International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 5 ǁ 2021 ǁ PP. 01-05

Securing Data in IOT using Cryptography & Steganography Techniques

R. Sangeetha, G.Koteeswari M.Sc., M.Phil.,
PG Department of Computer Science, Kamban Arts & Science College for Women, Tiruvannamalai

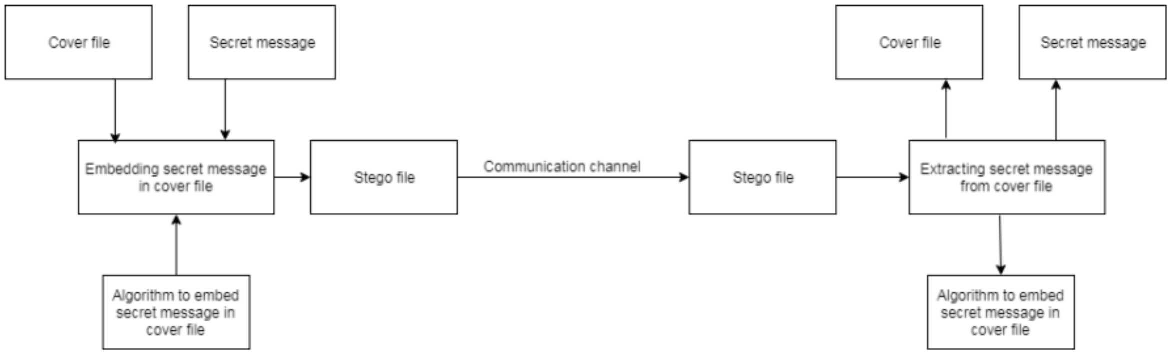
Abstract
Steganography is a technique of hiding every secret information like text, image, audio behind original cover file. Video Steganography is to hide the existence of the message from unauthorized party using Video as cover file and hiding information in video. Steganography is a type of cryptography in which the secret message is hidden in a digital picture but here in this project video steganography is applied on video which is transfer from sender side to receiver side. Steganography means covered writing it includes process of concealing information within other file and also conceals the fact that a secret message is being sent. In this project a technique proposed is Hash based least significant bit technique for video steganography. Least Significant Bit insertion method embeds data in the lower bits of RGB pixel of video and this changes will be minimal. Data hiding is the process of embedding information in a video without changing its perceptual quality and also keep away from knowledge of existence of message. A hash function is used to select the position of insertion in LSB bits. Besides this, anyone can modify and misuse the valuable information through hacking at the time. Nowadays, the use of a video based steganography is common and numbers of steganalysis tools are available to check whether the video is stegovideo or not.

Keywords: *LSB, DCT, Frequency Domain Analysis*

Date of Submission: 27-04-2021 Date of acceptance: 11-05-2021

I. INTRODUCTION

Steganography is a process that involves hiding important information or message inside other carrier data to protect the message from unauthorized users. The mixed data also called as stego objects will be seen by the Human Visual System (HVS) as one piece of data because the HVS will not be able to recognize the small change that occurs in the cover data. Message and cover data can be any data format such as text, audio, image, and video. As shown in figure 1, the basic steganographic system has different components like cover media, message and the main component which is the algorithm. Any successful steganography system should consider three main important factors: embedding capacity, imperceptibility, and robustness against attacks. First, the embedding payload is defined as the amount of secret information that is going to be embedded inside the cover data. The algorithm has a high embedding payload if it has a large capacity for the secret message. The embedding efficiency includes the stego visual quality, security, and robustness against attackers. Second, both a low modification rate and good quality of the cover data lead to a high embedding efficiency. The steganography algorithm that contains a high embedding efficiency will reduce attacker suspicion of finding hidden data and will be quite difficult to detect through steganalysis tools. However, any distortion to the cover data after the embedding process occurs will increase the attention of attackers . The embedding efficiency is directly affected by the security of the steganographic scheme. Increasing the capacity of the secret message will decrease the quality of stego videos that then weakens the embedding efficiency. Both factors should be considered


Cover file
Secret message
Embedding secret message in cover file
Stego file
Communication channel
Stego file
Extracting secret message from cover file
Cover file
Secret message
Algorithm to embed secret message in cover file
Algorithm to embed secret message in cover file

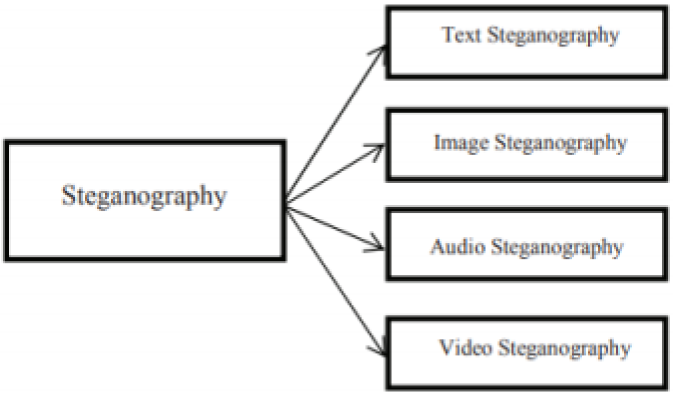
Basic stenography

Background

Cryptography and steganography are well known and widely used techniques that are basically used for manipulation of information in order to cipher or hide their existence respectively Steganography is a method which allows people to communicate and hide the existence of communication. Cryptography scrambles a message so it cannot be understood, in other words, cryptography is a method of transforming data so that only those for whom it is intended can read and process it. Even though both methods provide security, a study is made to combine both cryptography and steganography methods into one system for better confidentiality and security.

General Specification of Steganography

- Hidden Data : The data that is to be embedded or the data that must remain hidden from everyone other than intended receiver.
- Cover Media : The media in which the information is to be embedded. Cover/carrier media can be an image file, or an audio file or it can be a video file.
- Stego Media: Cover media containing the hidden information



Classification of stegnography

Steganography is the science of invisible communication. This transfer of information takes place by hiding data inside media. As shown in the figure, various steganographic techniques can be categorized into four main components. they are as follows

Image Steganography : We use an image file as a cover medium to hide the secret message. A digital image is a combination of low and high frequency contents. A low frequency region is strongly related with its neighboring pixels whereas a high frequency region strongly deviates from its neighboring pixels. By taking the advantage of human vision sensitivity the secret message is embedded within the image pixels depending on different transform techniques to hide the data in an image. Recently, a few machine learning techniques are also being used to increase the robustness, embedding capacity etc

Audio Steganography : It is a technique used to transmit a hidden message within an audio file. Embedding message in an audio file is much more difficult than hiding message in an image file as the human auditory system HAS) is more sensitive than human visual system (HVS). As the message is embedded in audio signals, there are various methods used for embedding process in an audio file like LSB coding, parity coding and echo data hiding

Text Steganography : It deals changing with format of an existing text within a file, changing the words within the text or generating random character sequences. Basically here we use the text file as a cover media to embed the secret information. It is more vulnerable for attack as it can be easy for an attacker to detect the pattern.

Video Steganography : A video file is used as a cover medium to hide the secret message. It is less prone for steganalysis as a video file is a combination of text, image and audio. It is a collection of certain frames running at some constant speed and is measured in frame per second. In order to embed a secret message in a video file first, we have to extract the frames from it. In order to embed the message in video file first, Frame conversion is done. It is a process of converting a video to consequent images or frames and then each or one frame is used as carrier data to conceal the hidden information. After the embedding process, all frames are merged together to produce the stego video.

EXISTING SYSTEM:

Nowadays, several methods are used for communicating secret messages for defense purposes or in order to ensure the privacy of communication between two parties. So we go for hiding information in ways that prevent its detection. Some of the methods used for privacy communication are the use of invisible links, covert channels are some of existing systems that are used to convey the messages.

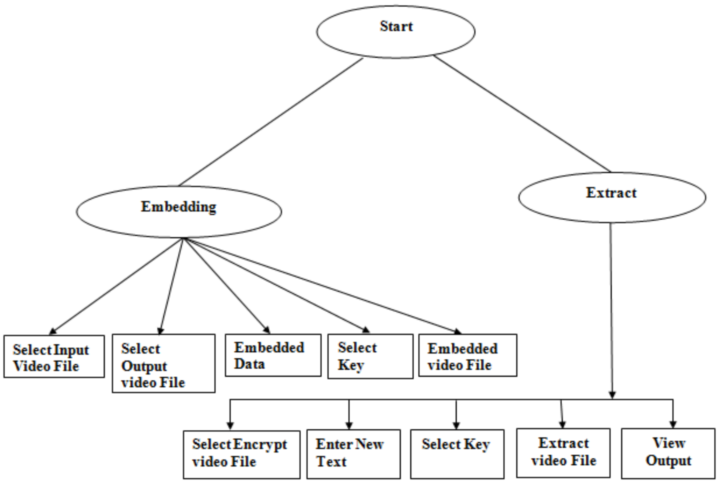
Currently, the emphasis has been on various forms of digital steganography. Commonly there are a number of digital technologies that the community is concerned with, namely text files, still images, movie images and audio. The majority of other organizations using steganographic techniques involve individuals or corporations interested in protecting intellectual property.

PROPOSED SYSTEM:

The proposed system uses video file as a carrier medium which add another step in security. The objective of the newly proposed system is to create a system that makes it very difficult for an opponent to detect the existence of a secret message by encoding it in the carrier medium as a function of some secret key and that remains as the advantage of this system

Steganographic techniques have obvious uses, some legitimate and some less so. The business case for protection of property, real and intellectual is strong. Individuals or organizations may decide to place personal, private or sensitive information in steganographic carriers. With advances in steganography, it is possible that this medium could serve as a relatively secure storage and transmission method. Steganographic techniques can also be used in the application of digital watermarks. Using a variety of techniques, images, music, movies can be imprinted with digital watermarks

System Design



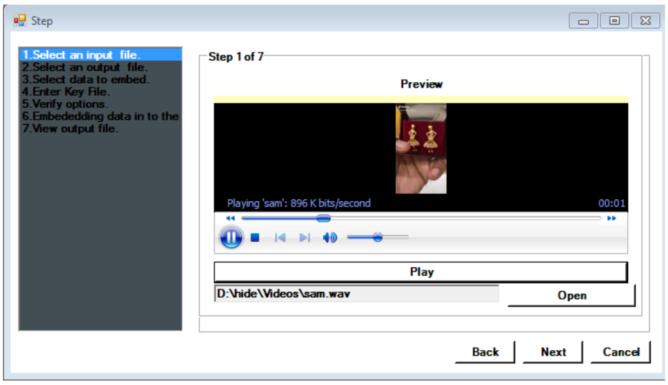
Implementation

Message Hiding:

Give original content as input with watermak data embedding. view flipping an edge pixel in text and file as shifting the edge location one pixel horizontally and vertically and can hide the message into the image. Data/text/message can be hide in pixels of video

Image/video/audio Hiding:

In video hiding user wants to hide the video or data file in the video or image. Then user have to select a particular image and video to hide the image. In this application we can also provide a dual security by using authentication verification. The general process of Steganography is that a data message is embedded within a cover signal. The output of the embedder is called a stego signal. After transmission, recording and other signal processing which may contaminate and distort the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor. The carrier of steganography can be an image, text, audio or a video file. Most of the steganography systems are developed in order to embed a text file, image or an audio file in a carrier file. Only a few algorithms are developed to embed a video file in a video file. This research is mainly carried out in order to embed a video in a video.



1.Select an input file.
2.Select an output file.
3.Select data to embed.
4.Enter Key File.
5.Verify options.
6.Embededding data in to the
7.View output file.

Step 1 of 7

Playing 'sam': 896 K bits/second 00:01

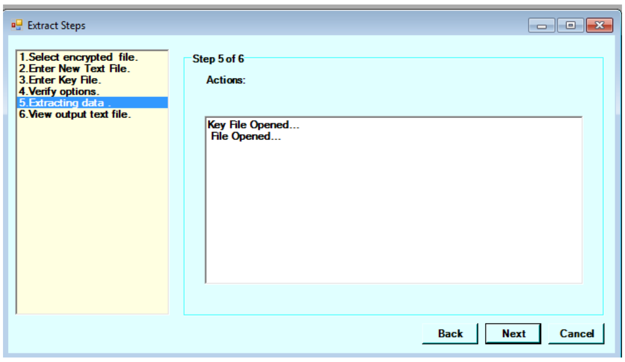
D:\hide\Videos\sam.wav

Embed Module (To embed the text file into the video file)

In this module, the first step is selecting an input video file . The selection is made through opening a new dialog box and the path selected is displayed through a textbox. The second step is selecting an output audio file in which text data or a text file is embedded. The third step is choosing a text file or typing any text message for embedding. Fourth step is selecting a key file. In the fifth step what ever the files that we have selected are viewed and verification of the path is done. In the sixth process data is embedded in to the video file using low bit encoding technique.

Extract Module (To extract the text file from the video file)

In this module, the first step is the process of selecting the encrypted video file. This is the file that a user has to extract information from the output video. Second process involved in selecting a new text file to display the embedded meassage. Symmetric encryption method is used here, so the key selected during the embedding process is used in decrypting the message. All the process done till now are displayed using a list box and finally the embedded message can be viewed with the help of a file or in a textbox



1.Select encrypted file.
2.Enter New Text File.
3.Enter Key File.
4.Verify options.
5.Extracting data .
6.View output text file.

Step 5 of 6

Actions:

Key File Opened...
File Opened...

II. CONCLUSION

Video steganography allows two individuals to communicate privately. The proposed technique can be used to securely send sensitive information without worrying about man-in-the-middle attack. Use of clustering technique in steganography provides greater security as it is harder for the attacker to find the pixels which are encrypted. Moreover, the encrypted pixels are hidden in the clusters which diminishes the probability of the message being found. Hiding information may introduce enough visible noise to raise suspicion. Therefore the carrier or cover audio must be carefully selected. This proposed system is to provide a good, efficient method for securing the data from hacker and sent to the destination in a safe manner. Embedding picture and text behind video and audio file and then combine into stego file at sender side and thereafter face authentication technique is carried out at receiver side to cross check the security parameter by authorizing the recipient hence ,the data is significantly secured. The secret text information is archive in video successfully moreover interpret the audio file and focused to extract secret text.

REFERENCES

[1]. MazharTayel, Ahmed Gamal, HamedShawky, "A Proposed Implementation Method of an Audio Steganography Technique", ICACT2016,

[2]. YugeshwariKakde, Priyanka Gonnade, Prashant Dahiwale , "AudioVideo Steganography", ICIIECS'15

[3]. Juanita Blue, Joan Condell, Tom Lunney," Identity Document Authentication using Steganographic Techniques",Signal and System Conference (ISSC) -21 June 2019.

[4]. Ankit Gambhir, SibaramKhara," Integrating RSA Cryptography & Audio Steganography",International Conference on Computing, Communication and Automation(ICCCA), Conference on 29-April2020.

[5]. Ratul Chowdhury, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Tai-hoon Kim," A View on LSB Based Audio Steganography", International Journal of Security and Its Applications, Vol. 10, No. 2

[6]. V. Santhi and LogeswariGovindaraju," Stego-audio Using Genetic Algorithm Approach", Research Journal of Applied Sciences, Engineering and Technology,

[7]. Prashant Johri, Arun Kumar, Amba," Review Paper On Text And Audio Steganography Using GA" International Conference on Computing, Communication and Automation,

[8]. Krishna Bhowal, "Audio Steganography using GA" 2019 International Conference on Computational Intelligence and Communication Networks.

[9]. Firoz Mahmud, Md. EnamulHaque, Syed TauhidZuhori, Biprodip," Human Face Recognition using PCA based on Genetic algorithm", Electrical Engineering and Information & Communication Technology (ICEEICT), IEEE.