INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume 5, Issue 1)***
Available online at: www.ijariit.com

# Secure and transparent file encryption system

*Urvashi Kodwani*
*kodwaniurvashi@gmail.com*
*Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra*

*Sakshi Agrawal*
*agrawalss16@rknec.edu*
*Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra*

*Jui Diwale*
*diwalejp@rknec.edu*
*Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra*

*Samiksha Thakur*
*thakursv1@rknec.edu*
*Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra*

*Devishree Naidu*
*naidud@rknec.edu*
*Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra*

## ABSTRACT

***The main aim of The Novel Approach to File Encryption application is to provide security to the files user is sharing. The concept is implemented by creating a website which allows the user to create an account and share his/her respective data with the other persons registered on the site. Due to increasing cases of password hacking even the user password is encrypted and then stored in a database. The user files are encrypted using various encryption-decryption algorithms like Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The concept of steganography was also used to enhance the level of security. Finally file splitting and merging algorithms added to the security of user data. The User Interface is designed keeping in mind the ease of the user.***

***Keywords***— *Advance Encryption Standard (AES), Data Encryption Standard (DES), Image steganography*

## 1. INTRODUCTION

In the past few years, cases of hacking have been increased considerably. Various encryption techniques on password like salting and hashing have also been hacked. Recently the user data of a renowned company known as Zomato was stolen. Although the password contained hashing, salting etc. but still a user called Nclay was able to hack the user data was willing to sell data pertaining to 17 million registered users on a popular Dark Web marketplace. So cryptographic techniques that contain such things can alone do no good. Even hackers have now become aware of steganography algorithms. So again this individual concept of steganography failed. Hence an algorithm was needed that could combine various approaches together and provide a better way of securing user data so that it doesn't get hacked.

## 2. FILE SPLITTING AND MERGING

This is was used initially to split the files during encryption and merging during decryption. In splitting a file is given by the user. The algorithm takes the size of the file and split it into two parts depending on the size. Later in the merging part, the files are read and written in one file one after the other [11,14].

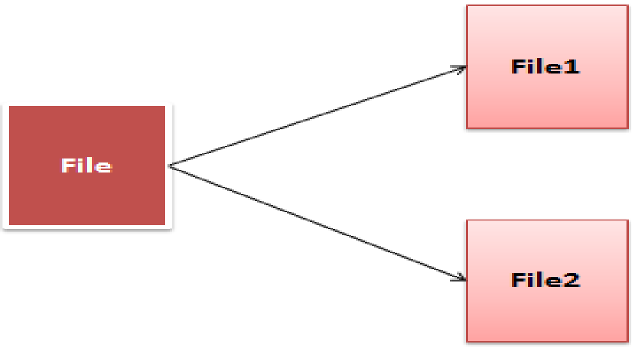

**Fig. 1: File Splitting**

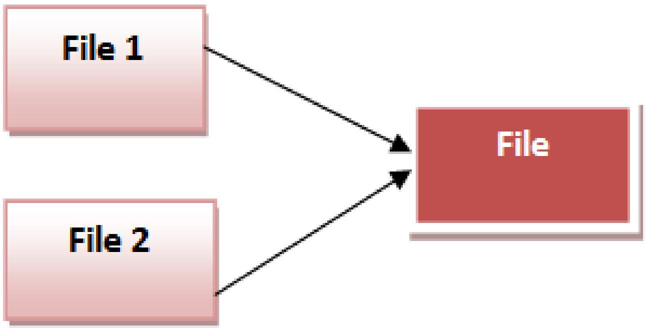

**Fig. 2: File Merging**

## 3. AES ALGORITHM

Following figures illustrate the working of the AES algorithm. During the encryption process, the file and key are given to AES Encryption algorithm and then it generates the encrypted file [3,4]. During the Decryption process, this encrypted file along with key is given to decryptor and it gives the original file [5,6].

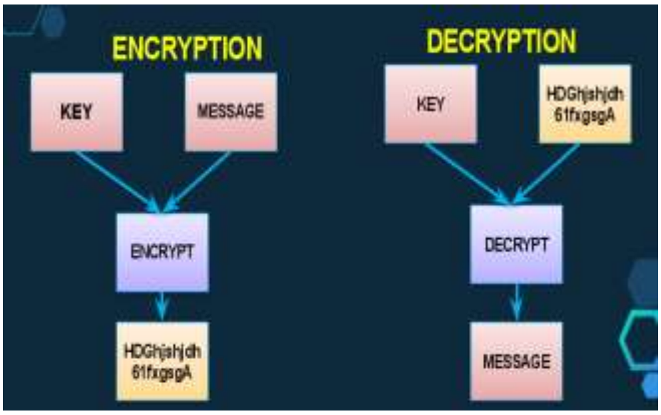

**Fig. 3: Encryption Decryption Process**

During the encryption process, various rounds take place depending on the size of the key. For 128 bit key 10 rounds take place in which 9 rounds repeatedly go through the same process and one final round takes place[1,2]. These four stages consist of the following:

- **Sub Bytes**: In this, every byte is substituted using standard S-Box. The value is obtained by looking up for the proper column and row value.
- **Shift Rows**: In this stage, every element is shifted by its corresponding row number.
- **Mix Columns**: In these columns of the matrix are interchanged.
- **Add Round Key**: At this stage, round key is added and it serves as input for the next stage.

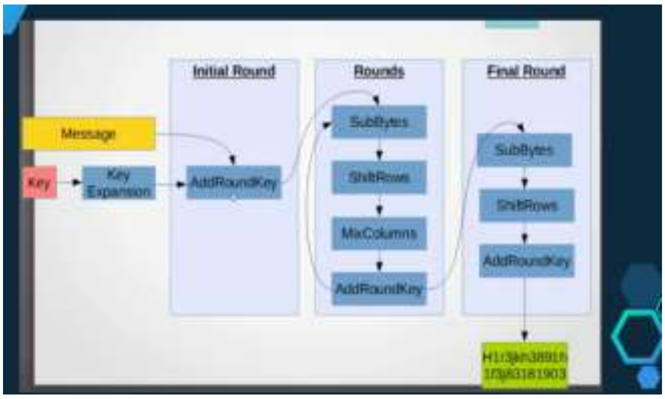

**Fig. 4: Encryption Process**

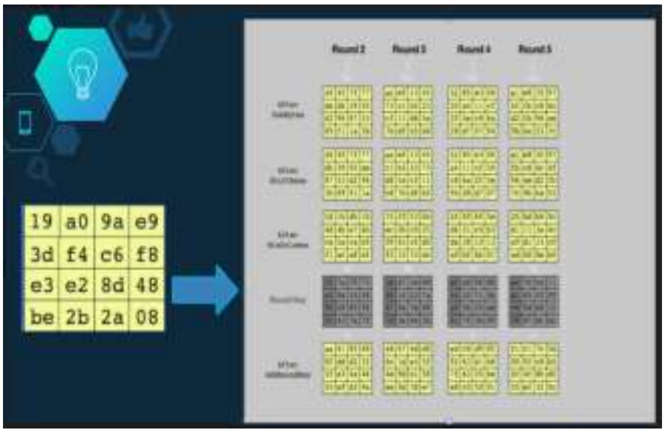

**Fig. 5: Detail of 4 stages**

## 4. DES ALGORITHM

Following figures illustrate the process of DES algorithm. This algorithm consists of 16 rounds along with 2 additional steps-initial and final permutation. It works in a round robin manner. Input is 64-bit plaintext and we obtain 64-bit cypher text as an output [12,13].

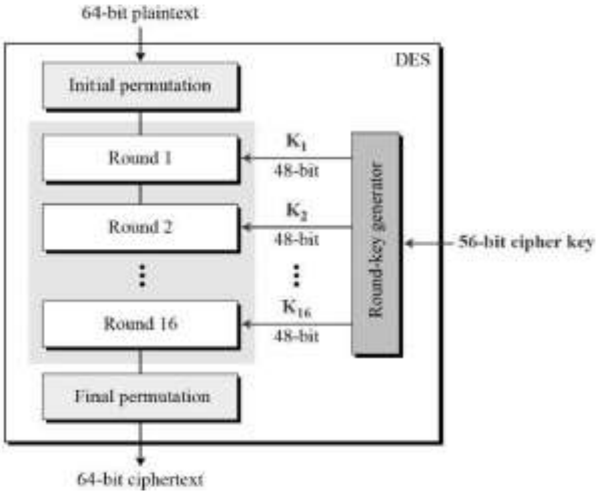

**Fig. 6: DES Process**

DES algorithm consists of three major steps:

- Initial and Final permutation
- Round Function
- Key Schedule

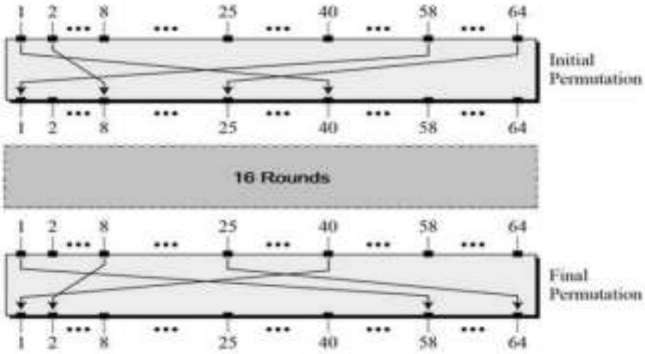

**Fig. 7: Initial and Final Processing**

48-bit key is applied to the rightmost 32 bit to produce 32-bit output.

- **Expansion Permutation Box:** Right input is 32 bit and the key is 48 bit so we need to expand input to 48 bits.
- **XOR:** After expanded permutation, DES does XOR with expanded input and produces 48-bit output.
- **Substitution Boxes:** The output of XOR is given to S-Boxes which consists of 8 S-boxes, each with a 6-bit input and a 4-bit output.

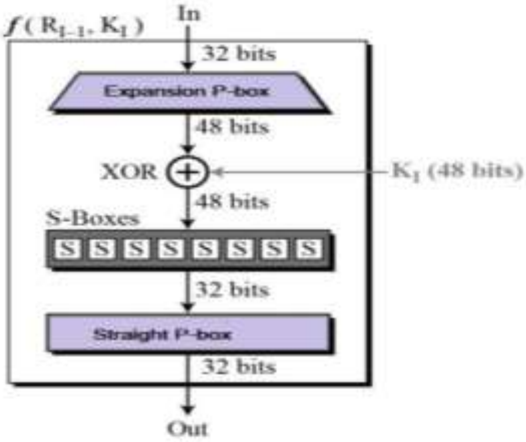

**Fig. 8: Round Functioning**

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The detailed process is depicted in the following diagram.

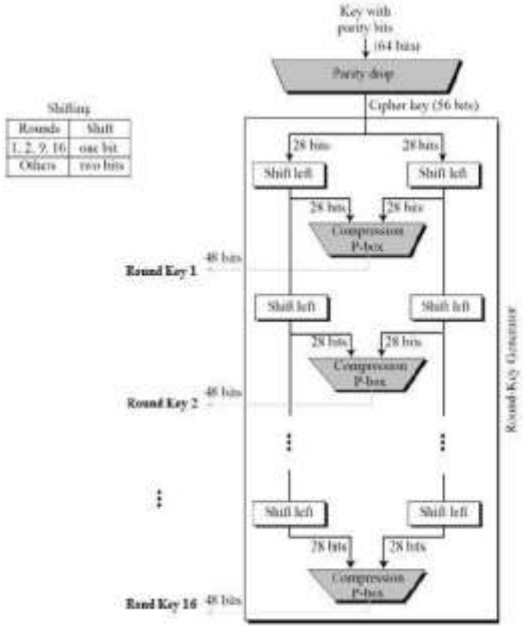

**Fig. 9: Key Schedule**

## 5. IMAGE STEGANOGRAPHY

Following figures illustrate the working of image steganography. The image is selected behind which we need to hide the file. First, the image is converted into 3 bytes/pixel each having R, G, B combination and then is converted into 8bit/bytes binary number [9,10].

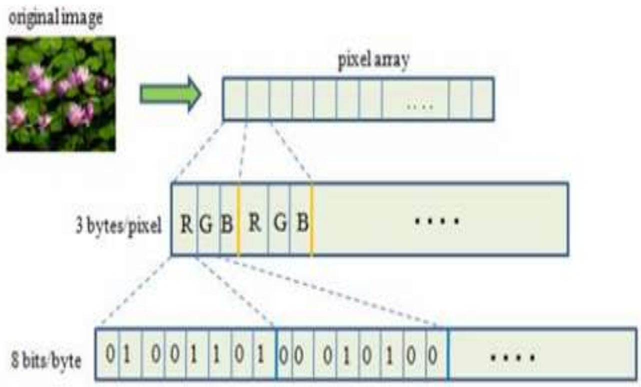

**Fig. 10: Original Image bits**

Then the file is being read character by character. Each character is converted into its ASCII value and then its equivalent 8 bit/byte binary sequence is obtained.

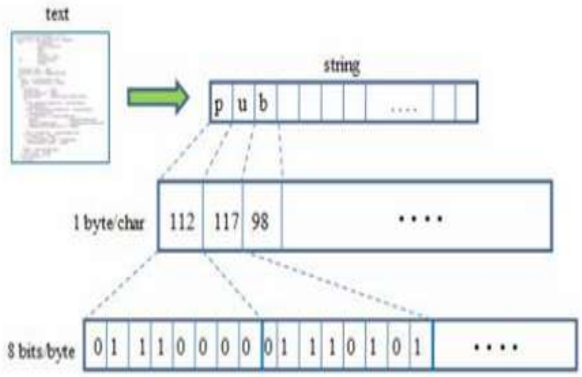

**Fig. 11: Accessing text bits**

Finally, the LSB (Least Significant Bit) algorithm is applied to change the least significant bit of each image byte. In this least significant bit of image, the bit is replaced by text bits and corresponding modified image bits are obtained [15].

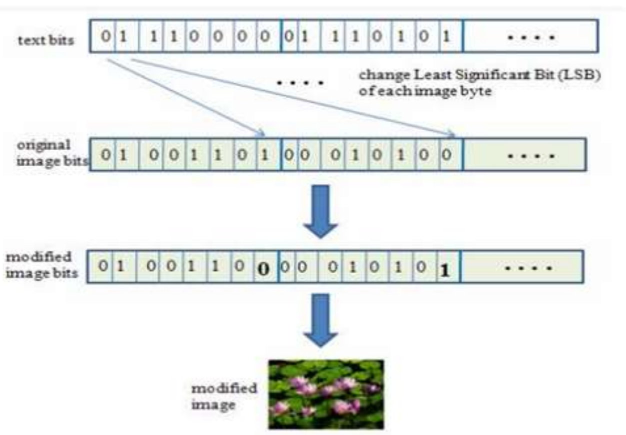

**Fig. 12: Inserting text bits into an image**

## 6. METHODOLOGY

Following diagram represents a snapshot of the internal working of the encryption algorithm. The file that user uploads go through the following steps before getting stored in the database.

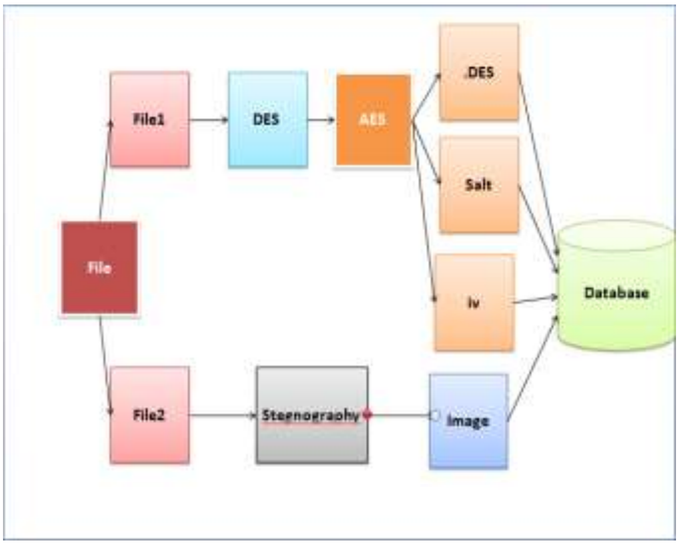

**Fig. 13: Encryption DFD**

- **File Splitting:** The file is split into two parts and these files are given to various encryption techniques. The first file is given to DES Encryption algorithm and the other is given two image steganography [11].
- **DES Encryption:** The DES Encryption encrypts the first part of the file and generates the encrypted file which is later given to the AES Encryption algorithm for further process. DES algorithm provides the first layer of security to the file
- **AES Encryption:** The encrypted file generated by the DES algorithm serves as an input to the AES Encryption and AES encrypts the file further and generates three files namely File1.des, Salt.enc and iv. Enc. These files are further stored in the database.
- **Image Steganography:** The second part of the file is given to image Steganography which steganographers the data inside the image and then stores the image in the database.
- **Database:** In the database, the sender and receiver's name gets stored first and then the corresponding encrypted files (.des, salt, iv) along with the steganographed image are stored sequentially[7,8].

Following diagram represents a snapshot of the internal working of the decryption algorithm. It is the reverse process of the encryption process.

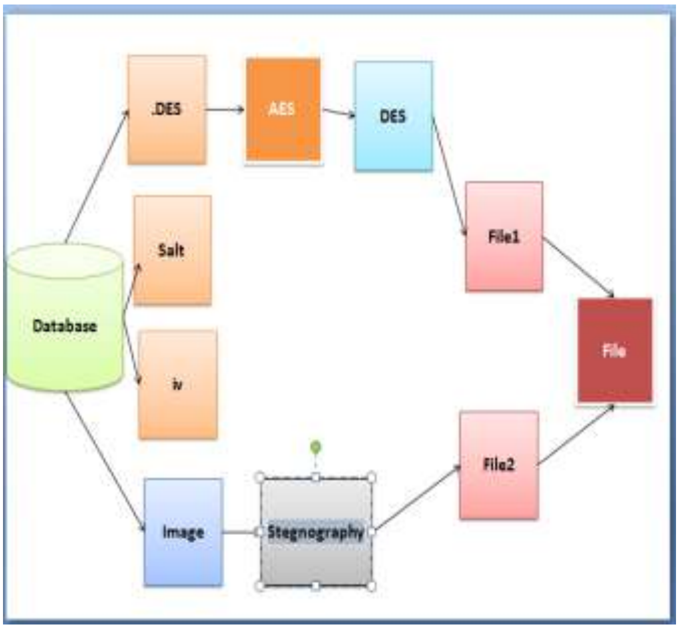

**Fig. 14: Decryption DFD**

- **Retrieving Files from the database:** In the background, all the files are retrieved from the database and given to decryption algorithms. The .des, salt.enc and iv.enc are given to AES decryption algorithm. The image is given to decode for extracting the data.
- **AES Decryption:** The AES Decryption takes three files from the database (.des, salt.enc, iv.enc) and does the decryption process and generates a file which is given to DES Decryption. It further does the decryption process.
- **DES Decryption:** The DES Decryption takes input from AES and does the decryption process and generates the decrypted file which is later combined with the steganographed file to generate the final output.
- **Data Extraction from Image:** The File obtained from the database is given for extraction purpose. It generates a file which is later combined with the first file to generate the output.
- **File Merging:** The two files are combined and generate the final output file which can be downloaded by the user [11].

## 7. IMPLEMENTATION

Following diagram represents a snapshot of implementation of the sender side. The user uploads the file to send to the intended receiver in the following steps.

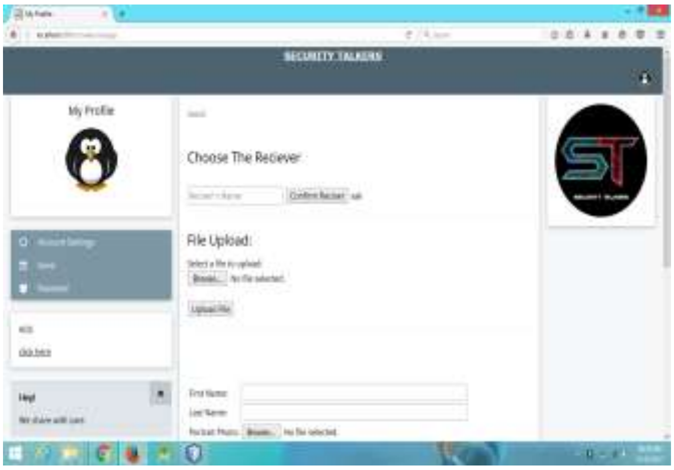

**Fig. 15: Sender side**

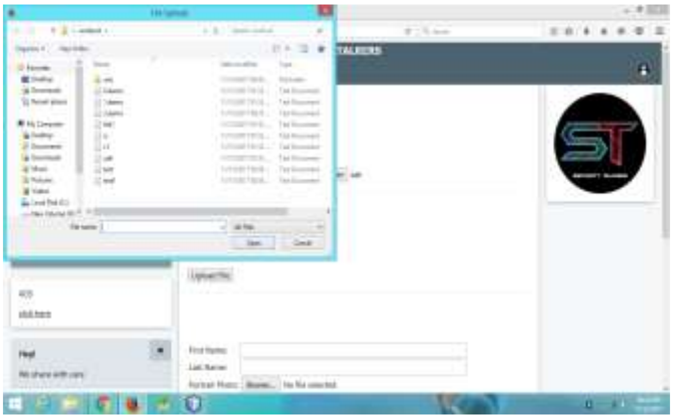

**Fig. 16: User selects a file to send**

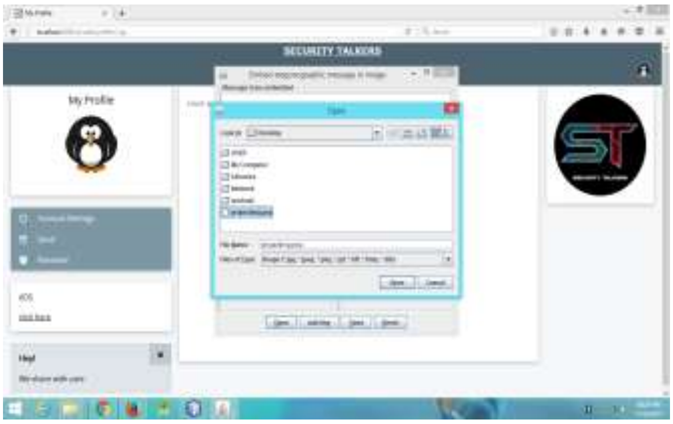

**Fig. 17: User selects an image**

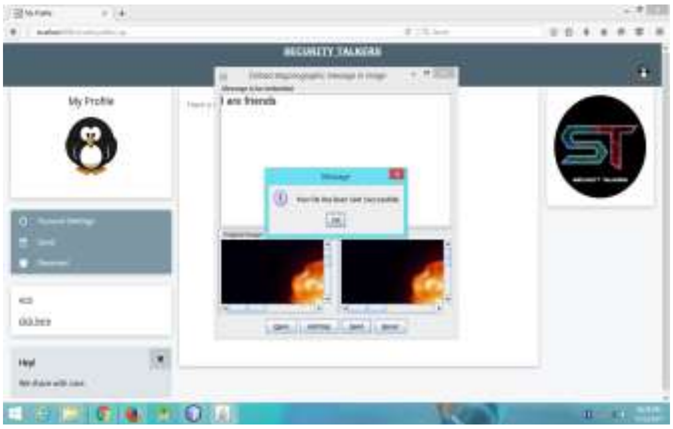

**Fig. 18: The file is encrypted and uploaded on the database**

Following diagram represents a snapshot of implementation of the receiver side. The user selects a file from the listed files that were received; the file is decrypted and downloaded.

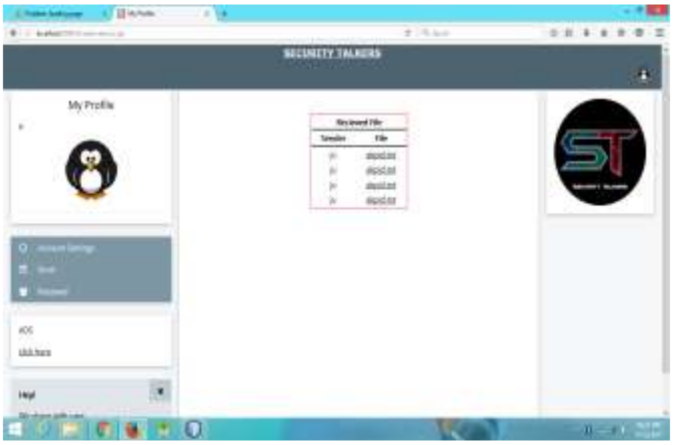

**Fig. 19: User selects a received file to view**

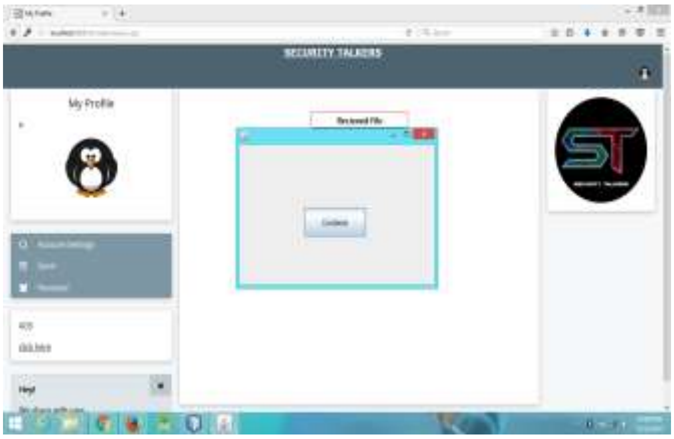

**Fig. 20: To continue decryption**

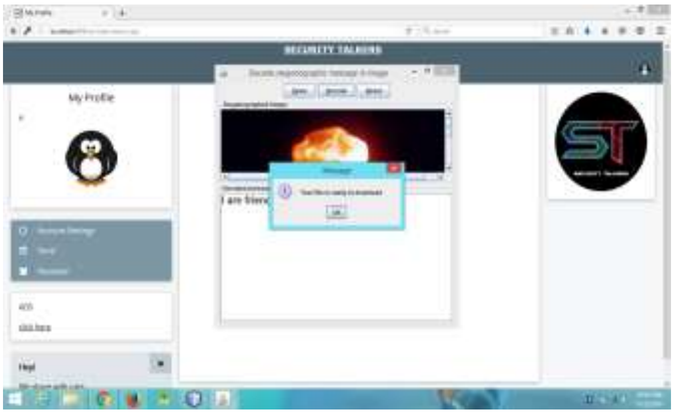

**Fig. 21: The file is decrypted and ready to download**

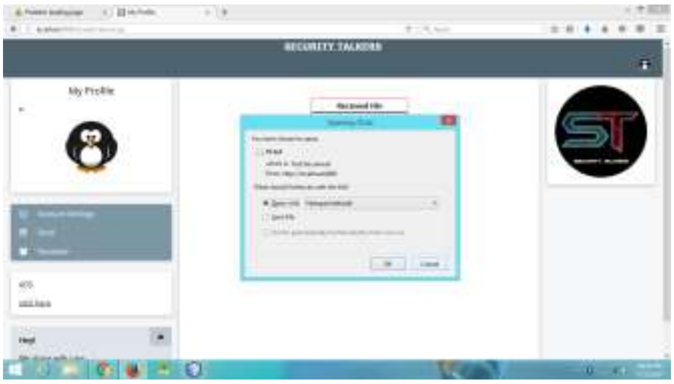

**Fig. 22: Receiver retrieves the original file**

**Table 1: Test Cases**

| Test case id | Description | Expected output | Valid response | Invalid response |
|---|---|---|---|---|
| 1 | The user enters the password | User is registered | Signup successful | Signup failed |
| 2 | A user enters email id | Email id is in the proper format | Validation successful | Validation failed |
| 3 | The user enters the password in the improper format | Format is incorrect | Signup and validation fails | Validated successfully |
| 4 | User tries to login | User logs in successfully | Login successful | Login failed |
| 5 | User enters the wrong password | Access restricted | Login failed | Login successful |
| 6 | User enters an incorrect username | Access restricted | Login failed | Login successful |
| 7 | Both username and password correct | Access is given to the profile | Login successful | Login failed |
| 8 | The encrypted password was not matched | Access denied | Login failed | Login successful |
| 9 | File not selected to send | Sending failed | Fail to send the file | A blank file is sent |
| 10 | The file format is invalid | Sending failed | File not sent | Blank file sent |
| 11 | Uploaded image is not in png format | Sending failed | File not sent | Blank file sent |
| 12 | The file is in proper format and image is in png format | Sending successful | File sent | File not sent |
| 13 | The file size is 0kb | Sending failed | File not sent | File sent as a blank file |
| 14 | The file size is 1kb | Sending successful | File sent | File not sent |
| 15 | File size is 2kb | Sending successful | File sent | File not sent |
| 16 | File size is 30kb | Sending successful | File sent | File not sent |
| 17 | File size is 50kb | Sending successful | File sent | File not sent |
| 18 | File size is 100kb | Uploaded in database | File should not get uploaded in database | File sent and uploaded in database |
| 19 | File not received by intended receiver | File was not sent properly | File not received | -------- |
| 20 | File not able to decrypt | Decryption failed | File retrieved will be encrypted | Garbled data is given |
| 21 | File decrypted | Successful file retrieval | File was received successfully | Garbled data is given |
| 22 | File downloaded | Successful retrieval | File was received successfully | Garbled data is given |
| 23 | Decrypting a 100 kb file | Decryption successful | Decryption successful | Decryption failed |
| 24 | The password was not encrypted during signup | Login failed | User will never get access to their profile | --------- |
| 25 | The file was not downloaded | Download failed | File decrypted but not able to download | File downloaded with garbled data |
| 26 | File downloaded with garbled data | Download failed | Decryption was not proper | --------- |
| 27 | Data not retrieved from database | Receiver side failed | Failure to display data | -------- |

🟥 Failed test cases

□ Successful test cases

### 7.1 Error Discovery Rate

Error Discovery Rate is the ratio of total number of defects found in application to total number of test cases executed.

Error Discovery Rate = Total number of defects found in application / Total number of test cases executed

**Table 2: Error Discovery Ratio Matrix**

| Total number of defects found in application | Total number of test cases executed | Error Discovery Rate |
|---|---|---|
| 5 | 27 | 0.19 |

Error Discovery Rate = 5 / 27
= 0.19 Defects /Test Cases

## 8. CONCLUSION

The Novel Approach to File Encryption is an attempt to help users to access and share their important files securely. As we have used different algorithms, security level has increased tremendously which will be difficult to crack. Knowledge for the project was gathered by surfing various websites. The final database was formulated by using information available on the official websites. The knowledge about cryptography, steganography algorithms was gathered by surfing various IEEE research papers [12,13].

## 9. REFERENCES

[1] B. NageswaraRao, ”Design of modified AES algorithm for data security”, International Journal For Technological Research In Engineering, vol.4, ISSN [2347-4718],2017

[2] R.D.Bajaj, “Design and Simulation of AES Algorithm for Cryptography”, vol.6, ISSN [2321-3361] © 2016 IJESC

[3] A. M.Abdullah, ”AES algorithm to encrypt and decrypt data”, International Journal of Computer Science and Software Engineering (IJCSSE), vol.4,2017

[4] A.Aggarwal and G.Singh, “Implementation of AES algorithm”, International Journal of Engineering Research & Science(IJOER), vol.2, ISSN [2395-6992],2016

[5] S.J.Haun, ”The improved data encryption standard (DES) algorithm”, in IEEE 4th International Symposium, IEEE ISBN**:** 0-7803-3567-8,1996

[6] D.K.Branstad, “Data Encryption Standard: past and future”, in Proceedings of the IEEE, vol.76,IEEE ISSN: [0018-9219],1998

[7] I.Basharat, “Policy Levels Concerning Database Security”, International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004)

[8] M.C.Murray, “Database Security: What Students Need to Know”, Journal of Information Technology Education

[9] A.Shrivastava, L.Singh, “A new hybrid encryption and steganography technique: a survey”, International Journal of Advanced Technology and Engineering Exploration, Vol 3(14) ISSN (Print): 2394-5443

[10] M.Jain, S.K.Lenka, “A Review of Digital Image Steganography using LSB and LSB Array”, International Journal of Applied Engineering Research ISSN 0973-4562 Vol 11, Number 3 (2016) pp 1820-1824

[11] M.Hayder, “Design and Implementation of a File Splitter and Merger Software”, Journal of Kerbala University, Vol. 7 No.4 Scientific. 2009

[12] J.Verma,” IEEE Standard Security Enhancement in Data Encryption Standard”, in International Conference on Information Systems, Technology and Management,2009, pp 325-334

[13] B.Bhat and A.Gupta, ”DES and AES performance evaluation”, in International Conference on Computing, Communication and Automation, Noida,2015

[14] S.Parkar et al, “Study of Different Algorithms and Techniques for Secure File Transmission”, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.2, February- 2015

[15] M.R.Choudhury, “LSB Based Audio Steganography Using Pattern Matching”, Journal of Multidisciplinary Engineering Science and Technology (JMEST), vol.2,IEEE Standard 3159-0040,2015