MULTI LAYER SECURITY USING ENCRYPTION AND STEGANOGRAPHY

[1]Uzochukwu Osakwe, [2]Dr. Umarani .C

[1]Student, [2]Associate Professor,
[1] Department of MCA,
[1]Jain University, Bangalore, India.

Abstract: With the high availability of internet and the huge growth of technology information security has become complex and a problem that needs urgent attendance, in this present era, security has become one of the major concerns in the IT industry, to enhance the security of information certain encryption mechanism has been created to resolve the issues. Encryption is the process of converting a message or information into code known as cipher to prevent unauthorized person from acquiring access to the information. Another technique use in this project is Steganography which is the hiding of the existence of information so that the information can be transmitted undetected. Steganography allows the sender hide the message within a cover message [1]. The use of steganography, in this project is combined with encryption to create an extra layer of security information.

This project Fibonacci series technique is use for encryption and decryption to secure the information, this technique can secure any type of file and the encryption and decryption is based on loss-less and key dependent. And the application of Audio and Image Steganography which will be used to hide the encrypted information, hence providing extra layer of security for files. These mechanisms are implemented using python.

Key words - Encryption, Decryption, Steganography, Cipher, unauthorized, Security, Fibonacci.

1.INTRODUCTION

On a daily basis millions of security breaches occur and one way to prevent it is by implementing information security management. Security management has become a top concern in the corporate world. Due to the high rate of internet availability millions of files are been generated and hence intruders try to get peoples' information stolen every day and very little approaches or steps has been taken in to minimize this issue. This project has been created to implement high level of security and provide an extra layer of security through encoding/hiding of data with the help of encryption/decryption and steganography.

The word 'cryptography' was formed by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.

Encryption has prevented unauthorized person from extracting any information, even if the jumbled messages fell in their hand, Cryptography involves converting plain text into cipher to ensure that it is protected from unauthorized person. Cryptography converts information into a format that is unreadable with bare eyes and from an unauthorized user, allowing the information to be transmitted without unauthorized entities being aware of the information in transit or decoding it back into a readable format. Information security uses cryptography and Steganography on several levels, the information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored.

Steganography is data hiding technique, which inserts the data into a cover data which are mostly media files. Steganography is a hiding technique that can be used along with cryptography as an extra-secure method to protect information. Steganography techniques can be applied to images, a video file or an audio file. Steganography is use by those seeking to pass secret message or code and ensure no one knows the where about of the information. Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content.

2.LITERATURE REVIEW

Although security has been considered in the design of the basic Internet protocols, many applications have been and are being designed with minimal attention paid to issues of confidentiality, authentication, and privacy. As our daily activities become more and more reliant upon data networks, the importance of understanding of such security issues will only increase [2] this is where cryptography comes into the picture.

Encryption is a method of transforming data with the intension of keeping it a secret. It uses an algorithm called a cipher to encrypt data and it can be decrypted only using a special key.

Encrypted information is known as cipher text and the process of obtaining the original information (plaintext) from the cipher text is known as decryption. Encryption is specially required when communicating over an untrusted medium such as internet, where information needs to be protected from other third parties. Encryption can be defined as the process of transforming information in such a manner that only authorized person can understand the shared information. In this paper, we have taken Playfair encryption algorithm for encryption and modified it by using Fibonacci series. Fibonacci series is used to generate a random key, which is used for encrypting the message in Playfair encryption algorithm [3]. Steganography is the technique in which a message is hidden in a carrier object. In image steganography, particularly, the hidden message should not be visible using simple eye inspection. The usual parties in a steganography technique are: the sender, who hides a message inside a medium and the steganography file receiver, who will unveil the transmitted hidden message. The message is embedded in an image called a cover image; after the message is hidden,

we have a steganography file. In this technique, data bits of the message to be hidden are arranged randomly and image pixel bits are also made unique making it unintelligible to recognize the pattern [4]. Steganography involves hiding of text, image or any sensitive information inside another image, video or audio in such a way that an attacker will not be able to detect its presence.

3.CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

There are three types of cryptographic techniques used in general:

- Symmetric-key Cryptography: In this technique, both the sender and receiver share a single key. The sender uses a single key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message to unveil the plain text.
- Hash Functions: No key is applied in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the plain text to be recovered. The Hash functions are also used by many operating systems to encrypt passwords.
- Public-key Cryptography: In Public-Key Cryptography two keys are used (public and private key). Public key may be freely distributed, while its paired private key remains a secret. In public key cryptography the public key is use to encrypt the text while the private key for decryption.

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise). The text steganography techniques include:

- Feature Coding: In feature coding, certain text features are altered, or not altered, depending on the codeword.
- Line-Shift Coding: the text lines are vertically shifted to encode the document uniquely.
- Word-Shift Coding: The codeword's are coded into a document by shifting the horizontal locations of words within text lines, while maintaining a natural spacing appearance.

Hiding information inside images is a popular technique, where a secret message can be hidden and then transferred to the intended receiver. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image, as mentioned below:

- LSB: A simple approach for embedding information in cover image is using Least Significant Bits (LSB). It is a technique in which we hide messages inside an image by replacing Least Significant Bit of image with the bits of message to be hidden.
- Masking and Filtering: It involves the modification of the image that can involve in discernible changes in the image, even if the changes are not visible to the naked eye.
- Transformation: This is an overwhelmingly complex technique for image steganography. This uses discrete cosine transformation that is majorly used in JPEG image compressions.

In audio steganography we embed the confined message into a digital sound, which can be WAV, MP3 and even AU sound files. The audio steganography consist of the carrier, message and password, the carrier is also known as cover file. secret messages can also be hidden in audio files using the following methods:

- Echo Hiding: In this technique, the secret message is embedded into the cover audio as an echo. They are adjusted in a way such that the echoes are inaudible to humans.
- LSB: The audio signals are converted to digital binary sequences. The Least Significant Bit of the binary sequence is converted to the binary value of the message.
- Phase Coding: It is based on the analysis of the phase discontinuities. The secret message is divided according to bits and is encoded as the phase shifts in the phase spectrum in the audio file.
- Spread Spectrum: There are 2 approaches in this method: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS)

4.PROPOSED SYSTEM

This project can be said to be a tool that uses encryption and steganography mechanism use to provide extra layer of security to data/information stored by the user in the system. This project uses Fibonacci series technique for encryption and decryption. In this technique one can secure any type of files. In this project, we propose an image steganography method which hides data in it. Image Steganography uses an image as the cover to hide the secret message.

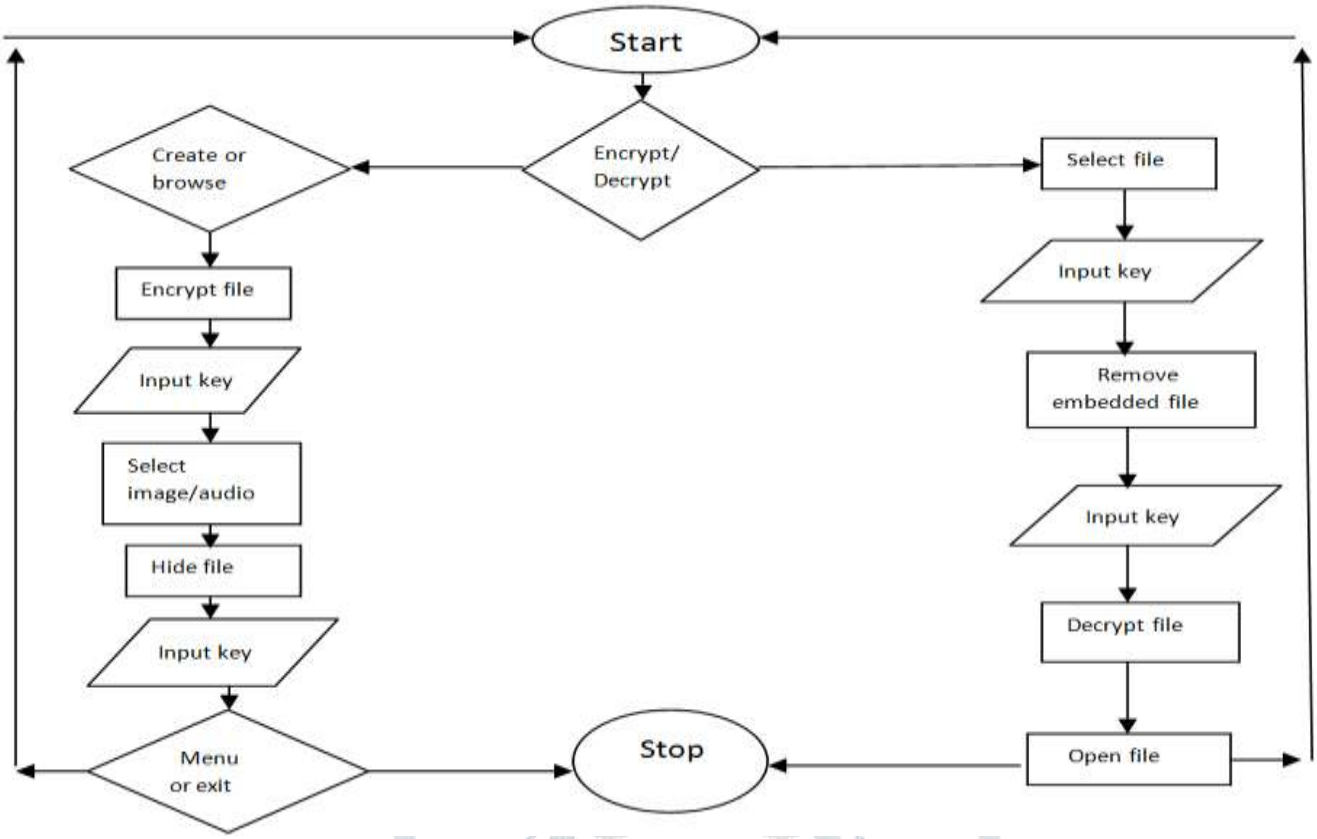

Fig 1: Proposed work

The proposed work provides two layers of security as it not only encrypts the message but also performs image and audio steganography by sending the encrypted message along with the image. This project is designed to flow in 2 phases; these phases include Cryptography and Steganography which has sub phases. The project has 2 phases; the first phase consists of an encrypter that encrypts the saved text file, this encrypter uses a principle of Fibonacci series, the file is shifted according to its position on the file in reference to the Fibonacci series principle. In the next sub-phase, we make use of series of codes to implement a steganography technique. At this phase, the program stores the encrypted text file inside an audio or image file for extra security.

5.ENCRYPTION AND DECRYPTION PHASE

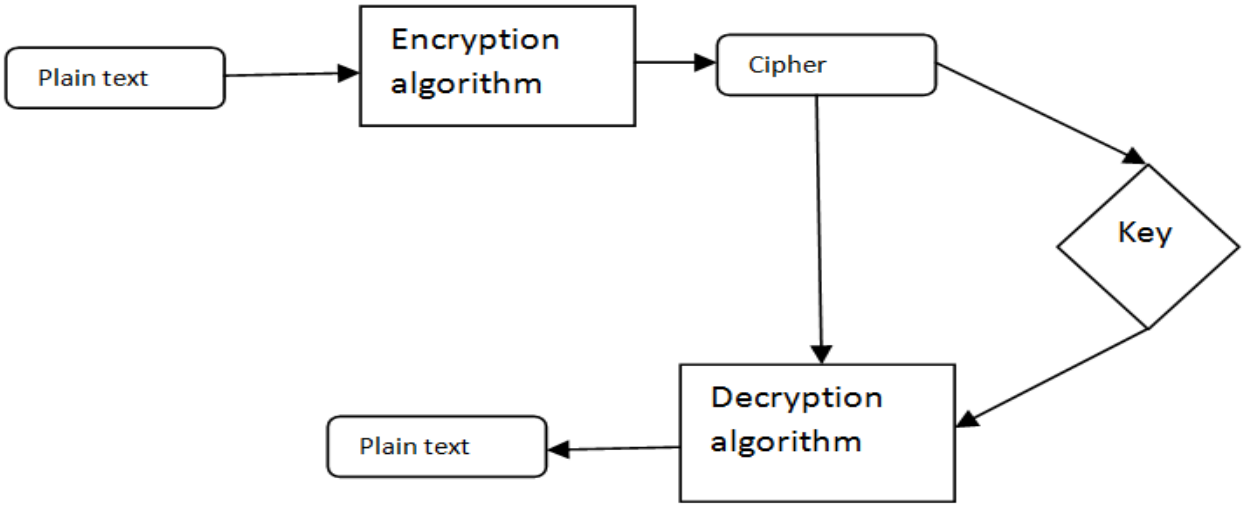

Fig 2: Data Flow

ENCRYPTION PHASE

Encryption is the process of transforming plain text into cipher text, which has no meaning. In the encryption phase, the message is taken into the encrypter and then the encrypter encrypts the message. this project uses Fibonacci series to implement the encryption phase. This happens by splitting the messages into their separated words, the words from the message are reversed and then that word is split into letters. These letters are now incremented and decremented alternatively based on the Fibonacci series. For example, if the word from a message is 'abc' and that word is reversed as 'cba'. That word ('cba') is now spitted into a letter. Now the number of letters in the word 'fed' is 3 so the Fibonacci series of the length of the word is '1, 1, 2' (This excludes the first 0).

- Now the first letter of the word 'c' is incremented by the first number in the Fibonacci series which is 1, making 'c' to become's'.
- The incremented letter 'd' is now incremented by the next Fibonacci series number which is 1 again. Therefore, converts 'd' to 'e'.
- The next Fibonacci series number is 2. The encrypted letter now 'e' is then incremented by 2 which convert 'e' to 'g'.
- Now the next letter 'b' will be decremented by the first number of the Fibonacci series which changes 'b' to 'a'.
- The incremented letter 'a' is now decremented by the next Fibonacci series number which is 1 again. Therefore, converts 'a' to '`', which is the minimum ASCII value our letters can be set as.
- The next Fibonacci series number is 2. The encrypted letter now '!' is then incremented by 2 which converts '`' to '^'.
- Then the next letter 'a' will be incremented by the first number of the Fibonacci series which changes 'a' to 'b'.
- The incremented letter 'b' is now incremented by the next Fibonacci series number which is 1 again. Therefore, converts 'b' to 'c'
- The next Fibonacci series number is 2. The encrypted letter now 'e' is then incremented by 2 which convert 'c' to 'e'.
- Now the encrypted text of 'abc' is now 'g^e'

DECRYPTION PHASE

In this phase, the project uses the Fibonacci series principle to convert the cipher text into a plain text. What this does it that the cipher text is passed into the decrypter. Then it splits that cipher message into letters just as the encryption phase does and then decrements and increments the letters alternatively. Remember the encrypted text created before was 'g^e'. Both the encryption and decryption phase act alike in this project but what differs is if the first letter is either incremented or decremented and then the rest of the letters in that word will follow alternatively to the previous letter. In decryption the first letter of the word is decremented.

- The encrypted word being passed in here is 'g^e'. This is divided into letters and the length of the word (g^e) is recorded as 3 to define the number of Fibonacci series will be implemented.
- Now the first letter of the word 'g' is decremented by the first number in the Fibonacci series which is 1, making 'g' to become 'f'.
- The incremented letter 'f' is now decremented by the next Fibonacci series number which is 1 again. Therefore, converts 'f' to 'e'
- The next Fibonacci series number is 2. The encrypted letter now 'e' is then decremented by 2 which convert 'e' to 'c'.
- Now the next letter '^' will be incremented by the first number of the Fibonacci series which changes '^' to '_ '.
- The incremented letter '_' is now incremented by the next Fibonacci series number which is 1 again. Therefore, converts ' _ ' to ' ` ', which is the minimum ASCII value our letters can be set as.
- The next Fibonacci series number is 2. The encrypted letter now '!' is then incremented by 2 which converts ' ` ' to 'a'.
- Then the next letter 'e' will be decremented by the first number of the Fibonacci series which changes 'e' to 'd'.
- The incremented letter'd' is now decremented by the next Fibonacci series number which is 1 again. Therefore, converts 'd' to 'c'
- The next Fibonacci series number is 2. The encrypted letter now 'e' is then incremented by 2 which converts 'c' to 'a'.
- Now 'g^e' is now converted to 'cba'.
- Then the word(cba) is now reversed to 'abc'

6.STEGANOGRAPHY PHASE

This phase works with basically two mechanisms: the insertion mechanism and the extraction mechanism. The insertion mechanism encodes the text to the image/audio and the extraction mechanism decodes the text out of the image/audio.

Images are simply made out of pixels; huge numbers of pixels are combined to make an image look the way they are. A pixel is the smallest unit of a digital image or graphic that can be displayed and represented on a digital display device. Pixels are combined to form a complete image, video, text.

Unlike image which is based on pixels, audio is a file format for storing digital audio file, the audio file is consist of sounds that are divided into bytes.

IMAGE STEGANOGRAPHY INSERTION/ EXTRACTION MECHANISM

The insertion mechanism simply involves embedding the secret message to the carrier image. It makes use of certain customized principles to hide message inside an image. The following explains the principles used in promoting data hiding in images.

- A copy of the selected image is used to hide the data
- The secret message is passed into the program, divided into multiple letters (including the spaces) and then converted into their binary format.

- Each letter/character is now in their binary form.
- Since the binary number contains 8 bits, we are going to take 3 pixels out of the image which is holding 3 RGB data and use those each data to hold a single bit.
- Then that RGB data is return back to the image and implemented

The extraction mechanism refers to the extraction of the secret message from the image. This removes the secret message that is still in its encrypted format out of the image. The extraction mechanism gets the pixels from the image by row and column. Since these pixels contains RGB data and the message has been entered into this data. The message can now be extracted.

AUDIO STEGANOGRAPHY INSERTION/ EXTRACTION MECHANISM

The LSB (Least Significant Bit) algorithm which is the classic steganography method is use, it represents the bit at units place in binary. LSB algorithm replaces the LSB of each byte in the carrier (audio file) with one bit from the secret message.

The sender embed the bit of secret message onto the carrier data byte by byte, whereas the receiver performs the extraction by reading the LSB bits of each byte of received data, by doing this the receiver reconstruct the secret message.

7.FUTURE SCOPE

In this Paper, we are dealing ensuring information security by using Encryption and Steganography. Future scope can be working on the time efficiency and portability of the GUI. System when fully deployed will ensure efficiency.

8.CONCLUSION

This project shows that an encryption and steganography algorithms once combined can provide extra layer of security, hence serving the purpose of ensuring information security through the implementation of cryptography for protecting sensitive data and steganography to hide the data in an image and audio.

With the results showing that the image and audio still remains intact and the encrypted file has been decrypted properly to its original state, it can be safely said that the procedures has been successfully implemented.

9.ACKNOWLEDGMENT

I want to specially thank **Dr. Umarani .C** for guiding me throughout this research paper, which has expand my knowledge on data security. Without her support I do not think this research paper will be a success, I am very thankful.

REFERENCES

[1] P. M. Asha Asok, "Implementation and Comparison of different Data," IEEE, p. 4, 2019.

[2] R. T. S. K. Lipi Kothari, "Data hiding on web using combination of," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019.

[3] S. B. Navneet kaur, "Audio Steganography Techniques," *IJERA*, vol. 5, no. 6, pp. 94-100, 2014.

[4] S. A.-M. A. B. NANDHINI SUBRAMANIAN, "Image Steganography: A Review," *IEEE*, vol. 9, pp. 23409 - 23423, 2021.

[5] M. U. S. M. M. U. F. Mohd Vasim Ahamad, "An Improved Playfair Encryption Technique Using Fibonacci," *International Journal of Engineering & Technology*, vol. 7, pp. 347-351, 2018.

[6] A.A. Lubis, R. Purba and I. A. Pardosi, "Combination of Steganography with K Means Clustering and 256 AES Cryptography for Secret Message," in *2019 Fourth International Conference on Informatics and Computing (ICIC)*, Semarang, Indonesia, 2019.

[7] G. Benedict, "Improved File Security System Using Multiple Image Steganography," in *2019 International Conference on Data Science and Communication (IconDSC)*, Bangalore, India, 2019.