiestal network and designed the TEA as a symmetric cryptography algorithm [4]. So far, TEA has been largely implemented in the encryption and decryption of textual data, as evident in various studies. A similar study was used to enhance text security with the application of TEA in combination with a steganographic technique called Pixel Value Differencing

(PVD) [5]. The study by Rahim et al. showed the application of TEA as an encryption algorithm in combination with PVD as a steganographic algorithm to hide the encrypted text. The study evidently increased the text security and also the efficiency as long messages were also easily transferred with higher security [5]. All these studies make it evident that TEA is a symmetric cryptographic algorithm which enhances security and the efficiency of a cryptosystem. There are various analysis conducted to validate this competence of TEA with respect to other cryptographic algorithms. Analogous to this, a study by Thu et al., compared the performance of file security system using TEA and Blowfish algorithms [10]. The study compared different file types like .pdf, .docx, .pptx, .xls, .jpg, .mp4 and .txt files. The studied simulation resulted in comparing the encryption and decryption time for all the input files and concluded TEA as a more efficient symmetric cryptography algorithm with higher security and lesser execution time, therefore, making it more suitable for a cryptosystem [10]. Another study by Chaitra et al.compared several cryptography algorithms with TEA [11]. The security remained not hampered as the application of either algorithm did not hinder the security of the data but with overall decreased power consumption but increased time delay, TEA was cost-effective, but prove to be less efficient, in comparison to the present algorithms [11]. Other than cryptography, there are various other techniques to ensure data security in a cryptosystem, like steganography. Steganography comes from the Greek words Steganós meaning ‘covered’ and Graptos meaning ‘writing’ [12]. Steganography in these days refers to information or a file that has been concealed inside a digital picture, video or audio file. If a third person views the embedded file he or she will have no clue that there is any hidden information; therefore the person will not try to decrypt the information. Digital steganography is a type of steganographic technique which follows the principle of hiding data within data in an invisible manner. It conceals the fact that message exists by hiding the actual message. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary, without the knowledge of any other person who accesses the data [12]. A study by Rajendranand Doraipandian uses a new chaotic series based image hiding scheme for implementing a new symmetric key based image hiding technique [13]. The scheme utilizes the LSB substitution technique for hiding the secret image and proves to be highly secure and efficient in comparison to other steganographic techniques [13,14]. The method has an increased security due to the added randomness in the system using a random cryptography key generator algorithm to generate permutations for random pixels which are further chosen for hiding purpose and hence, results in a very secure and efficient technique for exchanging text data with complete security [15]. Other than LSB, there exist various other techniques for steganography like DCT (Discrete Cosine Transform) which is generally applied for images and is accomplished using a different domain which is the frequency domain unlike LSB, which is applied using spatial domain in an image [20]. This method improved the process of extracting the original message from the encrypted image with 100% similarity between encrypted image and the original image **[21]**. DCT is largely used technique for image encryption and hence has been applied to health care also. A study by Dong et al. uses DCT based steganography technique for encrypting medical images for safeguarding the medical imaging data and making the data impervious to any unauthorized use **[22]**. The study proposes an algorithm to encrypt both the original medical image and watermark image by using DCT and Logistic map, followed by embedding watermark into the encrypted medical image. The study resulted that the algorithm was a robust approach to common image processes such as Gaussian noise, JPEG compression, median filtering and could also withstand levels of geometric distortions.A cryptosystem to be completely secure, should be not only able to encrypt and/or decrypt, but also hide the message, making it uncertain for an attacker to predict the mere presence of a secret message. Hence, an integrated model of encryption/decryption techniques along with steganography can prove to be not only secure but robust to various attacks. A highly secure cryptosystem of this degree, can further be implemented not only for maintenance of data confidentiality at an individual level, but can prove to be of national use by employing such secure cryptosystems for communication and other data transmission in national safeguard. Military forces have an essential need for communication for vehicle control, surveillance signal processing and is even more imperative in times of a war **[25]**.

III. METHODOLOGY

A. Existing System

In traditional architecture only server and client was present and mostly the server was only a database server that only offers data. So majority of the business logic was placed in the clients system. This process made it expensive. The client thus also needed training as how to use the application and the security related to the communication of the data is also to be considered here. In the present day security has become a necessity otherwise it is termed as “un-trusted”, i.e., it is easier for a hacker to hack the data. We also have to consider sending large data across the network will give some errors. In the present systems network security is very good with high security standards for exchange of information.

B. Proposed System

The transactions in between the clients in the network should take place in a secured format. This will provide flexibility to the user while transferring data across the network. It should provide the communication as per the prescribed level of security with the transfer of file as requested after identifying the user and if necessary run the required process at the server. Here the transferred data would be in the form of video file. And when the receiver receives the file will perform operations like de-embedding and decryption to extract the original file.

C. Feasibility Study

A feasibility study is basically high-level but smaller version of the entire System analysis and Design Process. The following feasibilities are considered for the project in order to ensure that the project is available and it does not have any major obstructions.

a. Technical Feasibility

It centers on the existing computer system (hardware, software) and to what extent it can support the proposed system.

b. Operational Feasibility

The user who wants to use this system would require to have a prior knowledge of how to use the operations such as encrypt, embed, de-embed, decrypt, etc.

c. Economical Feasibility

We say the system is economically feasible if a certain cost for the project is accepted.Since the proposed system is economically feasible so it will be beneficial for the organizations to develop and install the system. So that there will be no need for any further hardware or software for the system.

D. Technical Analysis

In the general digital communication system people have tried to sort problems with no affect till date. But as the systems evolved, a more secure and easy way to transfer data through the network know as Encryption and Decryption of a data file and converts the data file to a video file into cryptographic standards and steganography before transferring the file across the network. The advantages of such system are:

- High level Security
- Cost effective transfer

Now-a-days people have knowledge of hacking and with the network free to access it might be a threat to the organizations. However if the organizations install this Systems, then each and every employee can send information to the other employee without any third employee knowing about the information sent and thus more secured. But both those employees must be registered to the system. The video file sent to the other registered employee can then de-embed and decrypt to extract the original message for further use. The whole organization can be connected to a single host and thus one employee can communicate with the other employee regardless of the branch in the organization in a secured manner.

E. Functional Model

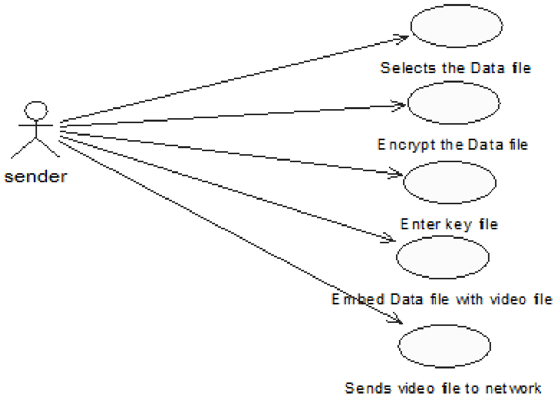


Fig. 1: Use case diagram for Sender

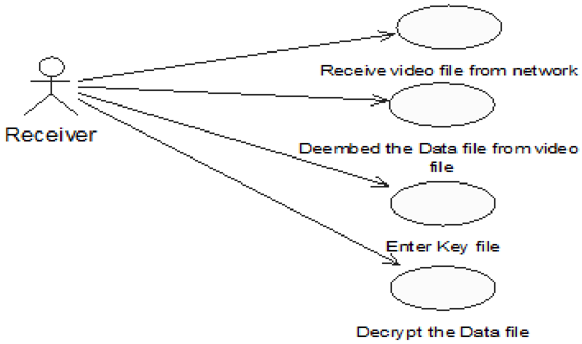

Receiver
Receive video file from network
Deembed the Data file from video file
Enter Key file
Decrypt the Data file

Fig. 2: Use case diagram for Receiver

F. Object Model

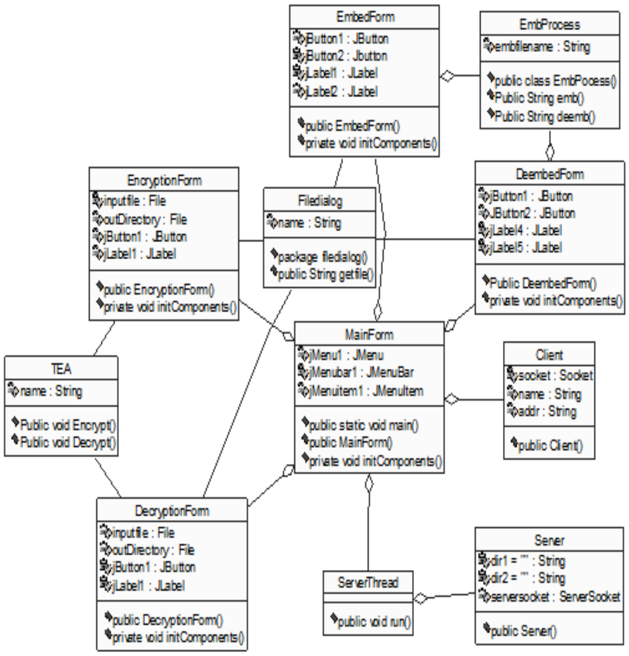


Fig. 3: Class diagram

G. Dynamic Model

a. Interaction Diagrams

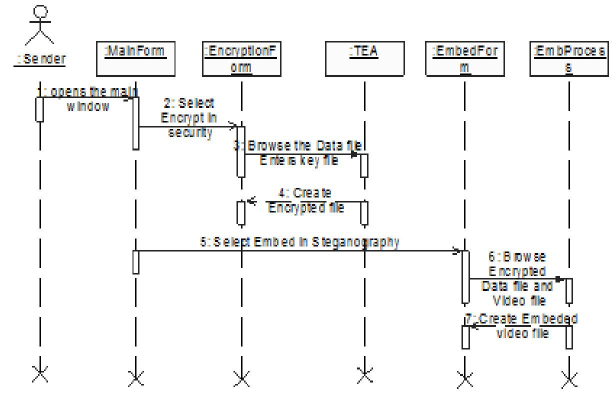

: Sender
:MainForm
:EncryptionForm
:TEA
:EmbedForm
:EmbProcess
1: opens the main window
2: Select Encrypt in security
3: Browse the Data file Enters key file
4: Create Encrypted file
5: Select Embed in Steganography
6: Browse Encrypted Data file and Video file
7: Create Embeded video file

Fig. 4: Sequence diagram for Sender

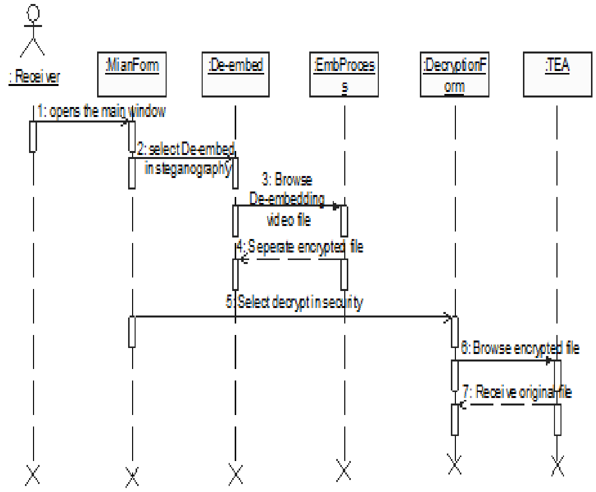


Fig. 5: Sequence diagram for Receiver

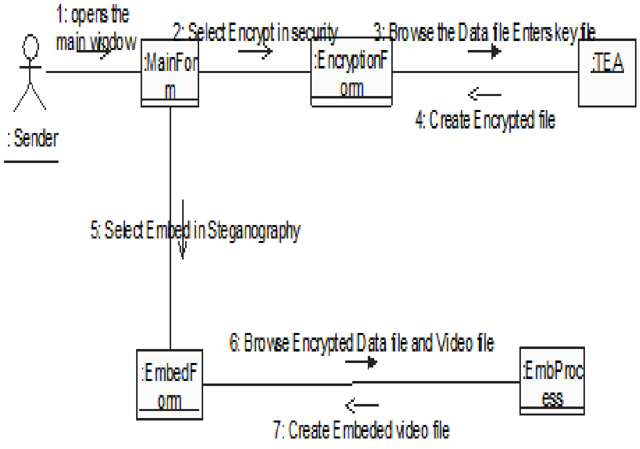

1: opens the main window
: Sender
:MainForm
2: Select Encrypt in security
:EncryptionForm
3: Browse the Data file Enters key file
:TEA
4: Create Encrypted file
5: Select Embed in Steganography
:EmbedForm
6: Browse Encrypted Data file and Video file
:EmbProcess
7: Create Embeded video file

Fig. 6: Collaboration diagram for Sender

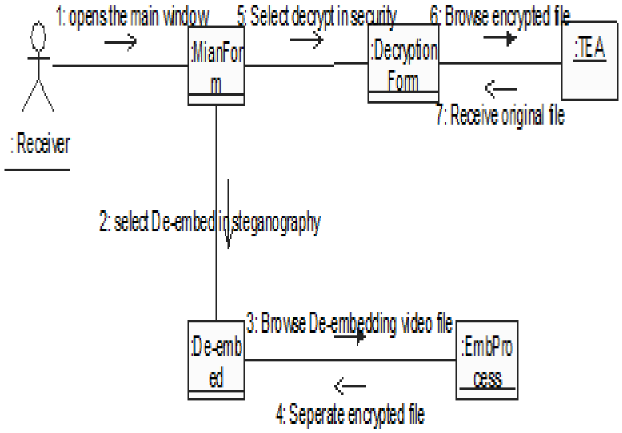


Fig. 7: Collaboration diagram for Receiver

b. Activity Diagram

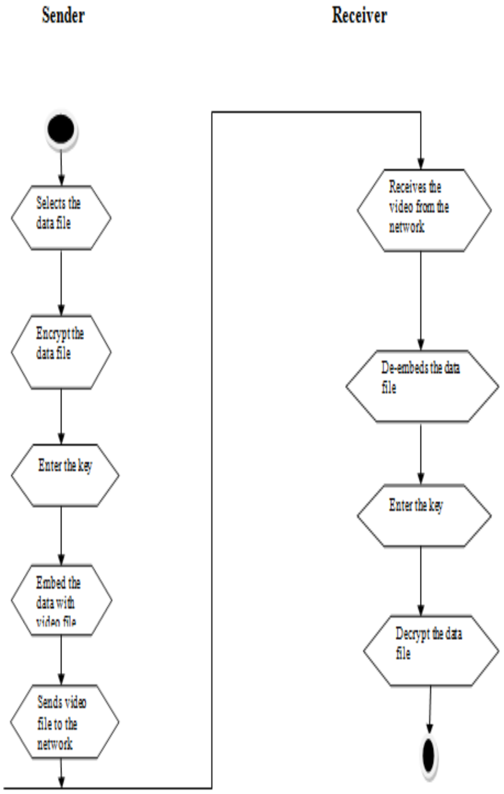


Fig. 8: Activity diagram

H. Software Overview

a. About Java

In 1995 ‘oak’ language was renamed to ‘Java’. The main reason of this language is of a platform-independent language that will help to create software that can be embedded in various consumer electronic devices.

- Java is a programmer’s language.
- Java is cohesive and consistent.
- Java gives the programmer the full control.

b. Application and Applet

A program under an operating system that runs on our computer is known as an application. Java's ability to create Applets makes it important. An Applet is an application designed to be executed by a Java compatible web browser and to be transmitted over the Internet. An applet is a small Java program that is dynamically downloaded through the network, just like an image. But it is also an intelligent program, not just a media file. It can act according to the user input and dynamically change.

c. About Swings

For developing graphical user interfaces a collection of APIs are used such as The Java Foundation classes, or JFC, etc.
The java foundation classes include the following APIs:-

Abstract window toolkit.
2D API
Swing Components
Accessibility API

The Abstract window tool kit, or AWT, is java's original tool kit for developing user interfaces. The 2D API provides additional graphical capabilities that are lacking in the AWT. Swing is basically a collection or set of lightweight components that are built on top of the AWT. Swing provides lightweight replacements for the AWT's heavy weight components, in addition to a multitude of additional components that the AWT lacks.

d. Lightweight Vs Heavyweight components

Initially, the AWT included only heavyweight components and not lightweight components as they were not associated with a native peer unlike heavyweight components.
Some of the Swing components are:-

e. JButton

It is a push button that is meant to replace java.awt.button.

Constructors
public JButton( )
public JButton(String, Icon)

f. JCheckBox

When activated checkboxes fire action events, Their bound properties are modified when the property change occurs.

Constructors
public JCheckBox( )
public JCheckBox(String, Icon, Boolean selected)

g. JMenu

Swing Menus are essentially buttons that have a popup menu associated with them. When a menu is activated, it's popup menu is displayed beneath the menu.

Constructors
public JMenu( )
public JMenu(String)
public JMenu(String, Boolean is Teal off)

h. JoptionPane

These are the components that are to be placed in the dialog box. It can display icons, one or more selectable variables, a message, and a ro of buttons.

Constructors
public JOptionPane( )
public JOptionPane(object message, int message Type, int Option Type, Icon icon, Object[ ]options, Object initial value)

i. JInternalFrame

These are frames because they are the exact copies of external frames; they are called as internal frame as they are contained with in another Swing Container, usually a Desktop Pane.

Constructors
public JInternalFrame();
public JDesktopPane();

j. JPopupMenu

It can be used even outside of a menu; it can be displayed anywhere within a component or relative to the screen.

Constructors
public JPopupMenu();
public JPopupMenu(String);

h. JPasswordField

It hides or seals the text by replacing the text with an '*'.

Constructors
Public JPasswordField();
public JPasswordField(Document, String, int);

IV. RESULTS AND DISCUSSION

To check whether our application is working as expected or not we did some test on it. The starting point of testing is unit testing. In this a module the coder himself performs tests separately along with the coding of the module. This is done to find out the working of different parts of the module and to detect the errors. After this, all the modules are integrated together into subsystems, then these subsystems are integrated within themselves to form an entire system. During integration of modules, integration testing is performed. The main objective of this testing is to find out any design errors, while also focusing on the interconnection testing in between modules. After the subsystems are integrated together, system testing is performed. Here the system is tested against the system requirements to see if all the requirements are met and the system performs as specified by the requirements.

A. Unit Testing

Unit testing is done on the smallest unit of software design module. All the modules in this system are tested under this strategy of unit test. In this each line of the code of all the classes were tested. Several general syntax errors were emcountered, which during the compilation of the classes were corrected.

Table 1: Test Report

S.No	Test Case	Expected Output	Result
1.	Variables	All variables are declared before using them.	Pass
2.	Classes in Different Packages	Required Built-in classes are imported from the packages.	Pass
3.	Syntax Errors	Syntax Errors are Eliminated.	Pass

B. Black Box Testing

Table 2: Test Case 1 Encryption

Input	1. Select the data file and enter the key. 2. Click on Encrypt button when the data file is not selected or when the null value is entered. 3. Click on Ok button when the key is not entered.
Result	1. It displays the mesaage “Your file has been encrypted and saved”. 2. Error message “Select the file” is displayed. 3. Error message “File decryption failed” is displayed.
Condition	You should select the data file and the key must be entered.

Table 3: Test Case 2 Embedding encrypted file

Input	1. Select encrypted file and video file. 2. When the file is not selected o when the null value is entered we have to click on embed button.
Result	1. Displays the “Embed process completed” message. 2. Error message “Embed process failed” is displayed.
Condition	You should select the embedding encrypted file and video file.

Table 4: Test Case 3 Send file

Input	1. Enter the correct IP address of receiver. 2. Click on Ok button when the address is not entered or when the null value is entered. 3. Enter the wrong IP address of receiver.
Result	1. Displays the “File successfully sent” message. 2. “Enter the IP address of receiver” is an error message that is displayed. 3. The message “File was unable to send” is displayed.
Condition	You should enter the correct IP address of receiver.

Table 5: Test Case 4 De-embedding Encrypted file

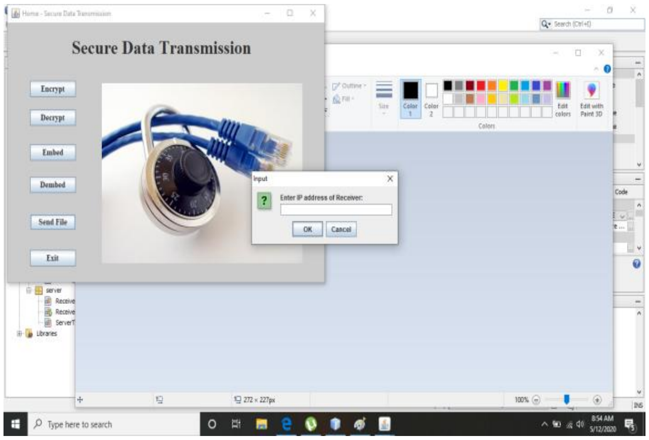
Input	1. Select the video file. 2. Click on De-embed button when the file is not selected or when the null value is entered.
Result	1. Displays the “De-embed process completed” message. 2. Error message “De-embed process failed” is displayed.
Condition	You should select the De-embedding Encrypted file.

Table 6: Test Case 5 Decryption

Input	1. Select the file and enter the key. 2. Click on decrypt button when the file is not selected or when the null value is entered. 3. Click on Ok button when the correct key is not entered.
Result	1. “The file has been decrypted and has been saved”message is displayed. 2. Error message “Select the file” is displayed. 3. Error message “File decryption failed” is displayed.
Condition	You should select the file and enters the correct key.

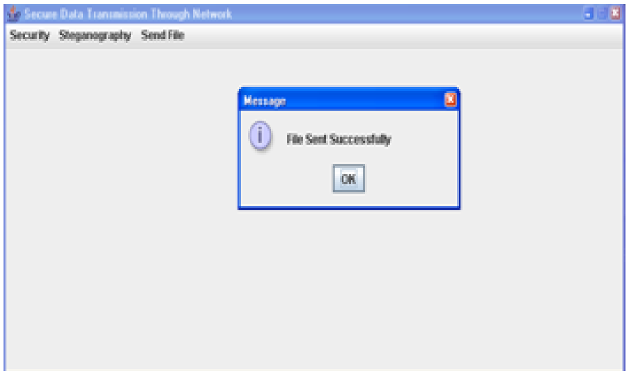
C. Functional Testing

It basically tells us about the operating condition, the input values and the expected results. The function should be designed to take care of the situation. Performance tests should be carried out to verify response time, secondary memory utilization and throughput.



Enter IP address of Receiver:

Fig. 9: File Sent Through the Network



File Sent Successfully

Fig. 10: File Sent Successfully

D. Integration Testing

Table 7: Test Case1 Security Module

Input	Expected Behavior	Observed Behavior	Status P=Passed F=Failed
Encryption	Encrypts the given data file and saved.	Encrypts the given data file and saved.	P
Decryption	Decrypts the data file and saved.	Decrypts the data file and saved.	P

Table 8: Test Case 2 Steganography Module

Input	Expected Behavior	Observed Behavior	Status P=Passed F=Failed
Embedding Encrypted file	Embed the encrypted file in a video file.	Embed the encrypted file in a video file.	P
De-embedding Encrypted file	De-embed the encrypted file from the video file	De-embed the encrypted file from the video file	P

Table 9: Test Case 3 Send File

Input	Expected Behavior	Observed Behavior	Status P=Passed F=Failed
Send File	File will be successfully send across the network	File will be successfully send across the network	P

E. System Testing

System is tested for volume of transactions, stress, online responses, usability and recovers from failure. System testing iss concerned with recovery procedures and throughput, the design logic, timing characteristics of the entire subsystem, control flow and capacity. The system will be staying at consistent state even if failure occurs in the middle of processing.

V. CONCLUSION

The developed software is tested with sample data and outputs obtained are in accordance to the requirements. The performance of the system is evaluated, and is found to be much more efficient than the existing system. It will meet the primary requirements of the concern. Even though we have tried our best to make it a best project, but due to time issue we could not add more facilities to it. So the project has to be modified and improved as and when necessary.

ACKNOWLEDGMENT

Acknowledgment is not a mere obligation but the epitome of humility and ineptness to all those who have helped in the completion of this project. We are thankful to Dr. Meenu Vijarania and Dr. Yojna Arpra, Department of CSE, ASET for their constant guidance and encouragement provided in this endeavour. I also thank my parents for their continued support, understanding and patience without whose support and understanding this endeavour would never be fruitful. We also thank all our friends for helping us out in completing this project and helping me in solving various problems encountered during the progress of this project.

REFERENCES

[1] Mollin RA, “An introduction to cryptography”, ‘CRC Press’, 2000.

[2] Schneier B, “Applied cryptography: protocols, algorithms, and source code in C”, ‘john wiley& sons’, 2007

[3] Rachmawati D, Sharif A and Budiman MA,“Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm”,‘InIOP Conference Series: Materials Science and Engineering’, vol. 300, no. 1, pp. 012042, 2018

[4] Wheeler, D.J. and Needham, R.M.,“TEA, a tiny encryption algorithm”, In the proceedings of ‘International Workshop on Fast Software Encryption’, Berlin, Heidelberg, pp. 363-366,1994

[5] Rahim R, Adyaraka D, Sallu S, Sarimanah E, Rahman MM, Chusna NL andKurniasih N,“Tiny encryption algorithm and pixel value differencing for enhancement security message”, ‘International Journal of Engineering and Technology’, vol. 7, no. 2.9, pp. 82-5, 2018

[6] Novelan, M.S., Husein, A.M., Harahap, M. and Aisyah, S., "SMS Security System on Mobile Devices Using Tiny Encryption Algorithm", In 'Journal of Physics: Conference Series', vol. 1007, no. 1, pp. 012037, 2018

[7] Rajesh, S., Paul, V., Menon, V.G. and Khosravi, M.R.,"A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices", 'Symmetry', vol. 11, no. 2, pp.293, 2019

[8] Sugiyanto, S.,"N-TEA (New-Text Encryption Algorithm) For Secure Chat In Android Based Application", 'In the proceedings of International Conference on Information Technology Applications and Systems 2018', 2018.

[9] Setyawan, R.A., Selo and Hantono, B.S.,"Effect of the Application of TEA Algorithm on the Development of Secure Phone Application Android Smartphones", In the proceedings of the conference of 'Journal of Physics', vol. 1175, no. 1, pp. 012073, 2019

[10] Thu, W.M., Win, T.L. and Tyar, S.M.,"Performance Comparison of File Security System using TEA and Blowfish Algorithms", 'International Journal of Trend in Scientific Research and Development', vol. 3, no. 5, pp. 871-877, 2019

[11] Chaitra, B., Kiran Kumar, V.G. and ShatharamaRai, C., "Comparative Study of cryptographic encryption algorithms", 'Journal of Electronics and Communication Engineering', International organization of scientific research, vol. 12, no. 3, version 2, pp. 66-71, 2017

[12] Walia, E., Jain, P. and Navdeep, N., "An analysis of LSB & DCT based steganography", 'Global Journal of Computer Science and Technology', 2010

[13] Rajendran, S. and Doraipandian, M.,"Chaotic Map Based Random Image Steganography Using LSB Technique", 'International Journal of Network Security', vol. 19, no. 4, pp.593-598, 2017

[14] Cheng, L.M and Chan, C.K. , "Hiding data in images by simple LSB substitution", 'Pattern recognition', vol. 37, no. 3, pp.469-474, 2004

[15] Jumaa, N.K., "Hiding of Random Permutated Encrypted Text using LSB Steganography with Random Pixels Generator", 'International Journal of Computer Applications', vol. 113, no. 13, pp. 20-27, 2015

[16] Kaur, R. and Singh, T., "Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography", 'International Journal of Computer Applications', vol. 117, no. 18, pp. 36-40, 2015

[17] Shen, J.J, Wang, Y.L. and Hwang, M.S., "An Improved Dual Image-based Reversible Hiding Technique Using LSB Matching", 'International Journal of Network Security', vol. 19, no. 5, pp.858-862, 2017

[18] Lu, T.C., Tseng, C.Y. and Deng, K.M., "Reversible data hiding using local edge sensing prediction methods and adaptive thresholds", 'Signal Processing', vol. 104, pp.152-166, 2014

[19] Wu, J.H. Lu, T.C. and Tseng, C.Y.,"Dual imaging-based reversible hiding technique using LSB matching", 'Signal Processing', vol. 108, pp. 77-89, 2015

[20] Setiadi D. R. I. M.,Rachmawanto, E.H. and Sari, C.A., "Secure image steganography algorithm based on dct with otp encryption", 'Journal of Applied Intelligent System', vol. 2, no. 1, pp.1-11, 2017

[21] Sari, Wellia, Rachmawanto, Eko, Rosal, De,Setiadi, De Rosal Ignatius Moses and Sari, Atika,"A Good Performance OTP encryption image based on DCT-DWT steganography",'TELKOMNIKA Indonesian Journal of Electrical Engineering', vol. 15, no. 4,pp. 1987-1995, 2017

[22] Dong, J., Li, J. and Duan, Y., "A robust watermarking algorithm for encrypted medical images based on dct encrypted domain", In the proceedings of the '2015 International Conference on Electronic Science and Automation Control', 2015

[23] Khalfallah A., Abdmouleh M. K. and Bouhlel M. S., "A Novel Selective Encryption Scheme for Medical Images Transmission based-on JPEG Compression Algorithm", 'Procedia Computer Science', vol. 112, pp. 369-376, 2017

[24] Shivani, J.L. and Senapati, R.K., "Robust image embedded watermarking using DCT and listless SPIHT", 'Future Internet', vol. 9, no. 3, pp.33, 2017

[25] S*tackPath*,[Online],Available:- https://www.militaryaerospace.com/communications/article/16706235/the-importance-of-military-information-security. [Accessed: 11-May-2020].