International Journal of Computational and Electronics Aspects in Engineering
Volume 2, Issue 3, July 2021, pp 57 - 60
https://doi.org/10.26706/ijceae.2.3.20210604

Steganography Using Data Encryption

Gaurav Rao
gauravraojob@gmail.com

Raju Borkute
rajuborkute2000@gmail.com

Vishal Gahane
vishalgahane1998@gmail.com

Yogeshwar Nagpure
ynagpure1994@gmail.com

Student, Department of Computer Engineering, Smt. Radhikatai Pandav college of Engineering, Nagpur, India

***Abstract*— We introduce the concept of steganography, which is largely hiding a system inside a system. We introduce additives The payload system is the system to be hidden. The cowl box is the medium wherein the payload system is hidden. The cowl system is the system that extracts the payload system from the duvet box and executes the payload system as a subprocess. We advocate what an implementation can be like the usage of photograph steganography and eventually video steganography. The payload system is a fixed of instructions. The payload system is damaged into payload additives, elements of the payload system. Each payload element is hidden right into a body of the video. Upon gambling the video, the payload system is extracted and executed. In the system, we pass over software program libraries and document sorts attempted and used. Impediments with inside the implementations are encountered and proposals for destiny paintings are offered Steganography consists of the concealment of data inside pc documents in virtual steganography digital communications might also additionally encompass steganographic coding internal of a delivery layer, which includes a report document, photo document, program, or protocol. Media documents are perfect for steganographic transmission due to their huge size.**

***Keywords*—** Steganography encryption, Description, Video, Audio, Image, Text.

I. INTRODUCTION

Steganography comes from the Greek phrases stegan´os or “covered” and gr´aphein or “to write”. Today, the time period has been generalized to encompass any shape of hidden communication. Steganography commonly has components, a cowl and a payload. The cowl is a distraction that hides the lifestyles of the payload. The payload is the hidden facts this is stored mystery to outside events. Steganography is used to prevent detection of a mystery, something that ought to be acknowledged simplest to a pick out variety of individuals. On the alternative hand, cryptography is utilized in anticipation that presence of the mystery could be detected, however its facts content material stays mystery. The mystery may be intercepted and/or changed withinside the absence of cryptography. Steganography on my own is simplest correct till suspicion approximately the name of the game arises from a 0.33 party. Steganography and cryptography are complementary in enhancing statistics protection [1]. Ramadhan et. al. describe "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC." the techniques of data hiding like low bit rate data hiding in detail.

Research Article
First Online on – 10 July 2021

Cite this article – Gaurav Rao, Raju Borkute, Vishal Gahane, Yogeshwar Nagpure, “Steganography Using Data Encryption”, *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 2, issue 3, pp. 57-60, 2021.
https://doi.org/10.26706/ijceae.2.3.20210604

Chikouche and Chikouche, describe “An Enhanced Approach to LSB-Based Image Steganography Using the AESA Algorithm” This article explores the different methods of steganography such as LSB, Masking and Filtering and also explains about different software tools present in the market for Steganography, such as Stego Dos, White Noise Storm, S-tool etc [2].

It is proposed that "Advanced Encryption Standard" (Spread Spectrum Image Steganography) SSIS is a blind scheme where the original image is not needed to extract the hidden information unless the receiver possesses the secret key to extract the secret message, otherwise it is virtually undetectable. Thus making this technique reliable and secure [3].

Shumeet Baluja proposes "Hiding images to the naked eye: deep steganography" highly accurate steganalysis technique which can even estimate the length of secret message embedded in LSB method [4]. In this method, the test image is divided into groups of n consecutive or disjoint pixels. This method exploits the modified pixel values to determine the content of secret message. A discriminating function is applied on the group of pixels. This discriminating function determines the regularity or smoothness of pixels. Then a permutation function called flipping is applied on the pixel groups. By using discriminating function and flipping, Pixels groups are classified in to three categories, i.e. Regular groups, Singular groups and Unused Groups. For a given mask, fraction of Regular groups Rm and fraction of singular groups Sm are calculated. Presence of noise in the image causes Rm to be greater than Sm. Bhadarkar et. al. gives the analysis of various methods of LSB techniques for image [5].

II. Method And Material

A. *Proposed Methodology*

The predominant purpose of steganography, as with cryptography, is facts security. So glaringly it become huge packages with inside the discipline of facts security. It may be used to bring messages undetectably among parties. This may be achieved via way of means of the sender importing a photograph or a video on his website. The supposed receiver can then down load the photograph and extract message from it. Since steganography makes it feasible to embed greater facts into media files, it is able to be used for watermarking and copyright manipulate structures as well. The unique writer ought to embed his fingerprint on any document he owns [6-10].

1. AES Algorithm

The US Public Foundation of Principles and Innovation (NIST) introduced that it'd preserve a resistance to choose some other rectangular code to be called the High degree Encryption Standard, or AES to displace DES. The code takes a plaintext block length of 128 pieces, or sixteen bytes. The key duration may be sixteen, 24, or 32 bytes (128, 192, or 256 pieces). The calculation is implied as AES-128, AES-192, or AES-256, structured upon the important thing duration. The contribution to the encryption and unscrambling calculations is a lone 128-piece block.

2. LSB Algorithm

One easy and famous picture steganography set of rules is the least big bit (LSB) substitution set of rules. It works simplest on lossless bitmap cowl photographs along with PNG photographs. The key concept in the back of this set of rules is that photographs are represented digitally the use of 24 bits of statistics for every pixel (eight bits for every shadeation aspect in RGB). So, there are 256 stages of intensities for every shadeation in every pixel, and converting the LSB of the shadeation intensities will, at worst, alternate the depth with the aid of using simply 1 level.

3. DES Algorithm

The DES (Data Encryption Standard) set of rules is a symmetric-key block cipher created with inside the early Seventies via way of means of an IBM. The set of rules takes the obvious textual content in 64-bit blocks and converts them into cipher text the use of 48-bit keys. Since it’s a symmetric-key set of rules, it employs the identical key in each encrypting and decrypting the data. If it had

been an asymmetrical set of rules, it might use one-of-a-kind keys for encryption and decryption. DES is primarily based totally at the Feistel block cipher, known as LUCIFER, evolved in 1971 via way of means of IBM cryptography researcher Horst Feistel. DES makes use of sixteen rounds of the Feistel structure, the use of a one-of-a-kind key for every round.

B. Modules

There are Six modules in our project.

1. Login Module

In this module there is one page in which consists of two fields such username and password and once enter these two credentials then system will initiate the system and provide a interface from there we can able to perform the stenography methods on image audio and video.

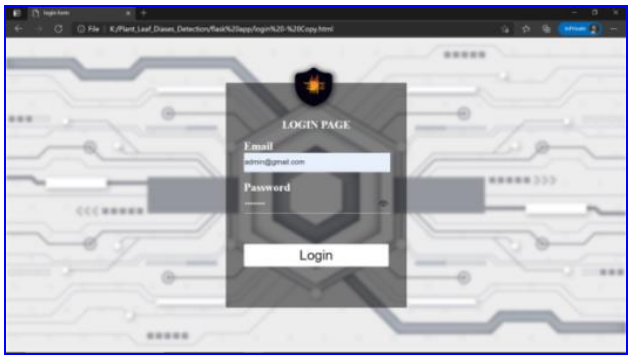

Figure 1: Login Module

2. Registration Module

By this module user able to create a new user account by entering its details such as name, number, password etc., and once it has done it will be able to login with the new credential and then user will able to perform.

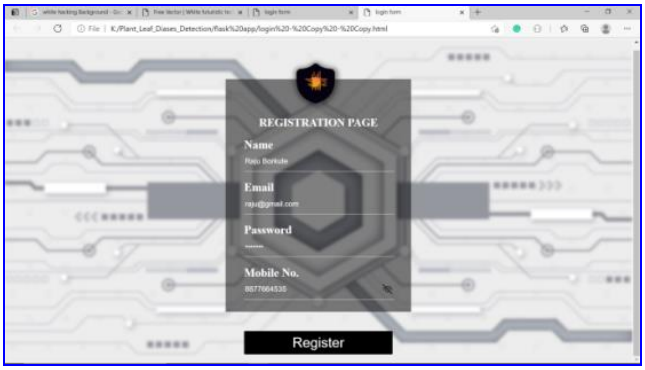

Figure 2. Registration Module

3. Home Screen Module

Basically, in this option we are providing three different options for user they can encode and decode the media such as Image, Video and Audio. Once the user selects the type of media then next screen will appear from, they can select the media file and enter the hidden text message and encode the secret message into the media and generate the new encoded media file.

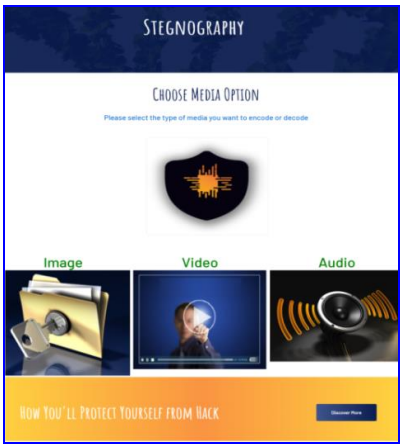

Figure 3. Home Module

4. Image Module

Basically, in this module it will allows user to choose the image file and hide a secret message inside the image and it will generate new image with the encrypted secret message.

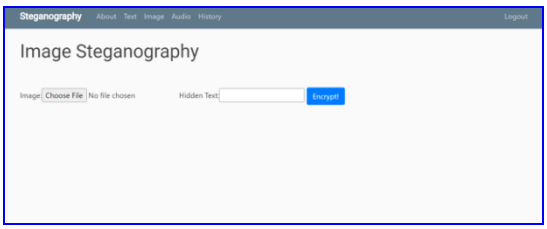

Figure 4. Image Module

5. Video Module

Basically, in this module it will allows user to choose the video file and hide a secret message inside the video and it will generate new video with the encrypted secret message.

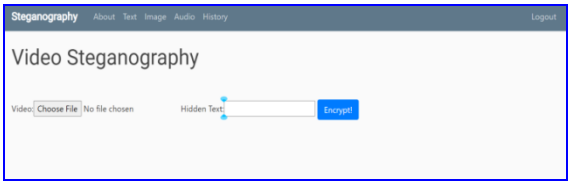

Figure 5. Video Module

6. Audio Module

Basically, in this module it will allows user to choose the audio file and hide a secret message inside the image and it will generate new audio with the encrypted secret message.

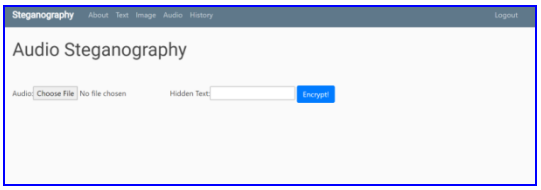

Figure 6. Audio Module

III. Result and Discussion

The effects and opinions of the layout primarily based totally on exceptional safety elements are presented. The major purpose is to look what number of functions were executed primarily based totally on safety necessities and specs enlisted within side the starting with a purpose to offer desirable safety for users.

V. Future Scope

In destiny this generation allows in safety to save you information and it allows to offer cryptography steganography aleven though continues to be a reasonably new thoughts there are consistent development withinside the laptop subject suggesting strengthen withinside the subject of steganography as properly it's miles probable that there'll quickly be extra green and extra development strategies a hopeful strengthen with inside the progressed sensitivity to small message understanding how tough it's miles to locate the presence of a reasonably.

VI. Conclusions

Steganography is a technique of embedding a thriller information or message from the sender to the recipient with the manner it covers for embedding, thinking about that steganography is not that easy to learn, so the sender and recipient need to understand the understanding of the steganography technique in each one Format and in any condition.

References

[1] Ramadhan J. Mstafa, Khaled M. Elleithy, and Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC.", *IEEE Access*, Volume: 5, 06 April 2017, pp. 5354 – 5365. DOI: 10.1109/ACCESS.2017.2691581

[2] Sofyane Ladgham Chikouche and Noureddine Chikouche, "An Enhanced Approach to LSB-Based Image Steganography Using the AESA Algorithm", *5th International Conference on Electrical Engineering* - ICEE-B, May 29-31. October 2001

[3] Jörg J. Buchholz, "Advanced Encryption Standard", December 19, 2016. https://www.researchgate.net/publication/2573880_Advanced_Encryption_Standard/citations

[4] Shumeet Baluja "Hiding images to the naked eye: deep steganography" *31st NIPS 2017 conference on neural information processing systems*, 2017.

[5] Priya Paresh Bandekar and Suguna GC, "LSB-Based Text and Image Steganography Using the AES Algorithm", *International Conference on Communication Systems and Electronics* (ICCES 2017) IEEE Xplore Part Number: ISBN: 978-1-5386 -4765-3, 2017

[6] C. Lalengmawia, A. Bhattacharya, "Image steganography using an advanced encryption standard for the implantation of audio / video data", *Fifth International Conference on Current Trends in Information Technology*, IEEE 2018

[7] Ranyiah Wazirali, Waeed Alasmary, Mohamed Mahmoud, "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms", *IEEE Access*, Volume 4, 2018, DOI 10.1109 / ACCESS.2019.2941440,.

[8] Dolnghui Hu, Shengnan Zhou, Qiang Shen, Shuli Zhenh, Zhongqiu Zhou and Yuqi Fan, "Digital Image Steganalysis Based on Visual Attention and Deep Reinforcement Learning", *Access to the IEEE*, Volume 7, 2019. DOI-10.1109 / ACCESS.2019.2900076.

[9] Souma Pal and Professor Samir Kumar Bandyopadhyay, "various methods of video steganography", *International Journal of Research and Information Review*, Vol.03, number 06, págs. 2569-2573, June 2019.

[10] Ramadhan J. Mstafa and Khaled M. Elleithy, "A Highly Secure Video Steganography Using Hamming Code (7, 4) *IEEE LISAT 2014 Long Island Systems, Applications and Technology*, 2014.