International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 07, July 2017
ISSN: 2455-3778
http://www.ijmtst.com

An Optimized Image with Digital Multimedia Files Hiding Audio, Video by Using DES Algorithm

N. Gayathri[1] | Dr.A.Nagarajan[2]

[1]M. Phil scholar in Department of computer application, Alagappa university, Karaikudi, Tamilnadu, India.
[2]Assistant Professor in Department of computer application, Alagappa university, Karaikudi, Tamilnadu, India.

To Cite this Article
N. Gayathri and Dr.A.Nagarajan, "An Optimized Image with Digital Multimedia Files Hiding Audio, Video by Using DES Algorithm", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 07, July2017, pp.-355-360.

ABSTRACT

Steganography is the process of hiding information for the purpose of communication in sender to receiver. All kinds of stegano files are send, such as audio, video, text. Security of data can be achieved by implementing steganography techniques. All of the existing steganography techniques use the digital multimedia files as a cover medium to conceal secret data. Audio and video file use as a cover medium in steganography because of its larger size compare to other carrier's file such as text, image. So there are more possibilities to hide large amount of data inside digital audio, video file. Signals Various file formats are can be used, but digital images are popular because it is frequency on the internet. It also supports steganography in audio files. Intruders are easily hack the information because it is not encrypted, so we propose the hiding secret information in images and audio to sender and receiver, it is the steganography hiding secret information in image, it is the process to encrypt the message using secret key and then sends it to the receiver. The receiver then decrypts the message to get the original one. Hiding the text message in an image file, video and audio WAV file. Encryption of the same message, so as to support more secure steganography. The decoding of the message, decryption and source message retrieval are also supported.so, this steganography techniques are user friendly.

Keywords: *Digital Audio Steganography shared data, user revocation, video files, cloud computing.*

I. INTRODUCTION

Data is important to any organization. They must be protected from the unauthorized access. Data should only visible to the sender and receiver of transmitted data, and they should be hidden from hackers. Hiding data is nothing more than protecting the data in some medium or encrypting the data. There are many techniques that use the concept of hiding data; cryptography and steganography are among them. Steganography and cryptography are closed related, with the main difference being their goals. Cryptography encrypts the data, which makes it unreadable, but the encrypted data cannot be hidden from unauthorized users as presence of hidden data is known. In contrast, steganography prohibits unauthorized users from even having any knowledge of the existence of the hidden data. Steganography is the art or practice of hiding a message, audio, video, image, or file within any of these formats. The word "steganography" is from Greek and means "covered writing." In this paper, we focus on hiding text in images files.

Steganography is necessary to hide data from unauthorized users, particularly in the following areas: Governments: There are many governments and investigative agencies that need to hide sensitive information when sending or receiving the data from their officers. Businesses: The competition among companies in the same field is growing daily. Each competitor wants to overcome its opponents by any means, so securing confidential data is very important. In this case, while sending or receiving the information, they use steganography. Individuals: Every individual has some private data to store, and they don't want anyone to view this information without permission, so the need for steganography arises when sending or receiving this information.

II. MODELS OF STEGANOFILES

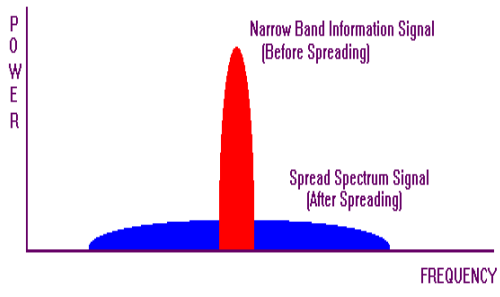
2.1: Audio File Format:

- Uncompressed File:
  - WAV
  - AIEF
- Compressed File:
  - Lossy
    Mp3, AAC, WMA
  - Lossless
    ALAC, FlAC, WavPack
  -

III. TECHNIQUES OF DIGITAL MEDIA FILES

- Low – bit encoding
- Spread spectrum
- Echo data hiding
- Perceptual masking
- MP3 Stego-A form of Radio Frequency Communication
- Data sent is spread over a wide frequency range. Adds random noise to the signal using a noise generator.

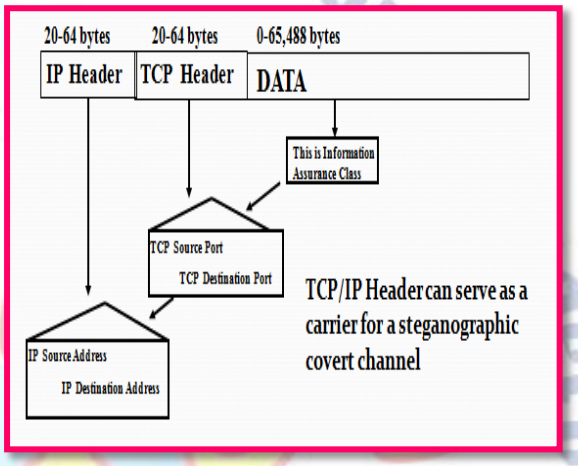
Video steganography is a technique to hide any kind of files into a carrying media



Information is hidden in each frame of the video.Large amount of data can be hidden and the fact that it is a moving stream of images and sounds.Any small and noticeable distortion might go unobserved because of the continuous flow of information.

Steganography in video uses Discrete Cosine Transformation Discrete Cosine Transform (DCT) – Effective way to hide secret data.

Image compression will destroy the integrity of the hidden message Communication in a non-obvious manner. There areTwo types:



Storage : information conveyed by writing or abstaining from writing, Clock not needed.

Timing : information conveyed by the timing of events, receiver need the clock Confidential communication and secret data storing.

Protection of data alteration. Access control system for digital content distribution. Media Database systems.

3.1: Fields of application

- Defence and intelligence
- Medical
- On-line banking
- On-line transaction
- To stop music piracy
- Other financial and commercial purpose

IV. IMPLEMENTATION

Implementation is the stage of the research when the theoretical design is turned out into a working system. Thus, it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new

system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. it is efficiency of the security for data to be send to receiver in original file of the encryption modification, data can be encrypted among the dynamic process and it is secure and vulnerable. It is the heart of DES.DCT – quantization on the least important part of the image in respect to the human visual capabilities It is a Lossy compression. It Will not impact on the integrity of the secret image.

V. ALGORITHM USED IN STEGANO FILES

Data Encryption Standard (DES) using 64-bit block size of plaintext & 56 bits of Secrete key. It changes the intensity of the pixels so the safety of the encryption scheme is improved. There is a scope for improvement as there are several new and strong encryption methods have been proposed. Gray Image Encryption Scheme by Discrete Logarithm with Logistic and HEH64 Chaotic Functions It is useful for the huge dark level Pictures. It holds better results in crypto examination assault, and brute force attack. There is a scope of minimization of Information loss. Encryption method based on transformation of a text file into an image file on both client and server machines. It is moreover profitable for text data through regardless of all around messages put away in the form of divided pictures and in this way regardless of the fact that somebody leaves the email page on it is troublesome for others to figure the significance (the first content) of these pictures. How to Set the felicity into blocks and now affect each block into an image and thus create individual key for each block is not determined.

VI. EXISTING SYSTEM

Steganography hide the secrete message in the format of image, in these formats large amount of data using process may be collision occur in the decryption file, within the host data set and presence imperceptible and is to be unreliably communicated to a receiver. The hostdata set is purposely corrupted, but in a covert way, it is corrupted by using encryption process to an information analysis.

6.1: Disadvantages of existing system:

- Sender used limited amount of communication and damaged file while process in large amount of data to be send resources, Shared data will not be secure.
- Unexpected collusions destroyed the data.
- Less amount of space to be used.

VII. PROPOSED SYSTEM

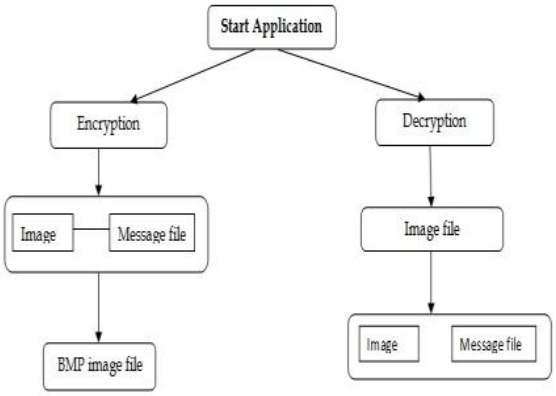
In proposed system collusion of shared data to destroy the decryption process to avoid in the collusion by using DES (data encryption standard) algorithm, large amount of data to be frequently process to encryption in this overloaded error process to rectify the DES algorithm reputation of its data services and avoid losing money of its data services. It's no collusion to be occurring in this task large number of users to share data in performance to sender to receiver, receiver get the original from the sender. We can send the any kind of digital media files (text, audio, video)

7.1: Advantages of proposed system

- It is large amount of space.
- It is no collision to be occurred.
- It is secure process, data to be communicated in secure manner.
- Large number of task to simultaneously and efficiently.
- we can send the any kind of digital media files (text, audio, video)

VIII. SYSTEM ARCHITECTURE

- Cover - Original picture, audio of video file
- Emb - Embedded secret message
- f_E -Embedding function
- f_E-1 - Extracting function
- Key - Parameter which controls the hiding process of the secret message
- Stego - Resultant file that contains secret message



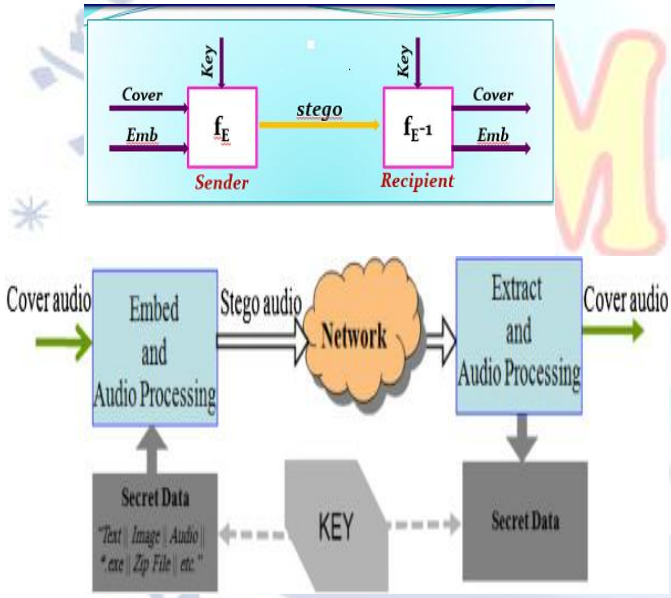
8.1. *Characteristics of steganofiles:*

- Unknown message passing
- Prevents discovery of the existence of communication
- Little known technology
- Technology still being develop for certain formats
- Once detected message is known
- Does not alter the structure of the secret message

8.2. *Audio file formet:*

Digital Steganography is based on artifacts like bitmaps and audio files (Redundant information JPEG & MP3 – Lossy compression techniques which eliminate the redundancyEmbedding secret message into digital sound.

The properties of Human Auditory System (HAS) are exploited in the process of audio steganography



Spatial domain: Pixel value directly modified for data hiding Apply Least Significant Bit (LSB) insertion and noise manipulation

Transform domain: Process the image based on the frequency Discrete Cosine Transformation (DCT) & Discrete Wavelet Transformation (DWT)

Cloud data storage block

Authorized person get the space from the cloud and stored data in this cloud it is secure and easy to get from this cloud.it is stored large number of data and may not be collusion. users and requestors retrieve and upload from the separate cloud storage.

Signatures block

Signature block it is unique from each user, asymmetric group key agreement (AGKA) it is highly secured in this task then the performance is high.it is the process of resigned and revocation users.

Cloud interface

Cloud interface it is intermediate to cloud data storage block, access members, and resigning request.

Resigning request

Allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves.

Access members

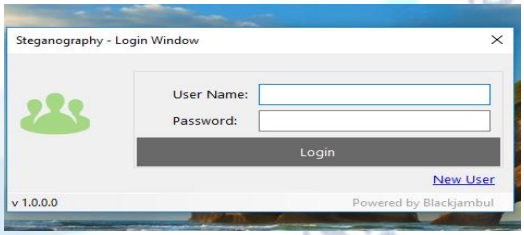
Third party auditor, group managers and group members those are allocated by cloud storage and intermediate to each other. It is the process reviews to be stored in database.

IX. MODULES

- Login page
- Registration page
- Encryption process
- Decryption process

9.1Login page

We can login the user name and password.it must be the predefined data. We can give the correct the user name and password.



9.2Registration page

The registration page can most important in the research of the stegano files.

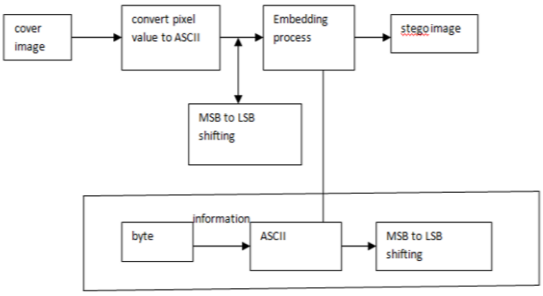


Figure:1. encryption process

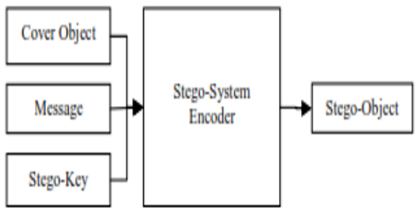
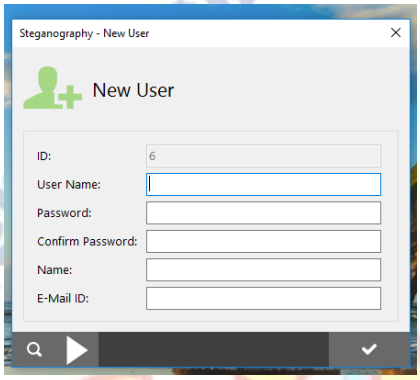


Diagram of a typical Steganography System.

Fig; Model of the file

The new user can create username and password.it must be unique. We can must fill the all the columns.



9.3Encryption process

Encryption the secret information is hiding in with any type of image file.

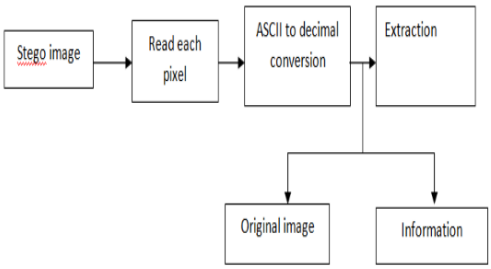
Sender securely sends data by using encryption process.

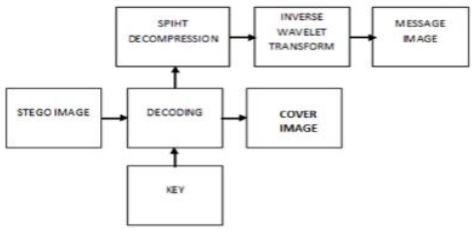
In the past decade, a number of data-hiding schemes have been proposed in literature, however, the majority of them deals only with digital image, audio or video documents. With the proliferation of digital media. Each 64 bits of data is iterated on from 1 to 16 times (16 is the DES standard). For each iteration, a 48-bit subset of the 56 bit key is fed into the encryption block represented by the dashed rectangle above. Decryption is the inverse of the encryption process.

Types of Steganography Attacks	Description
Steganography-only attack	Only the steganography module is available for analysis
Known-message attack	Hidden message is known.
Known-carrier attack	Original cover and steganography media are both available for analysis.
Known-steganography attack	Carrier and steganography medium or algorithm are known
Chosen-message attack	Used to create steganography media for future analysis and comparison to determine corresponding patterns in steganography medium (use of specific steganography tools or algorithm).
Chosen-steganography attack	Steganography medium and tool(or algorithm)are both known

Decryption process

Decryption is getting the secret information from image file.Steganography can be used for hiding information. We used the LSB technique to provide a means of secure communication. A stage-key has been applied to the system during embedment of the message into the cover image. This steganography application software is provided for the purpose to hide any type of files in the host file. The application supports any file format of an image, without converting it to any other format. Since ancient times, man has found a desire in the ability to communicate covertly. The recent research in watermarking is evidence that, beside military use or espionage application, steganography can be used in other areas where hiding of data or information security is required.





The sender encrypts the data using a password and hides it behind the image and then the image is encrypted using the same password and sent to the receiver. If the receiver is authorized then he will authenticate through the login process and the decrypt the image and the data respectively using the same password. This provides high level of security y to the user.

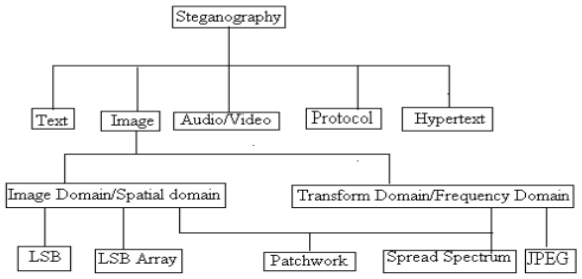


Figure: Classification of steganography

X. CONCLUSION

The research was completed successfully to build a tool called Hiding in Plain Sight. This tool can be used for hiding the text message in the image or the audio files. Also, the message that is sent can be encrypted, so as to support secure steganography. Regardless, the technology called steganography is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game.

REFERRENCE

[1] Petitcolas, F.A.P., Anderson, R., Kuhn, M.G., "Information Hiding - A Survey", July2014, URL:http://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf (11/26/0117:00).

[2] An archive of steganography and Steganalysis tools: URL:http://members.tripod.com/steganography/stego/software.html (11/26/01 17:00).

[3] Katzenbeisser, S., Petitcolas, F.A.P., Information Hiding Techniques for Steganography and Digital Watermarking, Norwood: Artech House, 2015, pg. 56 – 92.

[4] Johnson, N.F., Jajodia, S., "Steganalysis of images created using current Steganographic tools", April 2015, URL: http://www.ise.gmu.edu/~njohnson/ihws98/jjgmu.html (11/26/01 17:00).

[5] Provos, N., Honeyman, P., "Detecting Steganographic Content on the Internet", August 2016,http://www.citi.umich.edu/techreports/reports/citi_tr_01-11.pdf (11/26/01 17:00).