International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

REVIEW PAPER ON MULTI LAYER SECURITY USING ENCRYPTION AND STEGANOGRAPHY

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

[1]Student, [2]Associate Professor

Jain University, Bangalore, India

Abstract - The availability of internet has caused gigantic growth of information and with that leads necessity of information security in our present generation. Information security is the application of security mechanisms such as encryptions, steganography etc to ensure that information are not accessed by unauthorized individual. Encryption and steganography are one of the important mechanisms used to enforce security. Encryption is the encoding of texts/ messages so that only the person with encryption key can gain access while steganography is the hiding of texts/ messages into a cover message {Image, Audio and video }this mechanisms prevents unauthorized interceptions or access to data.

Key Words: Decryption, Steganography, Cipher, unauthorized, Security, Fibonacci

1. INTRODUCTION

On a day to day run millions of security breaches occur and the way to prevent it is by implementing information security mechanisms. Due to the high rate of internet availability files are been generated and hence intruders try to get peoples' information stolen every day hence the requirement of extra layer of security .

Encryption has prevented unauthorized person from extracting any information, even if the 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. Steganography is the process of hiding data, which inserts the data into a cover data (Image, Audio and video). Steganography is a hiding technique that can be used along with cryptography as an extra-secure method to protect information.

2. An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key

Nowadays, information security is the concern in the transmission of information over the internet. To ensure the security of information encryption mechanisms is used causing the information to be on unreadable format. In playfair encryption a biggest disadvantage is that it cannot be used to encrypt huge files and the key is easily detected hence the proposed work, we can see that playfair encryption and Fibonacci series which was use to generate secret key provided stronger security and good encrypt huge files.

2.1 Combination Of Steganography With K Means Clustering And 256 AES Cryptography For Secret Message

Information encryption is the process of ensuring that the information is not readable to unauthorized person. A traditional file security will be the use of a single security technique which in this present age is not efficient, hence the proposed system which combine cryptography and steganography to ensure a more secure means of protecting information.

The proposed methodology is AES 256; the message will be based on 32 keys and 14 rounds. The insertion process uses K Means Clustering, this p[process is use to divide message that will be inserted in the image.

2.2 Improved File Security System Using Multiple Image Steganography

Information security is becoming a vital asset hence the use of steganography to hide the information in the media file by doing so we are providing extra layer of security for information. Image steganography is the most common and secure method for steganography mostly applied. Traditional steganography techniques use a single cover image to hide the secret information which has few security shortcomings. Therefore, batch steganography has been applied which stores data on multiple images. A technique of data hiding is proposed in this paper which is least significant bit (LSB). All the selected cover image pixel values is used, Then the pixels are re-written with the secret data bits. A retrieval of the hidden data from the cover image files is also achieved through a Java Application for the simulation purpose.

2.3 A Dual Layer Image Encryption using Polymerase Chain Reaction Amplification and DNA Encryption

DNA encryption ensures that image files are highly secure and this is achieved through the use for DNA encryption which is based on biological sequence DNA Encryption and Polymerase Chain Reaction (PCR) Amplification is used to enhance the security of the image.

Two keys are use here which is one, the key provided by the user and the second key which is provided by the Primer, and once a wrong key is applied for decryption the image is force to loss its form.

3. CONCLUSIONS

The purpose of encryption and steganography is to implement security in information security. from a technical view encryption and steganography is the solution for security challenges present in transmission of information. The application of single mechanisms of security in this era is not efficient oriented hence the combination of two security mechanisms (encryption and steganography) as an added layer of security to information's,. By doing so it will reduce the rate of unauthorized persons gaining access to information.

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 media.

ACKNOWLEDGEMENT

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.