American Journal of Open Research, 3(3), March, 2024, 921-927
E-ISSN: 2834-7668

Enhancing Security through Advanced Image Steganography Techniques

Pooja Bhatt, Bhavik Pargi, Ritesh Kumar
CSE, Parul University. Vadodara, India
e-mail: pooja.bhatt28403@paruluniversity.ac.in, 200303126004@paruluniversity.ac.in, 2003031260013@paruluniversity.ac.in

Abstract: *The project aims to explore various types of steganography techniques, with a focus on image steganography, where information is concealed within images. This involves decrypting the hidden data to retrieve the message image, a process that can be achieved through different methods. The study delves into image steganography, which involves hiding information such as text, images, or audio files within other image or video files. Specifically, the project concentrates on utilizing steganography to embed an image within another image using spatial domain techniques. By examining this particular method, the project seeks to deepen understanding of how image steganography operates and its potential applications. This research contributes to the field by providing insights into the implementation and effectiveness of steganography techniques, offering valuable knowledge for information security and data protection purposes. Through practical demonstrations and analysis, the project aims to showcase the capabilities and limitations of image steganography, facilitating further research and development in this domain. Ultimately, the project endeavors to enhance comprehension of steganography methods and their significance in safeguarding digital information.*

Keywords: *Security, Steganography Techniques, Advanced Image.*

INTRODUCTION

The paper work concentrates on the process of steganalysis, application and limitations of Steganography (AlSabhany et al., 2020; Dhawan & Gupta, 2021; Muralidharan et al., 2022). It presents a deliberation on diverse steganography image file formats like JPEG, BMP, PNG and TIFF along with color models for image formats like CMYK model, RGB model, HSL, HSV, NCS, DCT, DWT, LSB, etc. A modified inspection of the existing models are performed, on the basis of parameters likes ego image perceptibility, technical resources and security facet. A souring range of PSNR reading designates fitter quality of stego image (K. N. Singh et al., 2022; Wang et al., 2021). The inspection shows that JPEG(DCT/DWT) algorithms are more unsusceptible to attacks and provide high reluctance to steganalysis. BMP spatial domain techniques have greater capacity but are easily vulnerable to steganography whereas the PNG palette To mediate the secret message, one must opt a suitable blend of steganography method accompanying fit cover image format so that it disallows the captivation of the attacker.

The paper work traverse distinct compression methods and cryptographic techniques (Patel & Vaish, 2020; R. K. Singh et al., 2021). Most applications online use image or video file for communicating content (Abkenar et al., 2021; Grewal et al., 2022). Due to restricted bandwidth available, compression methods are pertained, and to guarantee privacy of user encryption is executed. Apt solution is combination of encryption and compression techniques. The paper inspects methodologies in compression technique like Huffman coding, Run length coding, Arithmetic coding and Lempel- Ziv-Welch compression (Sha et al., 2023). Lossy compression involves Huffman coding and Discrete Cosine Transformation, whereas Lossless compression comprises of LZW and Run length coding. It also explores various cryptographic techniques like Caser Cipher, Data Encryption Standard and Rivest Cipher (Alenezi et al., 2020; Sharma et al., 2022). An investigation was done on testing of image compression and encryption algorithm that are classified as: Encryption followed by compression, Compression followed by encryption, Collaboration of encryption and compression (Ahmad & Shin, 2021; Hameed et al., 2020). The result presumed that the finest compression and encryption standards were performed by encryption of image initially followed by compression techniques.

The paper examines the cryptographic techniques AES, RSA, DES, 3DES, and Blowfish, as well as the steganography algorithm LSB. The cryptographic algorithms are Java programmers that have been imported into the MATLAB environment (Clemente-López et al., 2024; Kaur & Kaur, 2021). An

investigation is done on the mentioned algorithms at the same time and same environment to contrast the discrete factors such as encryption and decryption timespan, SNR, Histogram and MSE (Markus & Kertesz, 2020). To achieve high security, cryptography and The investigation output led by the survey is that the execution time of RSA is more than other algorithms mentioned (Karsa et al., 2024; Komarudin et al., 2023).

This paper explores on the steganographic techniques along with compression algorithm. It explains the embedding and extracting algorithm. Here a comparison is done between two different techniques. Firstly, LSB algorithm is used with no encryption and compression. In second technique the secret message is encrypted and LSB is applied with DCT algorithm to transform the image into frequency domain. From the outcome of the experiment, we come to know that, we need to hide the secret data while minimizing its size, enabling more security. MSE and PSNR are used to assess the performance of these two approaches. The result of the experiment shows that using LSB and DCT effectively reduce the number of bytes in file, hence can be transmitted faster and takes less space on a disk.

The motivation in the back of growing image Steganography methods according to its use in diverse companies to talk among its members, in addition to, it may be used for communication among participants of the armor intelligence operatives or agents of businesses to cover secret messages or in the subject of espionage. The main purpose of employing Steganography is to avoid attracting attention to the transfer of secret data. If suspicion is raised, then this aim that has been planned to reap the safety of the secret messages, because if the hackers make any changes to the sent message, this observer will try to figure out what data is buried therein.

MATERIALS AND METHODS

User needs to run the application. The user has two-tab options– encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file. This project has two methods – Encrypt and Decrypt (Cun et al., 2021; Xian & Wang, 2021). In encryption the secrete information is hiding in with any type of image file. Decryption is getting the secrete information from image The methodology for an image steganography project typically involves the following steps:

Problem Definition: Define the problem statement and the scope of the project. This includes identifying the type of steganography technique that will be used, the tools and technologies required, and the constraints and limitations of the project.

Data Collection: Collect the dataset of images that will be used for embedding and extracting the secret message. This may include public domain images or images that are specifically created for the project.

Pre-processing: Pre-process the images to ensure consistency in size, resolution, and format. This step involves adjusting the images to match the requirements of the chosen steganography technique.

Secret Message Encoding: Encode the secret message using a chosen encoding algorithm to convert it into a format that can be embedded in the image. The encoding algorithm should be chosen based on the size and complexity of the message.

Image Embedding: Embed the secret message into the image using the chosen steganography technique. The technique used should ensure that the image quality remains unchanged, and the embedded message is not easily detectable by visual inspection.

Image Extraction: Extract the secret message from the image using the chosen steganography technique. The extraction process should be able to retrieve the message accurately and reliably, even if the image has been modified or compressed

Evaluation: Evaluate the performance of the steganography algorithm by measuring the image quality, message retrieval accuracy, and detection resistance.

The Graphical Representation of this Project:

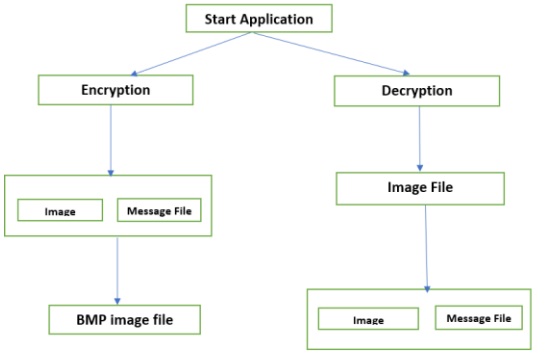

Figure 1. Project Flow Chart

RESULTS AND DISCUSSION

Steps to create an Image Steganography project using Django in python with VS code:

Environment Setup: Install Python: Install Python on your system . Python is the primaryprogramming language for Django.

Install Django: Use the Python package manager (pip) to install Django. You can run pipinstall django to install the latest version.

Set Up Visual Studio Code: Install assist in Django development, such as the ”Django” extension.

Create a Virtual Environment: Create a virtual environment for your project to isolate dependencies. You can create a virtual environment using python -m venv myenv,

Create a Django Project: Use the Django command-line interface (CLI) to create a new Django project. Run django-admin startproject projectname to initiate a new project.

Create a Django App: Inside your project, create a dedicated app to handle steganography features. You can create an app using python manage.py startapp appname.

Define Data Models: In your app's 'models.py', define data models to store information related to encoded images.For instance, you can create a model to store encoded images and their associated data.

Develop User Interface: Create HTML templates for your application. You'll need templates for encoding, decoding, and displaying the results. Create Django forms (e.g., EncodeForm and DecodeForm) to handle user input for encoding and decoding.

Develop User Interface: Create HTML templates for your application. You'll need templates for encoding, decoding,and displaying the results. Create Django forms (e.g., EncodeForm and DecodeForm) to handle user input for encoding and decoding.

Implement Steganography Functions: Develop Python functions for encoding and decoding messages within images. These functionswill use image processing libraries like Pillow (PIL) to embed and extract messages.

Create Views: Write views in your app's 'views.py' to handle encoding and decoding requests. These views will use the forms and steganography functions to process user input

URL Configuration: Set up URL patterns in your app's 'urls.py' to map URLs to the appropriate views. You shoulddefine URL patterns for encoding, decoding, and other relevant views.

Testing and Debugging: Thoroughly test your application to ensure that the encoding and decoding functionalities workas expected.

Run the Development Server: Start the Django development server with 'python manage.py runserver'. Access the project in your web browser at 'http://127.0.0.1:8000/'. Use the provided views to encode and decode images, demonstrating image steganography

Security Measures: Implement security measures to protect against unauthorized access and misuse of thesteganography features. This may include user authentication and proper authorization.

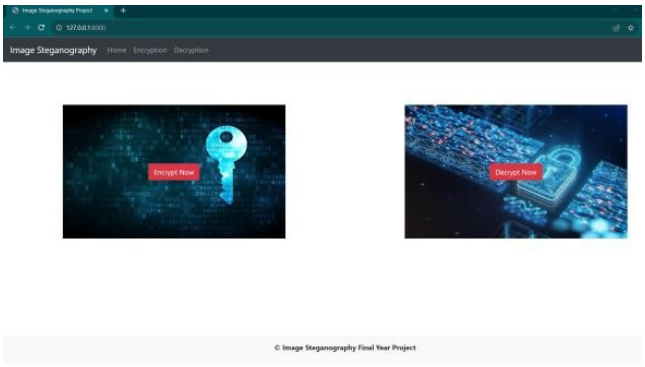

Figure 2. Home Page

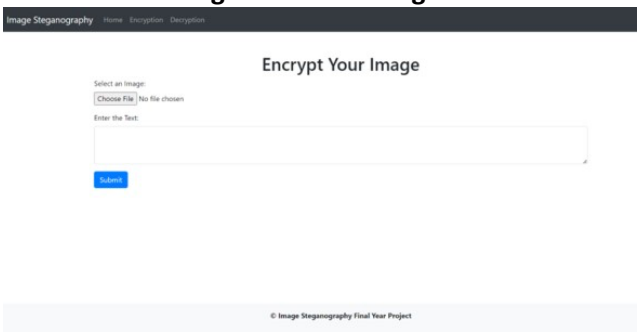

Figure 3. Encryption Option

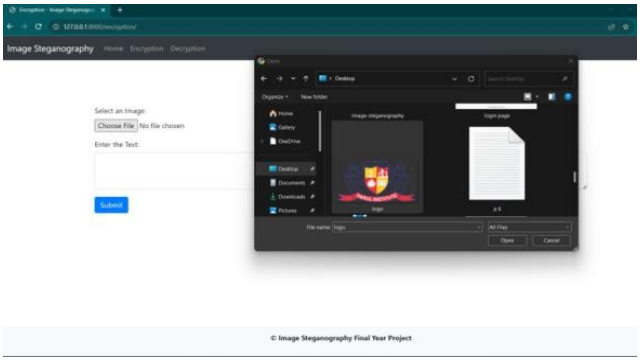

Figure 4. Select Image For Encryption

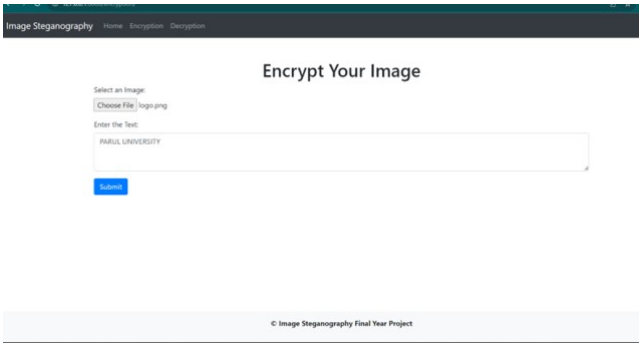

Figure 5. Encrypt Data

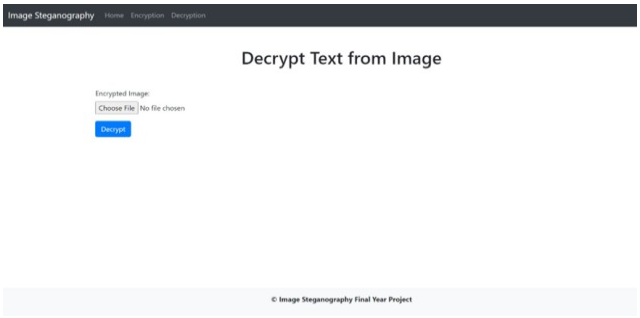

Figure 6. Decryption Option

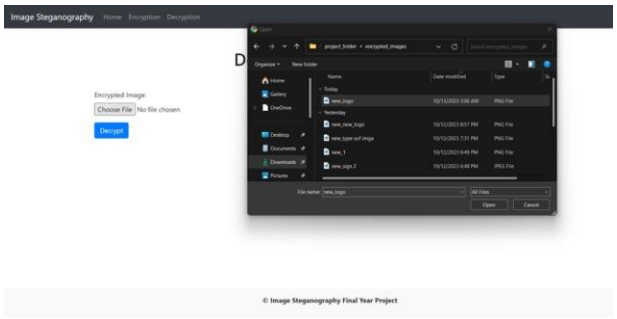

Figure 7. Choose Image For Decryption

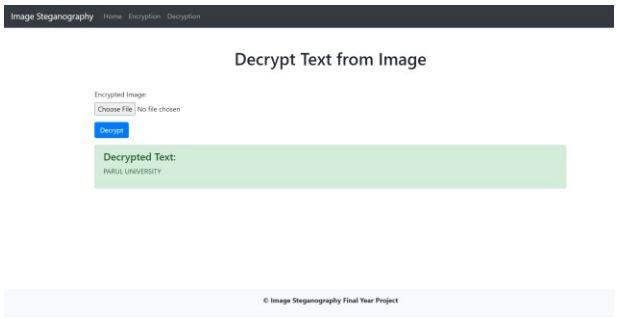

Figure 8. Decrypt Message

CONCLUSION

From the survey of existing methodologies and the techniques used for hiding the data, it can be seen that we need to use proper combination of techniques for security and efficiency of hiding the important data. Steganography conveys secrets across seemingly harmless covers in an attempt to hide a secret's existence. The employment and applications of digital steganography and its derivatives are increasing exponentially. Although the security of the Least Significant Bit technique is good, we can improve it in several ways by utilizing different carriers and different keys for encryption and decryption.

REFERENCES

Abkenar, S. B., Kashani, M. H., Mahdipour, E., & Jameii, S. M. (2021). Big data analytics meets social media: A systematic review of techniques, open issues, and future directions. *Telematics and Informatics*, *57*, 101517.

Ahmad, I., & Shin, S. (2021). A novel hybrid image encryption–compression scheme by combining chaos theory and number theory. *Signal Processing: Image Communication*, *98*, 116418.

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272.

AlSabhany, A. A., Ali, A. H., Ridzuan, F., Azni, A. H., & Mokhtar, M. R. (2020). Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. *Computer Science Review*, *38*, 100316.

Clemente-López, D., Munoz-Pacheco, J. M., & de Jesus Rangel-Magdaleno, J. (2024). Experimental validation of IoT image encryption scheme based on a 5-D fractional hyperchaotic system and Numba JIT compiler. *Internet of Things*, 101116.

Cun, Q., Tong, X., Wang, Z., & Zhang, M. (2021). Selective image encryption method based on dynamic DNA coding and new chaotic map. *Optik*, *243*, 167286.

Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63–87.

Grewal, D., Herhausen, D., Ludwig, S., & Ordenes, F. V. (2022). The future of digital communication research: Considering dynamics and multimodality. *Journal of Retailing*, *98*(2), 224–240.

Hameed, M. E., Ibrahim, M. M., Abd Manap, N., & Mohammed, A. A. (2020). A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. *Future Generation Computer Systems*, *111*, 829–840.

Karsa, A. H. A. N., Wahyuningsih, O., Jannah, R., & Saebah, N. (2024). Web-Based Car Rental Information System At Cv. Mandarental Cirebon. *Asian Journal of Engineering, Social and Health*, *3*(2), 374–380.

Kaur, L., & Kaur, R. (2021). A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm. *Global Transitions Proceedings*, *2*(2), 520–529.

Komarudin, K., Maulani, I. E., Herdianto, T., Laksana, M. O., & Syawaludin, D. F. (2023). Exploring The Effectiveness of Artificial Intelligence in Detecting Malware and Improving Cybersecurity in Computer Networks. *Eduvest-Journal of Universal Studies*, *3*(4), 836–841.

Markus, A., & Kertesz, A. (2020). A survey and taxonomy of simulation environments modelling fog computing. *Simulation Modelling Practice and Theory*, *101*, 102042.

Muralidharan, T., Cohen, A., Cohen, A., & Nissim, N. (2022). The infinite race between steganography and steganalysis in images. *Signal Processing*, *201*, 108711.

Patel, S., & Vaish, A. (2020). A systematic survey on image encryption using compressive sensing. *J Sci Res*, *64*(1), 291–296.

Sha, Y., Mou, J., Banerjee, S., Jahanshahi, H., & Cao, Y. (2023). Low-cost multiclass-image encryption based on compressive sensing and chaotic system. *Nonlinear Dynamics*, *111*(8), 7831–7857.

Sharma, D. K., Singh, N. C., Noola, D. A., Doss, A. N., & Sivakumar, J. (2022). A review on various cryptographic techniques & algorithms. *Materials Today: Proceedings*, *51*, 104–109.

Singh, K. N., Singh, O. P., & Singh, A. K. (2022). Ecis: encryption prior to compression for digital image security with reduced memory. *Computer Communications*, *193*, 410–417.

Singh, R. K., Kumar, B., Shaw, D. K., & Khan, D. A. (2021). Level by level image compression-encryption algorithm based on quantum chaos map. *Journal of King Saud University-Computer and Information Sciences*, *33*(7), 844–851.

Wang, X., Liu, C., & Jiang, D. (2021). A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Information Sciences*, *574*, 505–527.

Xian, Y., & Wang, X. (2021). Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, *547*, 1154–1169.