ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Survey on Data Security

Swapnil Bhosale[1], Ashish Nikalje[2], Swapnil Borude[3], Himalaya Wadhwani[4,] Latika Desai[5]

B.E Student, Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology Pimpri, Pune, India[1,2,3,4]

Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology Pimpri, Pune, India[5]

ABSTRACT: In now a day's data security is an essential need of the data transmission so a secure image transmission technique is proposed, which transfers our data through network to anyone. The rapid development of data transfer through internet made it easier to send data more accurately and faster to the destination. Beside this anyone can modify the data and misuse the valuable information by hacking into the system or the network. In this paper a new technique of data hiding is proposed for effective and efficient data hiding. In current generation the internet communication video is considered to be effective and important for communication. Data hiding is one of the common approaches to secure data. In this technique the exiting is concealed. For creating a secure transmission technique a number of reference papers and algorithms have been referred to give the proposed method. For this transmission techniques like mosaic image for data hiding is also used been used. Basically in our technique we basically focus on data like text data, image data, audio data and video data. For data hiding in video we focus on data frames.

KEYWORDS: Data Frame, Data Hiding, Genetic Algorithm, Information Hiding, Mosaic Image, Steganography

I. INTRODUCTION

Data sending or message passing has been one of the important and crucial tasks since ages. From past times sending data in safe, secure and a fast manner has been an area of concern. Earlier this task was accomplished use letters, telegrams or telegraphs. But now in the digital era internet have become the most powerful way of communicating and the most trending way of communicating.

Mailing websites like gmail , yahoo and social networking websites like facebook, twitter etc is most popular way of sending and receiving messages. In today's world hacking into the network, getting into someone others system, manipulating the messages has become a very easy task. Due to such situations data security has become an important and one of the most the critical issues.To solve such problems, many techniques like image Steganography, cryptography, digital signature and many other techniques and algorithms have been developed which worked effectively initially but smart and technologically smart hacker have found various techniques to even crack such advanced data security techniques.

To provide a new level to the data security, a new technique which a combination of various techniques and algorithm has been introduced in this paper which will make the hacker confuse about which packet to target and what to hack to get the correct and transmitted data.

II. RELATED WORK

To develop the above mentioned technique a rigorous, deep and a complete study of various existing technique is required. The technique developed is a blend of 10 – 12 various techniques and algorithms which are specified in various reference papers and journal. The prominent papers from which the basic idea of the project or the combining technology has been derived are as follows:

I. A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Image by Nearly Reversible Color Transformation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

By referring this paper we got an idea of hiding an image behind another image using different technique. In this paper the technique converts a secret image into a sensible and a meaningful mosaic image of the same size and looking like a preselected target image. The conversion or more precisely the transformation is controlled by a secret key and only the person having the secret key can recover the secret image from the mosaic image. Basically the mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. In this technique the secret imageis divided into rectangular tiles and which are then fit into the similar target block, according to the similarity criteria based on color variation. Then the characteristic of each tile image is transformed to be that of the corresponding target block in the target image resulting in mosaic image which is similar to the target image.

II. Audio – Video Steganography Using Forensic Technique For Data Security

This paper mainly focuses on image hiding or image secrecy using a video file instead of only using a image file. The main reason behind using a video file is that allows the user to also add text type of data to get encrypted in the file. In this paper a technique is introduced in which a video file is selected and is divided into separate files of audio and video formats. Then the data is encrypted in audio file using a key and image in one of the frames of the video file then the two files are combined back into the video which was same as that before encryption and is send to the receiver where the receiver does the process of reverse engineering i.e. separates the encrypted video file into audio and video format which are also encrypted then decodes the data from the audio file and secret image from the video file using the key which was used while encryption and retrieves the required data

III. Audio-Video Crypto Steganography using LSB Substitution and advanced chaotic algorithm

In this paper the method described for data security is same as that described in *Audio – Video Steganography Using Forensic Technique for Data Security* which is the paper stated above i.e.a video file is selected and is divided into separate files of audio and video formats. Then the data is encrypted in audio file using a key and image in one of the frames of the video file then the two files are combined back into the video which was same as that before encryption and is send to the receiver where the receiver does the process of reverse engineering i.e. separates the encrypted video file into audio and video format which are also encrypted then decodes the data from the audio file and secret image from the video file using the key which was used while encryption and retrieves the required data. The main catch in this method is the use of advanced chaotic algorithm. Due to its extremely sensitive nature to initial conditions and many more interesting characteristics they have shown several remarkable properties. The sequences which are generated by these chaotic functions are very complicated and random. One of the characteristics of such functions is their sensitivity to initial conditions. One of the main reason and advantage of using the chaotic function is shape of the chaotic signal which looks like noise to the unauthorized user.

IV. Genetic Algorithm in Audio Steganography

Using the LSB techniques for hiding the data in an audio file is an effective and a simple technique but it becomes very easy for any person to read the audio sample in sequence and to check whether it gives some meaningful message or not. Thus the security of the sequence also lies in the sequence of accessing audio frames and hence target bits used for data hiding. To overcome this drawback a new method called Genetic Algorithm has been introduced which has been inspired from the biological genetics, and chromosomal phenomenon. Various concepts from the real biological terms like genes, chromosomes and their functionalities have been taken into consideration and as per the specified method or technology these concepts has been implemented in the paper. Biological terms like mutation, generating population etc. have been used in this paper with reference to the technical conditions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

V. Audio Steganography using RSA Algorithm and Genetic based Substitution method to enhance security

The technique explained in this paper is an enhancement to the technique of genetic algorithm and it adds a new level to the audio Steganography. In this paper they used the both the techniques i.e. RSA Algorithm and the Genetic algorithm. This paper gives a solution the problems related to the substitution technique of audio Steganography. It basically works in two levels. In first level RSA algorithm is applied on the data to encrypt the message, and then in the next level encrypted message is encrypted in audio data using genetic algorithm based substitution method. The basic idea to use these techniques in such a manner and order to increase and enhance security and robustness.

VI. Secure Data Hiding Technique Using Video Steganography and Watermarking

In this paper a technique which shows the authentication of the owner is introduced which is called as watermarking. Digital watermarking is a technique in which a digital signal or pattern can be inserted in a digital content. The main reason or the advantage behind using such techniques is that it can be used to identify the owner of the work, to trace illegal copies and to authenticate the content of the work. The difference between Steganography and watermarkingis that the object of communication in watermarking is the host signal with the embedded data providing copyright protection. In steganography, the object to be transmitted is the embedded message and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability.

VII. Improved Security Mechanism of Text in Video using Steganographic Technique

A combination of two algorithms i.e. RSA algorithm and HASH - LSB algorithm has been used to encrypt text in a video file. Parameters like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Bit Error Rate (BER) has been used to define and set the standards for the quality of the video. In this method first the method first the message is encrypted using the RSA algorithm and then the original message, encrypted message and the video is brought together and the HASH – LSB algorithm is applied on it which is then used to generate the key file and the stego video. To extract the secret data from the stego video the same key is used and the process of reverse engineering is applied.

III. FINDINGS AND RESULTS

The above stated papers have been studied and many more journals and references have been studied to find a unique techniques which comprises of the benefits of the studied techniques and removes the loop holes of the referred techniques so that a software can be developed which no loop holes exists and is full proof technique for securing the data. The techniques which are adopted or will be used to develop the software are specified below:

1. Creation of Mosaic Image Creation and hiding the secret image behind the target image using a fragment image creation -A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations

2. Technique of genetic algorithm and use of it in audio Steganography- Genetic Algorithm in Audio Steganography

3. The idea of dividing the video file into a audio file and a video file and then encrypting the text data in audio file and image in the video is derived from this paper - Audio - video Steganography using forensic technique for data security

4. Encrypting the text in a video file was the technique derived from this paper where techniques of RSA and HASH LSB is used - Improved Security Mechanism of Text in Video using Steganographic Technique

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

5. The technique of visual cryptography is adopted from this paper - Use of Genetic Algorithm and Visual Cryptography for Data Hiding in image for Wireless Network

6. Use of concepts like genetic algorithm in encrypting the data in video filespecified in this paper - Optimized Video Steganography using Genetic Algorithm (GA)

7. The concept of watermarking which is a method of authenticating the digital content is one of the best and the secure method for encrypting the data and avoids it illegal copies, authenticate the content. So basically the security of the content while the content is in the network is provided by this technique - Secure Data Hiding Technique Using Video Steganography and Watermarking

IV. CONCLUSION

In this project we proposed a new technique to hide a data and transfer it securely. Initially user must give the input in the format of text, audio or video. User may give input in all three formats. Then by applying different algorithm for encryption input data is encrypted. For more security in this system we are introducing mosaic image to create illusion finally at the end all the input data and mosaic image are combined together and form one package that contain text, audio and video data. This package is transferred to receiver. By using this system we can provide better transmission and network security. Our primary aim is to receive the data at receivers end lossless. In today's world data security is one of the most critical and sensitive issue.

REFERENCES

1. A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations Ya-Lin Lee, Student Member, *IEEE*, and Wen-Hsiang Tsai, Senior Member, IEEE
2. Genetic Algorithm in Audio Steganography Manisha Rana, Rohit Tanwar
3. AUDIO - VIDEO STEGANOGRAPHY USING FORENSIC TECHNIQUEFOR DATA SECURITY Athira Mohanan, Reshma Remanan, Dr. Sasidhar Babu Suvanam, Dr. Kalyankar N V
4. Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm Praveen. P, Arun. R
5. A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS SELECTION Odai M. Al-Shatanawi1 and Nameer N. El. Emam
6. Optimized Video Steganography using Genetic Algorithm (GA**)** Kousik Dasgupta, Jyots na Kumar Mondalb, Paramartha Duttac
7. Audio Steganography using RSA Algorithm and Genetic based Substitution method to Enhance Security Gaurav Singh,Kuldeep Tiwari,Shubhangi Singh
8. Secure Data Hiding Technique Using Video Steganography and Watermarking Shivani khosala, Paramjeet Kaur
9. Improved Security Mechanism of Text in Video using Steganographic Technique, Manpreet Kaur, AmanDeep Kaur
10. Use of Genetic Algorithm and Visual Cryptography for Data Hiding in image for Wireless Network , Yogita Patil

BIOGRAPHY

Swapnil Bhosale is a student in the Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology Pimpri, Pune, India. Pursuing Bachelor Of Engineering degree in Computer Science.

Ashish Nikalje is a student in the Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology Pimpri, Pune, India. Pursuing Bachelor Of Engineering degree in Computer Science.

Swapnil Borude is a student in the Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology Pimpri, Pune, India. Pursuing Bachelor Of Engineering degree in Computer Science.

Himalaya Wadhwani is a student in the Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology Pimpri, Pune, India. Pursuing Bachelor Of Engineering degree in Computer Science.