DOD DATA HIDING TECHNIQUE USING ADVANCED LSB WITH AES-256 ALGORITHM

Dr. M.P. CHITRA[1], N. KAVITHA SRI[2], V. BHAVYA PRIYANKA[3], M. HARINI[4]

[1]Professor, Department of Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India,
[2,3,4]Student, Department of Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India,

---***---

Abstract - *This project is to make a secure and robust method of information exchange so that confidential and private data must be protected against cyber attacks and illegal access. Various algorithms are developed for data hiding as of now but each have some limitations and some advantages too. According to the level and kind of application one or more data hiding method are used. Data hiding can be done in audio, video, text, image and in other form of information. Some data hiding techniques emphasizes on digital image security and robustness of digital image hiding process while other's main focus is on imperceptibility of digital image. Hide is also a main concern in some of the applications. Here AES-256 algorithm is used to encrypt the user data and then using advanced LSB technique Data can be hidden in any file format such that except the sender and receiver, no one even suspects the existence of the secret hidden Data. The data may be of any kind of file from normal text file to huge video achieved.*

***KeyWords*: Aes Algorithm, Encryption, Decryption, RSA Token, Safe and Secured**

1. INTRODUCTION

Capacity of digital Information which has to hide is also the main concern in some of the applications. Here AES-256 algorithm is used to encrypt the user data and then using advanced LSB technique Data can be hidden in any file format such that except the sender and receiver, no one even suspects the existence of the secret hidden Data. The data may be of any kind of file from normal text file to huge video achieved. We are in the world of digitization. Each and everything are digital, Digital Information is ubiquitous nowadays. For the integration, confidentiality and security of Digital Information, traditional data hiding schemes have to be upgraded and need to be used in conjunction with other schemes.

1.1SECURE DIGITAL INFORMATION

For this various schemes has been proposed to protect and secure the Digital Information which are stegnography, watermarking and cryptography and their combinations. All of these schemes have different issues to handle and different aims to be achieved which is particularly depends upon the type of application domain in which Digital Information is being used and manipulated. Security, robustness and fragility are the main concern which are associated with these data hiding techniques and some parameters are being used for the acceptability of scheme being used subject to the above concerns which may have different values for different applications.

2. TO ACHIEVE ROBUSTNESS

The key of this project is to achieve two or more than two parameters i.e. Security, robustness, imperceptibility and capacity but some of the parameters are trade-off which mean only one can be achieved on the cost of other. So the data hiding techniques aiming to achieve maximum requirements i.e. security, robustness, capacity, imperceptibility etc. and which can be utilized in larger domain of applications is desired.

3. RELATED WORK

For the implementation of this paper, we had reference with below related ideas.

1. Secure Data Hiding Technique by Video Steganography and Watermarking International Journal of Computer Applications Shivani Khosla ,Paramjeet Kaur. This paper presents video steganography using digital watermarking techniques provides a strong backbone for its security.

2. Implementation and Design of HDFS Data Encryption Scheme using ARIA Algorithm on Hadoop, Youngho Song, Young-Sung Shin, Miyoung Jang, Jae-Woo Chang. ARIA algorithm is used as a standard data encryption scheme for domestic usages.

3. In this paper, we propose a HDFS data encryption scheme that supports both ARIA and AES algorithms.

4. Data Hiding using Advanced LSB with RSA Algorithm. Varsha, Rajender Singh Chhillar the message is encrypted and then encrypted message is being divided in two parts. First part of the encrypted message is done xor operation with odd position and next part with even position of LSB+1.

4. EXISTING SYSTEM

1. Only Image and video files can be encrypted using watermarking.

2. Cannot Process Higher data files and Application .EXE files.

3. Lacks Two Factor Authentication so lacks Data security during transmission.

4. Needs High memory Space (RAM Usage) during Data Processing.

5. PROPOSED SYSTEM

In order to achieve the Secure transmission over internet securely Original File is secretly hidden in a Normal File of any kind. RSA Key is taken as a cover medium for encryption and AES 256 algorithm is used for encryption.

In this proposed method advanced LSB bit manipulation method is used for embedding the message in the any DATA file and the message is itself encrypted using the existing RSA Key.

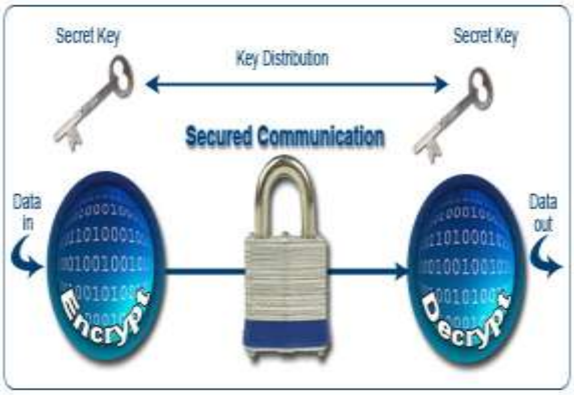

Fig -1: SECURED COMMUNICATION

For embedding the Secret File in Data file firstly both the info are converted into binary equivalent and then text is encrypted. The encrypted secret file is then embedded into the Data file.

At the receiver side, the sent Normal DATA file must be selected to extract the secret Data File. After selecting the file and advanced lsb method is applied to extract the encrypted message and this message is decrypted using the Reverse AES 256 algorithm. A comparison is made between the original image file and the embedded one to indicate CRC.

6. BLOCK DIAGRAM

The data may be of any kind of file from normal text file to huge video achieved.

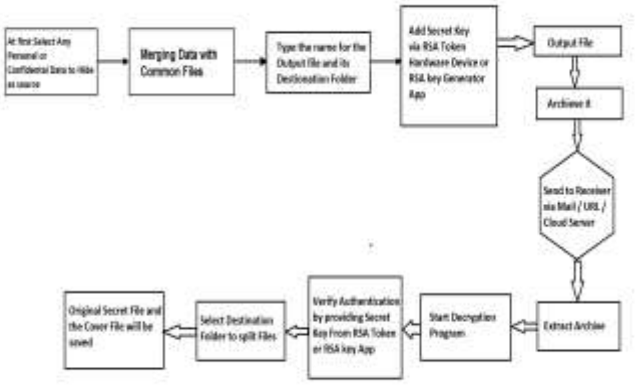
At first Select Any Personal or Confidential Data to Hide as source
Merging Data with Common Files
Type the name for the Output File and its Destionation Folder
Add Secret Key via RSA Token Hardware Device or RSA key Generator App
Output File
Archieve it
Send to Receiver via Mail / URL / Cloud Server
Extract Archive
Start Decryption Program
Verify Authentication by providing Secret Key From RSA Token or RSA key App
Select Destination Folder to split Files
Original Secret File and the Cover File will be saved

Fig -2: BLOCK DIAGRAM OF THE PROCESS

7. LITERATURE SURVEY

1.Shivani Khosla M.Tech (CSE),Indo Global College of Engineering, Abhipur,Mohali-Punjab, India andParamjeet Kaur A.P (CSE),Indo Global College of Engineering, Abhipur,Mohali-Punjab, IndiaSecure Data Hiding Technique Using Video Steganography and Watermarking International Journal of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014. The rapid development of data transfer via internet made it easier to send the data withaccuracy and faster to the destination. Besides this, anyone can modify and misuse the valuable information through hacking at the same time. This paperpresents video steganography with digital watermarking techniques as an efficient and robust tool for protection. This paper is a combination of Steganography and watermarking which provides a strong backbone for its security. Here considers video as set of frames or images and the changes in the output image by hidden data is not recognizable visually.

2. Monica Adriana Dag,Emil Ioan Slusanschi,Razvan Dobre from University Politehnica of Bucharest, Faculty of Automatic Control and Computers,Computer Science and Engineering Department done Data Hiding Using Steganography and published in 2013 IEEE 12th International Symposium on Parallel and Distributed Computing. It is a truth universally acknowledged that “a picture is worth a thousand words”. The emerge of digital media has taken this quote to a new level. By using steganography, one can hide not only 1000, but thousands of words even in an averagesized image. This article presents various types of techniques usedby modern digital steganography, as well as the implementation of the least significant bit (LSB) method. The main objective is to create an application which uses insertion of LSB in order to encode data into a cover image. Both serial and parallel version are proposed and an analysis of performances is made byimages ranging from 1.9 to 131 megapixels.

3. Youngho Song, Young-Sung Shin, Miyoung Jang, Jae-Woo Chang, Dept. of Computer Engineering Chonbuk National University, Republic of Korea done Design and Implementation of HDFS Data Encryption Scheme using ARIA Algorithm on Hadoop and published in 2017 IEEE International Conference on Big Data and Smart Computing. Hadoop is developed as a distributed data processing platform for analyzing big data. Enterprises can analyze big data containing users' sensitive information by using Hadoop and utilize them for their marketing. Therefore, researches on data encryption are widely done to protect the leakage of sensitive data present in Hadoop. However, the existing researches support only the AES international standard data encryption algorithm. Meanwhile, the Korean government selected ARIA algorithm as a standard data encryption scheme for domestic usages. In this paper, we propose a HDFS data encryption scheme which supports both ARIA and AES algorithms on Hadoop. First, the proposed scheme provides a HDFS block-splitting component that performs ARIA/AES encryption and decryption under the Hadoop distributed computing environment. Second, the proposed scheme provides a variable-length data processing component that can perform encryption and decryption by adding dummy data, in case when the last data block does not contains 128-bit data. Finally, we show from performance analysis that our proposed scheme is efficient for various applications, such as word counting, sorting, k-Means, and hierarchical clustering.

8.1 AES ALGORITHM

Advanced Encryption Standard (AES) is a combination of both substitution and permutation, and is fast in both software and hardware.

Most AES calculations are done in a 2 special finite field. The number of repetitions of transformation rounds that converts the input, called the plaintext, into the final output, called the cipher text is denoted by the key size of an AES Cipher. Each each containing four similar but different stages, including one that depends on the encryption key itself.

8.2 HARDWARE REQUIRED

Fig -3: HARDWARE CONNECTION

- Desktop Pc / laptop with Internet Connectivity
- Dual core processor Or Higher
- 2GB RAM or higher
- 250GB HDD Space or higher
- LAN/Wifi/NDIS
- Hardware RSA Key

Fig -4: RSA TOKEN

8.3 SOFTWARE TOOLS

- System Software: Win8 x86 or higher version
- Application Software:

1. Microsoft .net 3.5 or higher

2. Java 8 Update 151 CPU Java 8 Update 152 PSU (OTN) Release Oct17, 2017 or higher version

3. Embedded System Simulator 0.9.0

9. FLOWCHART

Here is the flowchart on how the procedure takes place and it is given below.

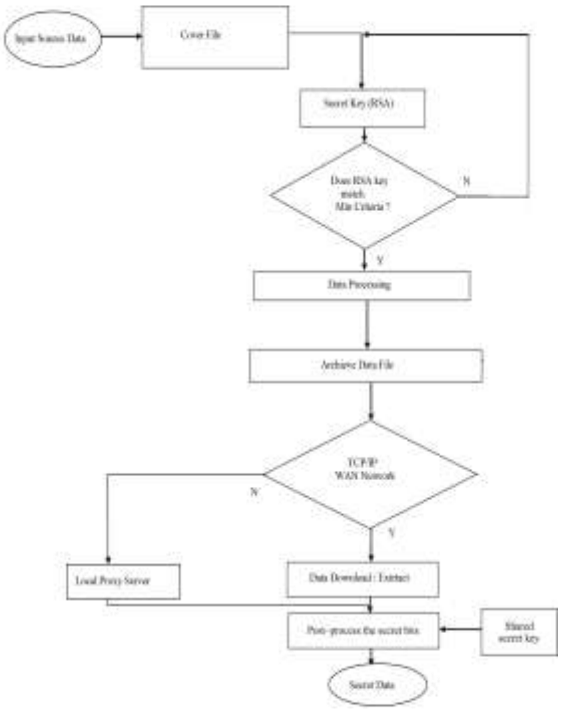

Fig -5: STEPS TO BE FOLLOWED DURING DATA TRANSMISSION

10. ADVANTAGES

Below are the several Advantages,

- ❖ Practically All File Types can be encrypted and sent securely over internet
- ❖ This Algorithm Can Process Higher size data files, .exe files, .apk files, Disk Image files
- ❖ High Grade AES256 Encryption and Two Factor Authentication enables high Data security during transmission
- ❖ Can Run on Basic Desktop Pc/Laptop even with Low ram and processor during Data Processing

11. RESULT

The purpose of hiding information depends on the application and the needs of the owner of digital media. Some requirements of data hiding are: Reliability- Reliable communication is one of the properties of the data hiding. The data hiding should guarantee the reliable transmission of the information to the recipient. Security- The data hiding Method should provide security for data such that only intended user can access it, in other words it is unable of unauthorized user to access secrete information. Payload Capacity- It refers to the amount of secret information can be hidden in the cover medium. So, provide the sufficient embedding capacity. Robustness**-** It refers to the amount of information that can be hidden without any effect and destroying hidden information.

12. CONCLUSION

Nowadays, information hiding techniques become more important in a number of applications. Such as Digital audio, video, and images, which may contain a hidden copyright notice or help to prevent unauthorized copyright. Military communications systems makes more use of traffic security techniques.In this project work a new system for the combination of both encryption with data hiding has been presented which could be proven as a highly secured method for data communication in near future. The proposed High secured system is tested and a research is made by taking Data samples and hiding them in images/audio files/video or even a document. The results that are obtained from these experiments and time took for encoding and decoding the file are noted down. The Proposed algorithm provides more security in comparison to previous algorithm.

REFERENCES

[1] M. Qiu, M. Zhong, J. Li, K. Gai, and Z. Zong. Phase-change memory optimization for green cloud with genetic algorithm. IEEE Transactions on Computers, 64(12):3528 – 3540, 2015.

[2] K. Gai and S. Li. Towards cloud computing: a literature review on cloud computing and its development trends. In 2012 Fourth Int'l Conf. on Multimedia Information Networking and Security, pages 142–146, Nanjing, China, 2012.

[3] J. Li, Z. Ming, M. Qiu, G. Quan, X. Qin, and T. Chen. Resource allocation robustness in multi-core embedded systems with inaccurate information. Journal of Systems Architecture, 57(9):840–849, 2011.

[4] L. Chen, Y. Duan, M. Qiu, J. Xiong, and K. Gai. Adaptive resource allocation optimization in heterogeneous mobile cloud systems. In The 2nd IEEE International Conference on Cyber Security and Cloud Computing, pages 19–24, New York, USA, 2015. IEEE.

[5] J. Niu, Y. Gao, M. Qiu, and Z. Ming. Selecting proper wireless network interfaces for user experience enhancement with guaranteed probability. Journal of Parallel and Distributed Computing,72(12):1565–1575, 2012.

[6] K. Gai, Z. Du, M. Qiu, and H. Zhao. Efficiency-aware workload optimizations of heterogenous cloud computing for capacity planningin financial industry. In The 2nd IEEE International Conference on Cyber Security and Cloud Computing, pages 1–6, New York, USA,2015. IEEE.

[7] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. Journal of Network and Computer Applications, 59:46–54, 2015.

[8] K. Gai, M. Qiu, and H. Zhao. Security-aware efficient mass distributed storage approach for cloud systems in big data. In The 2nd IEEE International Conference on Big Data Security on Cloud,pages 140–145, New York, USA, 2016.

[9] K. Gai, M. Qiu, L. Tao, and Y. Zhu. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Security and Communication Networks, pages 1–10, 2015.

[10] G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, and X. Qin. A decentralized approach for mining event correlations in distributed system monitoring. Journal of parallel and Distributed Computing,73(3):330–340, 2013.