INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

STEGANOGRAPHY TECHNIQUES FOR HIDING SECRET INFORMATION

[1]Mrs G. SWETHA, [2]KATIKA VENKATESH YADAV, [3]MOGULLA SIDDHU, [4]THOKALA VISHNUVARDHAN

[1]Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

Swethareddy630@gmail.com

[2,3,4]BTech Student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad

Venkateshyadav563@gmail.com, ssid32671@gmail.com, thokalavishnu8790@gmail.com

Abstract: *Steganography is a technique for hiding data behind the file such as image, audio, video etc. and that data securely transfer from sender to receiver. It serves as a better way of securing message than cryptography which only conceals the content of the message not the continuation of the message. Original message is being hidden within a file such that the changes so occurred in the file are not noticeable. To hide the secret information verity of steganography techniques can be used and are more complex than others while all of them have respective strong and weak points. The absolute invisibility of the secret information is maintained by different applications, while others require a large secret message to be hidden. This paper discusses an overview of image steganography, its uses and techniques to satisfy the need for privacy on the internet. Various steganography techniques to provide privacy while transferring data from source to destination.*

Keywords: *steganography, cryptography, secret information, digital image.*

I. INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered. Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images. Project Report Submitted by Rahul Kumar Singh, Reg No-1201210132 5 The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requiring to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

II. LITERATURE SURVEY

A new steganography algorithm based on color histograms for data embedding into raw video streams Steganography, embedding secret data into unsuspected objects, has emerged as a significant sub-discipline of data-embedding methods. While mostly applied to still images in the past, it has become very popular for video streams recently. When steganographic methods are applied to digital video streams, the selection of target pixels, which are used to store the secret data, is especially crucial for an effective and successful-embedding process; if pixels are not selected carefully, undesired spatial and temporal perception problems occur in the stego-video. In this paper, two new steganographic algorithms are proposed utilizing similar histograms and dissimilar histograms. Both algorithms are based on selecting appropriate pixel approaches by focusing on perceptibility and capacity parameters of the cover video. When compared to traditional steganographic techniques, they not only result in improved temporal and spatial perception levels in the stego-video but also offer a relatively high dataembedding capacity.

In this paper, we present a novel data-embedding system with high embedding capacity. The embedding algorithm is based on the quantized projection embedding method with some enhancement to achieve high embedding rates. In particular, our system uses a random permutation of the columns of a Hadamard matrix as projection vectors and a fixed perceptual mask based on the JPEG default quantization table for the quantization step design. As a result, the data-embedding system achieves 1/167 (1 bit out of 167 raw image bits) to 1/84 hiding ratios with a BER of around 0.1% in the presence of JPEG compression attacks, while maintaining visual distortion at a minimum.

With the rapid advance in digital network, digital libraries, and particularly WWW (World Wide Web) services, we can retrieve many kinds of information anytime. Thus, security has become one of the most significant problems for distributing new information. It is necessary to protect this information while communicated over insecure channels. Thus a need for developing technology that will help to provide security as well as authenticity. Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. Steganography and cryptography are similar in the way that they both are used to protect important information. Nowadays the term "Information Hiding" relates to both watermarking and steganography. So we proposed combined strategy of cryptography, steganography and digital watermarking to hide secure image with watermark logo inside cover image. For this purpose we use

DCT, DWT, SVD and RSA approach. Using DCT, encrypted watermark logo (encryption perform using RSA) is hide inside Secure image, results in Stego image. This Stego image is hiding inside cover image using DWT and SVD. Our approach can be used to transmit secure information like copyright information of company, movie with their respective image, finger-print or thumb impression of particular person. This method can be used for security purpose. Thus would be beneficial to nation for over all security.

To ensure reliability and integrity in information transmission, image steganography is cutting edge technology in today's digital world. It can be implemented in spatial, time and frequency domain. In this research article, an effective algorithm has been introduced which would embed secret message data, scrambled by Arnold Transform, in frequency domain using the quantization coefficient modification in Discrete Cosine Transform (DCT). At first the cover image is split into blocks, then two dimensional DCT is applied on each image block and transformed secret message is inserted by analyzing mid-band coefficients of DCT.

Steganography is one of the methods of secret communication that hides the existence of message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. It is the process of embedding secret data in the cover image without significant changes to the cover image. A cryptography algorithm is used to convert the secret messages to an unreadable form before embedding. These algorithms keep the messages from stealing, destroying from unintended users on the internet and hence provide security. Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So the propose technique use a combination of steganography and cryptography for improving the security. The proposed technique use Discrete Cosine Transform (DCT) and Blowfish algorithm. The proposed method calculates LSB of each DC coefficient and replace with each bit of secret message. The proposed embedding method using DCT with LSB obtained better PSNR values. Blowfish algorithm is used for encryption and decryption of text message using a secret-key block cipher. This technique makes sure that the message has been encrypted before hiding it into a cover image. Blowfish is an improvement over DES, 3DES, etc designed to increase security and to improve performance

Steganography is the method of hiding information in a multimedia carrier. The carrier(cover) can be an image, audio or video. In this case image is taken as the carrier and the hidden information or secret information. So here dealing with image steganography. Gray level image is taken as both cover and secret images. This paper implements the steganography in frequency domain. A DCT transformation technique is used to convert the cover image from spatial to frequency domain.

III. PROPOSED SYSTEM

In this project data is secured by hiding information in text, video, audio and image for text we will use ZWCs for image we will use dct or for audio modified lsb for video steganography with rc4 encryption with key scheduling algorithm Pseudo random generation Algorithm

Advantages

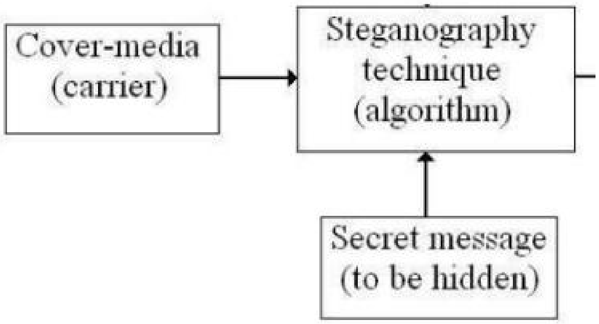
• The advantage of steganography is that messages do not send consideration to themselves. Clearly detectable encrypted message no matter how tough will stimulate suspicion, and may in themselves be compromising in countries where encryption is illegitimate.

• In steganography, cryptography secures the contents of a message, steganography can be said to secure both messages and connecting parties.

• This approach featured security, capacity, and robustness, the three needed element of steganography that creates it beneficial in hidden exchange of data through text files and creating secret communication.

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system. Organized in a way that supports reasoning about the structures and behaviors of the system.


Cover-media (carrier)
Steganography technique (algorithm)
Secret message (to be hidden)

System Design Introduction:

The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

MODULES

USERMODULE:

Using this module user will register with application and store data in database and upload text, audio, video and image with data to hide in the web page and apply encoding and then upload encoded data to redrive data from image.

TEXT ENCRYPTION MODULE:

Using this module user will upload sample text file with data to hide inside it and encode using ZWCs-ZWCs- algorithm and hide data in text. Encoded text is uploaded to website to see encoded text.

IMAGE ENCRYPTION:

Using this module user will upload sample image file with data to hide inside it and encode using DCT DWT- algorithm and hide data in IMAGE. Encoded IMAGE is uploaded to website to see HIDDEN text.

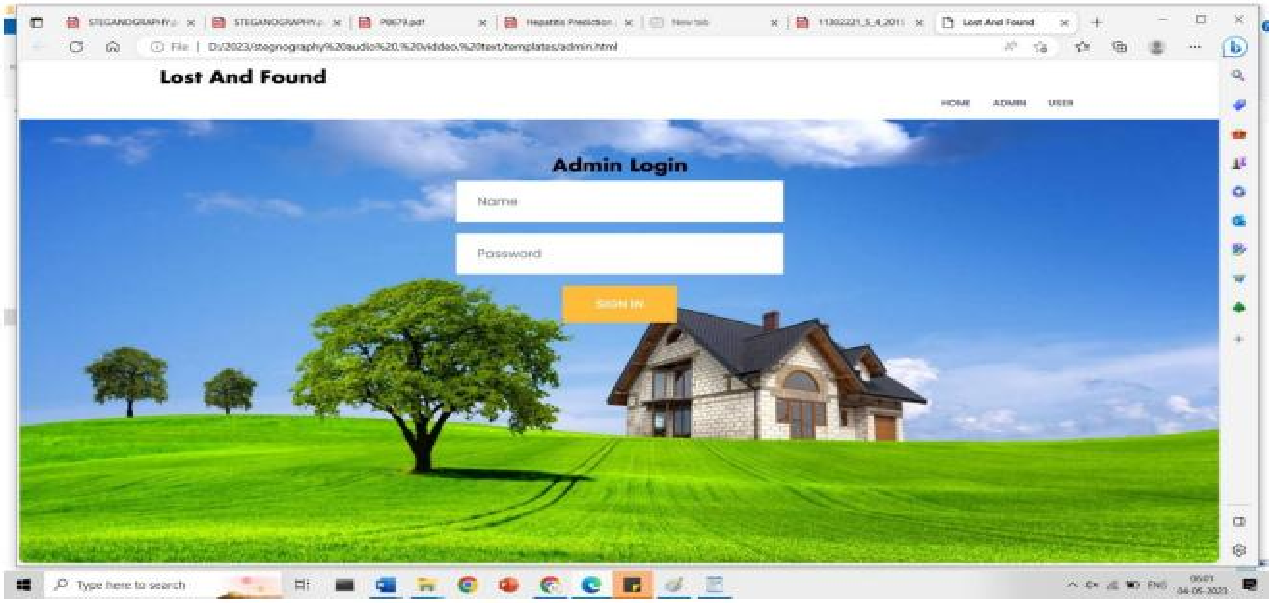
AUDIO ENCRYPTION:

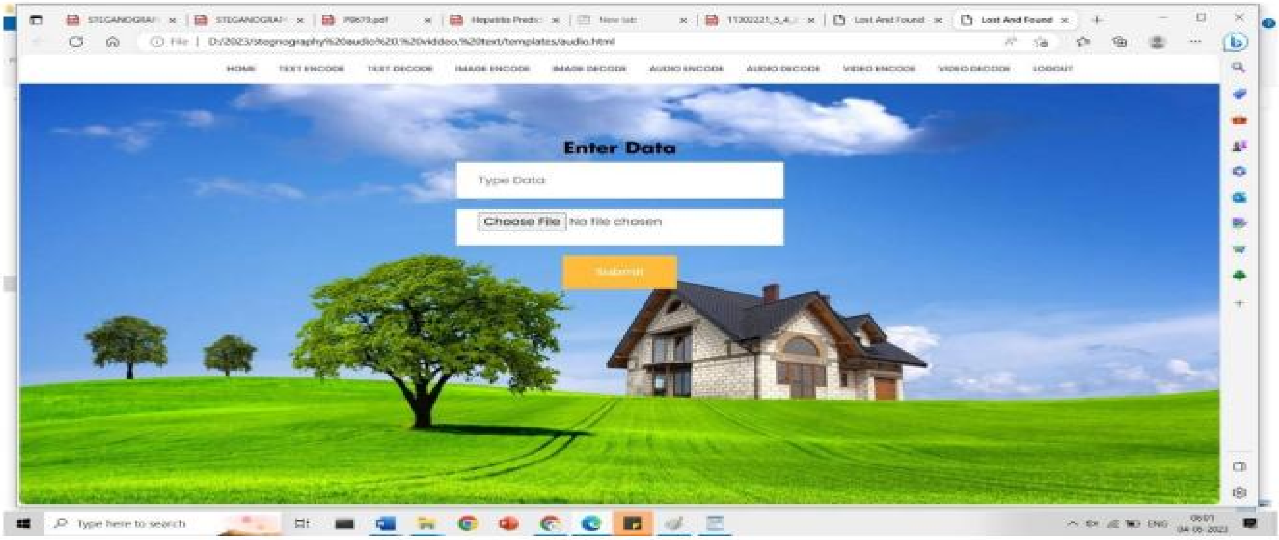
Using this module user will upload sample audio file with data to hide inside it and encode using LSB- algorithm and hide data in audio. Encoded audio is uploaded to website to see hidden text

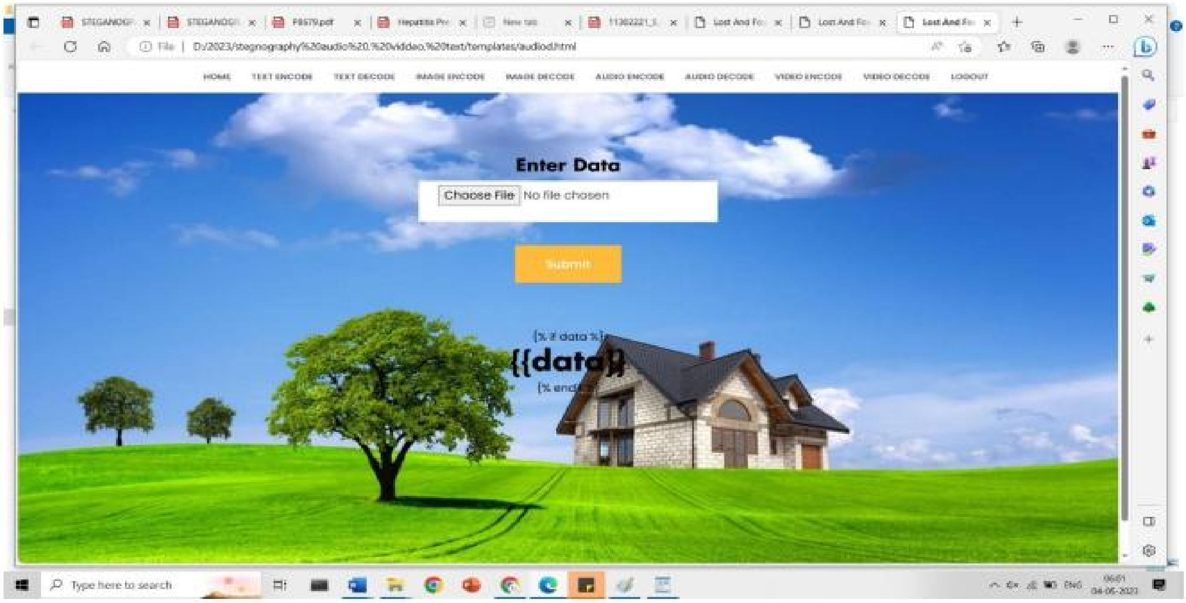
VIDEO ENCRYPTION:

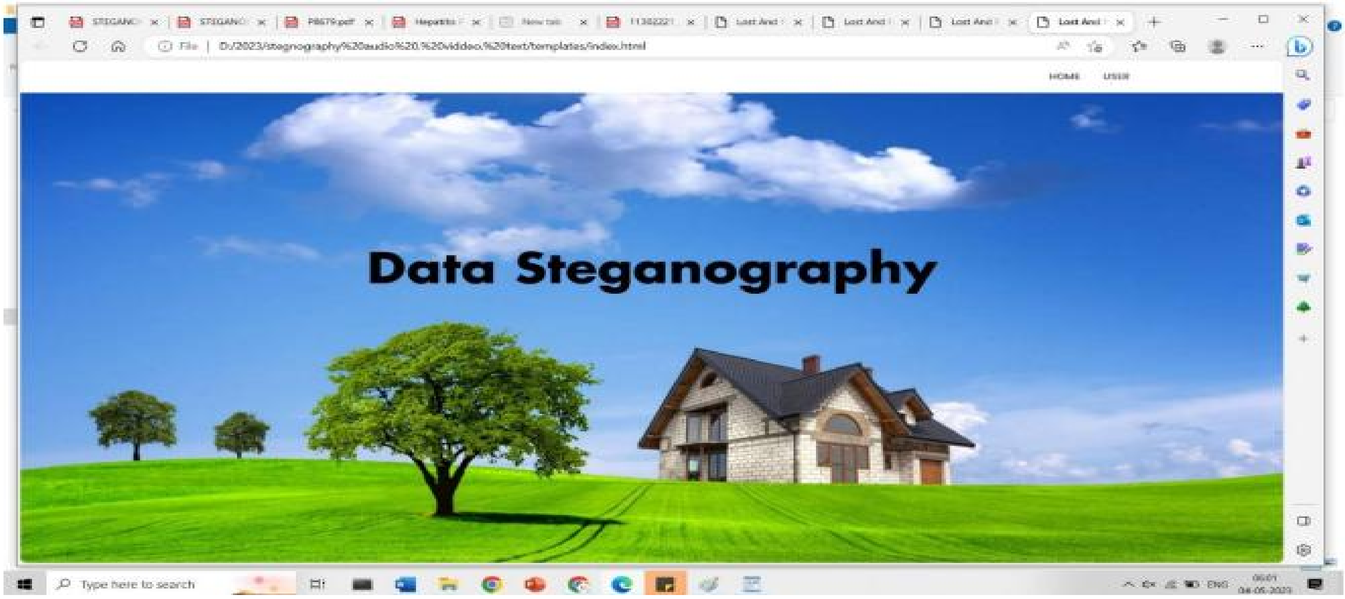
Using this module user will upload video file with data to hide inside it and encode using rc4 encryption- algorithm and hide data in video. Encoded video is uploaded to website to see hidden text

IV. RESULTS


D:/2023/stegnography%20audio%20,%20viddeo,%20text/templates/admin.html
Lost And Found
HOME
ADMIN
USER
Admin Login
Name
Password
SIGN IN
Type here to search


D:/2023/stegnography%20audio%20,%20viddeo,%20text/templates/audio.html
HOME
TEXT ENCODE
TEXT DECODE
IMAGE ENCODE
IMAGE DECODE
AUDIO ENCODE
AUDIO DECODE
VIDEO ENCODE
VIDEO DECODE
LOGOUT
Enter Data
Type Data
Choose File No file chosen
Submit
Type here to search




D:/2023/stegnography%20audio%20,%20viddeo,%20text/templates/index.html
HOME
USER
Data Steganography
Type here to search

V. CONCLUSION

This project provides an overview of steganalysis and introduced some characteristics of steganographic software that point signs of information hiding. This work is but a fraction of the steganalysis approach. To date general detection techniques as applied to steganography have not been devised and methods beyond visual analysis are being explored. Too many images exist to be reviewed manually for hidden messages so development of a tool to automate the process will be beneficial to analysts. The ease in use and abundant availability of steganography tools has law enforcement concerned in trafficking of illicit material via web page images, audio, and other transmissions over the Internet. Methods of message detection and understanding the thresholds of current technology are under investigation. Success in steganographic secrecy results from selecting the proper mechanisms.

REFERENCES

[1] Mental Disorder Detection : Bipolar Disorder Scrutinization using Machine Learning, published in 2019.

[2] Intelligent data mining and machine learning for mental health diagnosis using genetic algorithmAzar, Ghassan &Gloster, Clay & ElBathy, Naser & Yu, Su&Neela, Rajasree&Alothman, Israa. (2015). Intelligent data mining and machine learning for mental health diagnosis using genetic algorithm. 201-206. 10.1109/EIT.2015.7293425

[3] A Framework for Classifying Online Mental Health-Related Communities With an Interest in Depression B. Saha, T. Nguyen, D. Phung and S. Venkatesh, "A Framework for Classifying Online Mental Health-Related Communities With an Interest in Depression," in IEEE Journal of Biomedical and Health Informatics, vol. 20, no. 4, pp. 1008- 1015, July 2016.

[4] Detecting Cognitive Distortions Through Machine Learning Text AnalyticsT. Simms, C. Ramstedt, M. Rich, M. Richards, T. Martinez and C. Giraud-Carrier, "Detecting Cognitive Distortions Through Machine Learning Text Analytics," 2017 IEEE International Conference on Healthcare Informatics (ICHI), Park City, UT, 2017, pp. 508-512

[5] Prof. Prajkta Khaire, Rishikesh Suvarna, Ashraf Chaudhary, "Virtual Dietitian: An Android based Application to Provide Diet", International Research Journal of

Engineering and Technology (IRJET),Volume: 07 Issue: 01 | Jan 2020

[6] Shivani Singh, Sonal Bait, Jayashree Rathod, Prof. Nileema Pathak," Diabetes Prediction Using Random Forest Classifier And Intelligent Dietician " , International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 01 | Jan 2020

[7] Uday Chandrakant Patkar, Sushas Haribabu Patil and Prasad Peddi, "Translation of English to Ahirani Language", *International Research Journal of Engineering and Technology(IRJET)*, vol. 07, no. 06, June 2020.