How to Cite:
Welekar, R., Rajurkar, S., & Kodwani, U. (2022). A novel approach for file encryption. *International Journal of Health Sciences*, *6*(S2), 9447–9455. https://doi.org/10.53730/ijhs.v6nS2.7474

A novel approach for file encryption

R. Welekar
Asst. Professor, Department of Computer Science & Engineering, Shri Ramdeobab a College of Engineering and Management, Nagpur, India
Corresponding author email: welekarr@rknec.edu

S. Rajurkar
Student, Vellore Institute of Technology, Vellore, TN, India
Email: 3sonal.srajurkar@gmail.com

U. Kodwani
Software Developer, Barclays Global services Company, Private Ltd. India
Email: kodwaniurvashi@gmail.com

***Abstract*---**A novel approach to file Encryption is concerned with protecting files being shared among users. The idea revolves around storing files securely so that If someday database is hacked, then data doesn't leaked. To ensure files are protected they are split in 3:1 ration and encrypted using various algorithms like Advance Encryption System (AES) and Data Encryption Standard (DES). Audio steganography method has also been used to improve protection standard.

***Keywords*---**advance encryption standard (AES), data encryption standard (DES), audio steganography, file splitting, file merging.

Introduction

In last few years, cyber-attacks have increased significantly. Many organizations have failed to protect their customer's data. As a result, people now fear sharing their credentials even with well known organizations. Recently, a well trusted bank State Bank of India leaked data of 422 million customers. This happened as one of its servers was unprotected. The server, situated in Mumbai, contained partial bank account numbers, bank balances and phones of individual using the bank's SBI Quick service. Thus cryptographic methods containing these stuff alone will do little harm. Even hackers have now been aware of algorithms in steganography. And the single definition of steganography will fail again. Therefore, an algorithm was required that could combine various approaches and enhance security of existing systems.

Literature Review

It is found from the literature survey that most of the available file encryption mechanisms aren't fully stable. Some of the encryption methods are either AES [1, 2, 3, 7], DES [8] or AES, DES and RSA [6] combinations. Such algorithms give a fair deal of protection. Some file protection frameworks use Audio Steganography [4, 5] to enforce. The technique for separating and merging files was introduced in [9]. We have tried in this paper to combine all these approaches, i.e. to break the input file into two folders. Apply DES and AES to one file, and Audio steganography to another file, and do the reverse on the side of the receiver. We explore ways for safe image transmission in [13]. Cloud data encryption strategies were given in [14,15].

Implementation

Internal Working of the Algorithm

Initially the file that needs to be secured is split into two parts in the ratio of 3:1. This involves file splitting mechanism. The ratio being 3:1 means 75% of the file will undergo encryption using AES Algorithm & DES Algorithm while the other part which is 25% of the file uses Audio Steganography for its encryption purpose. There is two level encryptions involved in first part. The file has to perform DES encryption followed by AES encryption. After performing AES encryption, three different extensions file is generated which is stored in the database. In the latter part, the file goes through audio steganography which means hiding the file behind audio file. The output of this is also stored into the database. The overall encryption workflow is explained in Fig. 1.

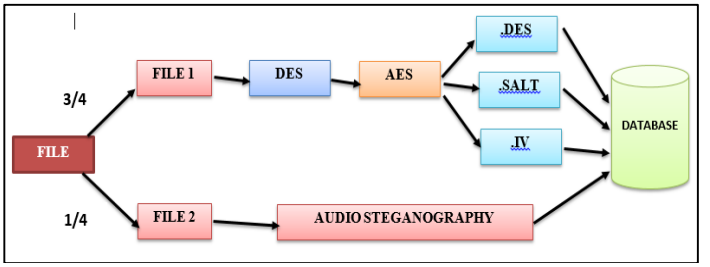

Fig. 1:Internal working of Encryption Algorithm.

Decryption is opposite to the encryption process. In decryption, the different extension files are retrieved using AES decryption method from the database. The output of this is given as input to the DES decryption mechanism. Now the latter part is retrieved from the audio file using the same key used in encryption. Finally, both the files are merged using file merging algorithm. The overall decryption workflow can be seen in Fig.2.

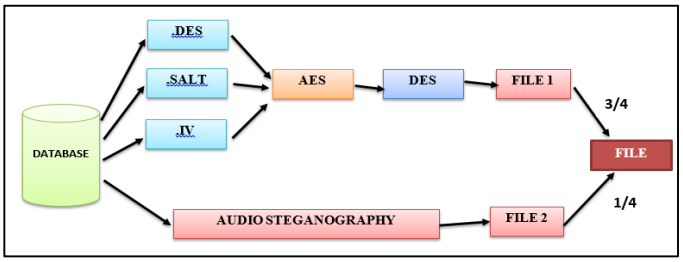

Fig. 2:Internal working of Decryption Algorithm.

The implementation is done in following parts:

1) File Splitting. The file which needs to be encrypted is split into two parts as shown in Fig.3 and these files are given to various encryption techniques. The splitting of file is done in 3: 1 ratio. The reason for keeping the ratio as 3:1 is that the hiding the file behind the audio file posses' little limitations. As a result, only one-fourth part of the file is send to the audio steganography part for efficient working of the system. The first file is given to DES Encryption algorithm and the other is given to audio steganography [9].

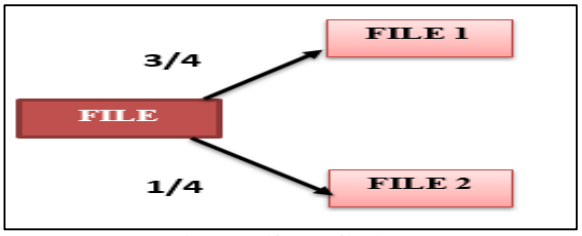

Fig. 3:File Splitting

2) DES Encryption. After applying file splitting algorithm, the bigger part of file is given as input to the DES encryption mechanism. This proves as first level security of the file [8]. Fig.4 and Fig.5 illustrates the detailed process of DES algorithm. This algorithm basically consists of 16 rounds with 2 additional steps which are termed as initial and final permutation. 64-bit plaintext is provided as input to initial permutation block. Then after the output from initial permutation is given to round 1. At each round the file is X-ORed with the 48-bit key which is generated from Round Key generator. Finally, the values from subsequent rounds is given to the final permutation block. After that we obtain the 64[bit cipher text or encrypted text. It works in round robin manner [3,8].

Fig. 4:Internal Working of DES Algorithm

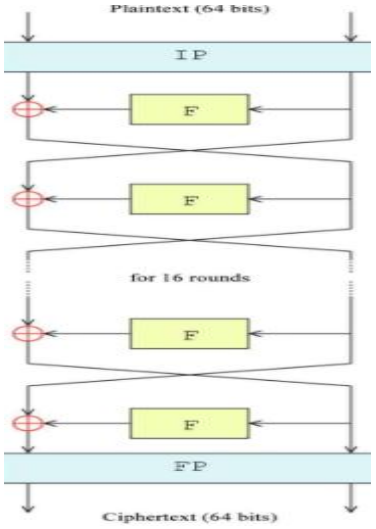

Fig. 5:Working of Initial and Final Permutation

Now there is need to convert the 64-bit plaintext to 48-bit text as the key generated is of 48-bit. So to accomplish this, the 64-bit file is distributed equally into two 32-bit (right and left). Then following three steps are applied on that 32-bit values.

Expansion Permutation Box: The key is 48-bit long so the input needs to be enlarged so that it matches with the key. So 32-bit right input is given to the expansion block so as to make it equal to 48-bit key

XOR: Now the key as well as input is of 48-bit size so the XOR operation is performed between them so as to produce 48-bit output.

Substitution Boxes: Commonly known as S-Boxes. It has 8 boxes that accepts 6-bit input and produces 4-bit output each. So the output of XOR step is given to

the S-Boxes which takes 48-bit input (8*6=48) and produces 32-bit output (8*4 = 32).

AES Encryption. The output of DES encryption is given as input to AES algorithm. This acts as second level of security for the file. AES generally generates three encrypted files which has extensions as .des, .salt and .iv. Finally, these files are stored in the database collectively.

Fig. 6 illustrates the working of AES algorithm. Unlike DES algorithm that has 56-bit key, AES algorithm has variable key including 128, 192, 256-bit. It uses 10 rounds for 128-bit key, 12 rounds for 192-bit key and 14 rounds for 256-bit keys. It is more efficient as compared to DES algorithm. In the following figure, 128-bit plaintext is given as input to the AES algorithm. Initially pre round transformation takes place then the result is passed on to subsequent rounds. At every round particular key is provided based on number of rounds. Finally, the encrypted cipher text is obtained which is of 128-bit.

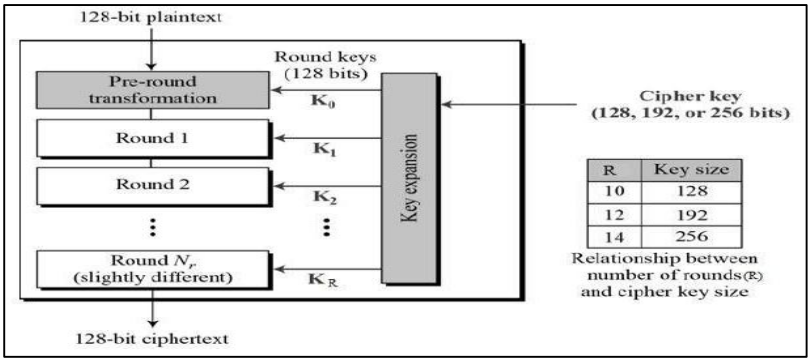

Fig. 6:Internal working of AES Algorithm

Every round has four steps each namely a) Sub Bytes b) Shift Rows c) Mix Columns d) Add Round Key [1]. Initially, the plaintext is XORed with first 128-bit round key. Then after for 9 rounds the process is repeated. This can be observed in the Fig.7. The four basic sub steps are:

Sub Bytes: In this, 16 input bytes are substituted using standard S-Box. The value is computed by taking unique column and row value. The resultant matrix is generally of the form four rows and four columns.

Shift Rows: In this, every value is shifted towards its left depending on its row number. For example, first row values will be shifted by 1 towards its left. Second row values will be shifted by 2 and so on.

Mix Columns: In this, each column is transformed into new column values using special mathematical function. This function takes the values of one column and outputs the new values that replaces the original column values. This step is not performed in the last round.

Add Round Key: At this stage round key is XORed and it acts as input for the next round. In the last round it gives the cipher text.

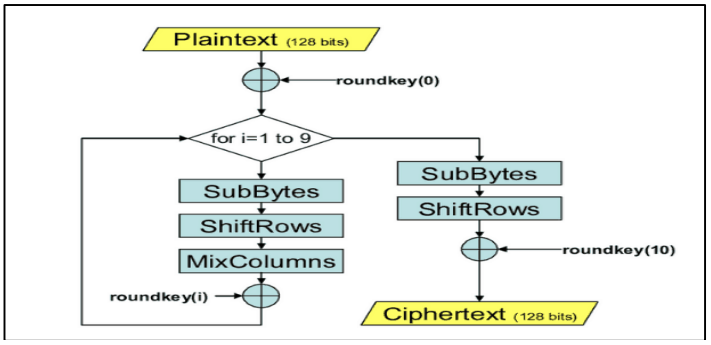

Fig.7Steps involved in AES algorithm

Audio Steganography. The second part of file is given to audio Steganography which hides the data inside the audio and then stores it in the database. Audio Steganography is the algorithm in which file is stored behind the audio or any multimedia device. It is way of hiding secret text or audio information in a host message. Fig 7 provides the overall flow of the audio steganography. Initially the original file which needs to be secure is provided along with the audio file. These are given to the steganography tool which hides the data into audio. One such tool is DeepSound steganography tool. It helps in hiding the data into the corresponding audio file. It is independent of the format of the message and can therefore convert the data into audio converter system. Audio is considered to be more secure as compared to the images.

When the data needs to be decrypted it is again given to the steganography tool and the particular data is retrieved from the audio file.

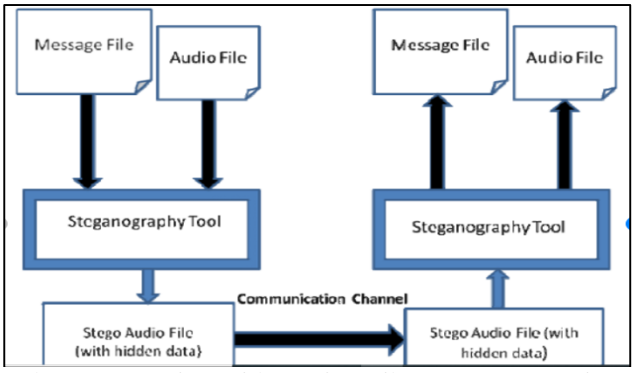

Fig.8Internal working of Audio Steganography

There are different types of audio steganography techniques available namely:
LSB Coding
Phase Coding
Echo Hiding
Spread Spectrum

Out of these LSB Coding is considered as efficient because it has low computational complexity, easier implementation and variations available. The

following figure depicts the steps involved in the LSB algorithm. There are mainly four steps involved:

Step 1: Initially it receives the audio file and convert it into the bit pattern.
Step 2: Every character in the text is converted into bit pattern.
Step 3: LSB is replaced using RC4 algorithm.
Step 4: Replaces the LSB bit from audio file with LSB bit from text file.

Fig.9Steps involved in LSB Algorithm

The following figure explains how the changing of bits takes place. The LSB bit is chosen and then is given to the RC4 Algorithm. RC4 algorithm are basically of two types a) The key scheduling algorithm and b) The pseudo-random generation algorithm.

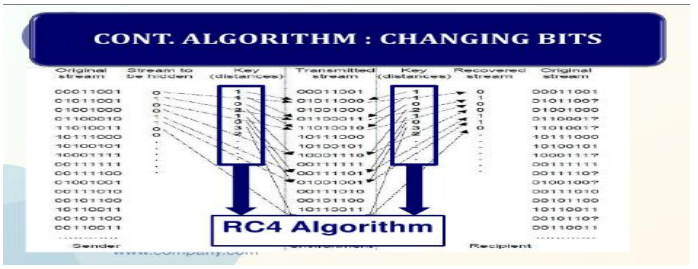

Fig.10Bits Changing

Database. The name of the sender and receiver is first stored in the database, and the corresponding encrypted files (.des, salt, iv) are then stored sequentially along with the steganographed audio file.

AES Decryption. The decryption process starts at the side of the recipient. The files from the database are retrieved using the AES decryption mechanism. These files are .des, .salt and .iv. After obtaining the files, AES decryption algorithm is applied and the output of it is given to the DES algorithm for decryption purpose. This decrypts the second level security of the file.

DES Decryption. Now the output of AES decryption mechanism serves as an input to the DES decryption algorithm. This decrypts the first level security of the file. At this time, the original bigger part of the file is retrieved with us.

Data Extraction from Audio. Now the second part needs to be decrypted. This is done by decryption process of audio steganography. For this purpose, the audio

file that is stored in database is retrieved using the key that is used during encryption process. This results in retrieving of the remaining part of the file.

File Merging. Both the files are now retrieved successfully and needs to be merged to obtain the original text back. This is performed using file merging algorithm. [9].

User Interface Implementation

Implementation on Sender Side
On the website the user must build an account. Upon signing up, the user is directed to his profile, where various choices are made available, such as sending file, displaying files received. The user can sign in to the program directly if he / she already has an account.

User can choose to upload any file. The uploaded file is split into file1 and file2. The file is split into two parts according to their size. The file1 is then passed for two level encryption. The file 2 is given for audio steganography. The encrypted audio file is then sent to the user.

Implementation on Receiver Side

Even the recipient must have a website account. File cannot otherwise be exchanged. The receiver can view the message from the sender. The table shows up containing two columns such as the name of the sender and the name of the file. In fact, this filename is a connection from which the receiver can download the file.

A hybrid solution to improve file protection and thereby make it more difficult to decrypt even if anyone wants to snatch a file, the file cannot be hindered unless and until all four files are accessed and organized in the same manner and decrypted using certain algorithms in the same order, making it more difficult to decipher the con-tents, the files splitting adds more security to the original data. Hampering the files or stealing the information from the database is not enough to decrypt the original data of the file, the added rates to these existing algorithms allow the file to be decoded more complexly, the algorithms operate in a fixed order and use fixed keys for encryption, To decrypt the file one need a key to decrypt, a proper solution to such formulas, a proper sequence of operations to follow to encrypt and decrypt the file, these added rounds to the encryption method improve the degree of data protection, including the exact file merging algorithm.

Conclusion

The Novel Approach to File Encryption is an effort to help users safely access their essential files and share them. Since various security algorithms has been used, the degree of protection has increased exponentially and would be hard to crack. Knowledge was gathered for the project by visiting different websites. The final database was constructed using the details available on the official websites.

References

1. Ahmad N, Hasan R, Jubadi W.: Design of AES S-Box using combinational logic optimization. IEEE Symposium on Industrial Electronics & Applications. IEEE, Penang. 696-699 (2010).
2. Gayathri K, Yasmeen W. :Data encryption and decryption using AES with key length of 256 bits. International Journal of Scientific Engineering and Technology Research. 4143-4146.(2014)
3. Dadhich S.: Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java. International Journal of Computer Trends and Technology (IJCTT) .35(4). 179-183. (2016)
4. Jain R, Boaddh J.: Advances in Digital Image Steganography. IEEE International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). IEEE, Noida (2016).
5. Joseph P, Vishnu Kumar S.: A study on stenographic techniques. In: Proceedings of IEEE global conference on communication technologies (GCCT), pp 206–210.(2015)
6. Singh G., Kinger S.: A Study of Encryption Algorithms (RSA,DES,3DES and AES) for Information Security. International Journal of Computer Applications. 67(19). 33-38.(2013)
7. Bajaj R, Gokhale U.: Design and Simulation of AES Algorithm for Cryptography. International Journal of Engineering Science and Computing. IJESC.(2016)
8. Verma J., Prasad S.: Security Enhancement in Data Encryption Standard. International Conference on Information Systems, Technology and Management. Springer, Berlin.325-334. (2009).
9. Koli N, Parkar S., GiriM. : Secure File Transmission using Split and Merge Technique. International Journal of Computer Science and Mobile Computing. 59-64. IJCSMC. (2015).
10. Thakur N., Razzaque A. : Image Compression and Encryption: An Overview. International Journal of Engineering Research and Technology 1 (5), 1-7.(2012)
11. Thakur N., Razzaque A. :An Approach for Image Compression and Encryption. International Journal of Image Processing and Vision Sciences 1 (2), 52-55. (2012)
12. Deshmukh K., Thakur N. :An Overview and Approach for Joint Image Encryption and Compression. International Journal of Scientific & Engineering Research 7 (2), 403-408. (2016)
13. Pande A., Thakur N. :A Survey on Different Ways of Secure Image Transmission. International Research Journal of Engineering and Technology 5 (2), 407-413. (2018)
14. Kale P., Welekar R. : Secure ranked keyword search algorithm for encrypted cloud data using double indexing technique. Journal of Engineering and Applied Sciences 13(1),32-37. (2018)
15. Kale P., Welekar R. : A survey on different techniques for encrypted cloud data. International Conference on Intelligent Computing and Control Systems (ICICCS). pp. 245-247, Madurai. (2017)