Enhancing Security through Advanced Image SteganographyTechniques

1st Asst.Prof Dr. POOJA BHATT
CSE, Parul University.
Vadodara, India p

2nd Bhavik pargi
CSE, Parul University.
Vadodara, India

3rd Ritesh Kumar
CSE, Parul University.
Vadodara, India

absract:

The project aims to provide and learning about the various types of steganography available. Image steganography is performed for images and the concerning data is also decrypted to retrieve the message image. Since this can be done in several ways, image steganography is studied and one of the methods is used to demonstrate it.

Image steganography refers to hiding information i.e. text, images or audio files in another image or video files. The current project aims to use steganography for an image with another image using spatial domain technique.

I. LITERATURE REVIEW

1) Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez A Comparative Study of Recent Steganography Techniques for Multiple Image Formats",
(2019)

The paper work concentrates on the process of steganalysis, application and limitations of Steganography. 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. 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.

2) Siddharth Singh and Raghav Devgan, "Analysis of Encryption and Lossless Compression Techniques for Secure Data Transmission", (2019)

The paper work traverse distinct compression methods and cryptographic techniques. Most applications online use image or video file for communicating content. 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. 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. An investigation was done on testing of image compression and encryption algorithm that are classified as:
a) Encryption followed by compression, b) Compression followed by encryption, c) Collaboration of encryption and compression.

The result presumed that the finest compression and encryption standards were performed by encryption of image initially followed by compression techniques

3) Masoumeh Dam Rudi, Kamal Jaidy Aval, "Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish", (2019)

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. 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. 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.

4) Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf and Hanafy M. Ali, "Hiding data in images using steganography techniques with compression algorithms", (2019)

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.

5) Rashmi Kasdan and Nitesh Gupta, "A New Approach of Digital Signature Verification based on Bio Gamal Algorithm", (2019)

Information security consists of aspects like authentication, confidentiality and integrity of data. In order to achieve this digital signature by original sunderances time complexity. Outcome of this experiment shows that, it is 30-40%efficient with respect to play Gamal algorithm with encryption/decryption time.

6) Christy Atika Sari, Giovani Ardiansyah, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography", (2019)

Cryptography and steganography are two recurrent methods to implement security in information security domain. The paper prospects on methods like Discrete Wavelet Transform (DWT), AES and Huffman coding. The method lodged is combination of AES, Huffman coding and DWT which reduces the total bits in message. Examination of the experiment is done by PSNR and MSE.
The conclusion of the lodged method is that it lays out a good quality stego image with soaring capacity in DWT for steganography by diminishing the total message's bit up to 22.319% from the original message's bit. A good quality

7) Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed and Ahmed Bouridane, "Image Steganography: A Review of the Recent Advances", (2021)

This paper recce the recent advances of image steganography. It elucidates the traditional methods like LSB, PVD, DCT and EMD. These methods lead to distortion due to high capacity by encumber the cover image with more pixels for hiding secret message. The paper also explains the CNN based image steganography techniques and GAN steganography. An inspection is done with PSNR value comparison, which gives the output with prime PSNR value64.7 obtained using cycle GAN. GAN based method uplifts security and hidden capacity. The paper also elaborates on challenges faced, scopes in future, etc. The paper terminates that deep learning proves prodigious potential in image steganography.

8) Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", (2019)

The paper traverses the distinct streams of cryptography and steganography. It explains the three primitives for steganography algorithms i.e., Security, Capacity and Robust. The proposed algorithm avail steganography and Hybrid cryptography. Firstly, using AES algorithm the message is encrypted and using public key of RSA even the symmetric key is encrypted, which escalates the security. The Hash value of message is engendered using public key of RSA to produce digital signature. At receiver end, this is used to examine integrity. The message is embedded using LSB technique.

The result of the experiment is that the histogram for both cover image and stego image is identical, hence provides confidentiality, integrity and authentication.

9) Vikas Singhal, Yash Kumar Shukla, Navin Prakash, "Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256", (2020)

The paper scouts the amalgam of three methods LSB, AES and SHA256. The proposed method accomplishes the task obscuring information. It first hides the data using LSB technique and surfeit the protection of data using cryptographic technique AES-256 as well as the weak point that a hacker could target that is key, it also has been protected via the use of hashing technique SHA256.

The result shows a disguised image, making it non-viable to attract imposters. Hence, proposed system proves high security for classified information and exchanging it with no susceptibility.

10) Mustafa S. Abbas, Suadad S. Mahdi and Shahad Hussein, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography", (2020)

The paper traverse on the drawback in cloud environment, security issues of data storage. The proposed algorithm is, initially the data is compressed using LZW algorithm, later hybrid encryption using AES symmetric and RSA asymmetric algorithms is performed. The encrypted data is hidden using LSB technique and hashing algorithm is applied. Analysis is done using PSNR and SSIM values, which were calculated before and after applying compression technique. The result shows that PSNR values of stego image are better for compressed data when contrasted with non-compressed data.

II.MOTIVATION

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.

The main motivations are:

- Protection of digital data and
- Information transferred via the Internet is kept private.

The goals are:

- By encasing the transmitted data in a cover material, the information becomes invisible.
- To improve the information's security and resilience to attackers.
- To achieve the CIA Triad of Information Security (Confidentiality, Integrity, and Authentication

III. methodology

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.
- 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:

1.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.

2.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.

3.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.

4.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.

5.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.

6. 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

7. 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:

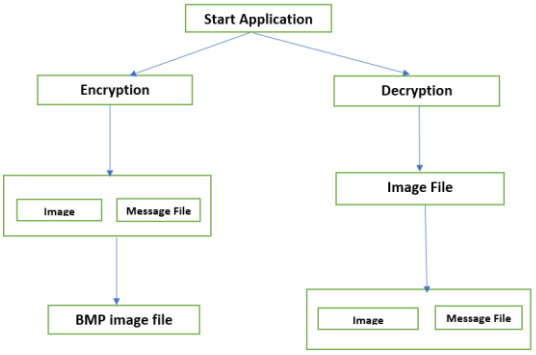

Figure 1:project flow chart

IV.IMPLEMENTATION

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

1. 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,

2. Create a Django Project and App:

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.

3. 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.

3. 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.

4. 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.

5. 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.

6. 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

7. 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.

8. **Testing and Debugging:-**

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

9. 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

10. Security Measures:

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

V. RESULT

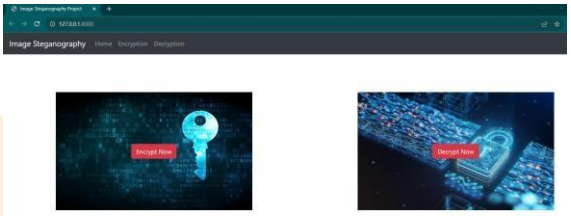

Figure 2:home page

Figure 3: Encryption option

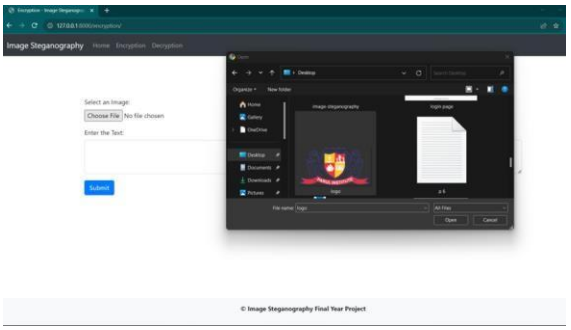

Figure 4: select image for encryption

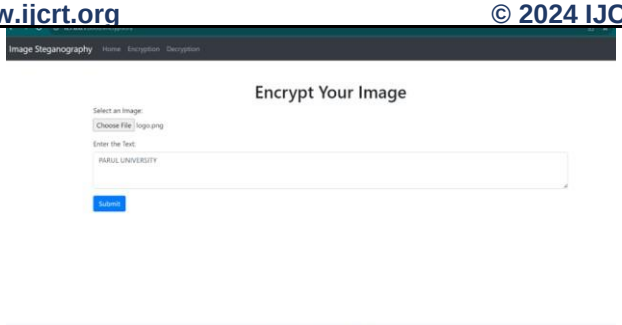

Figure 5:Encrypt data

Figure 6:decryption option

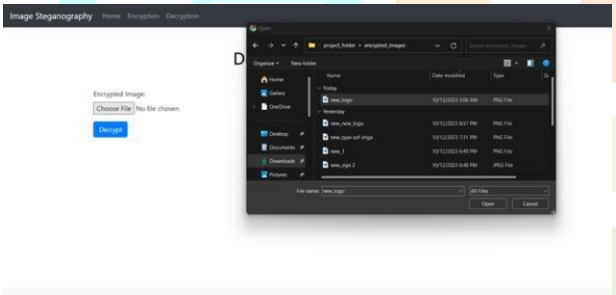

Figure 7:choose image for decryption

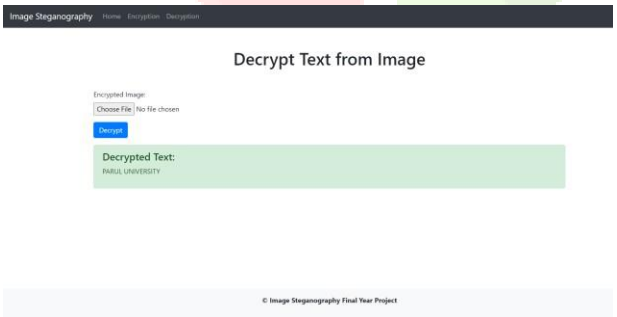

Figure 8:Decrypt message

III. 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.

IV. REFERENCES

[1] Ashraf A. M. Khalaf, O. F. Abdel Wahab, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques", IEEE Access, volume: 9, Feb 2021.

[2] Arshiya Sajid Ansari, Mohammad Sajid Mohammadi and Mohammad Tanvir Parvez, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", I. J. Computer Network and Information Security, 2019, 1, 11-25 Published Online January 2019 in MECS (http://www.mecspress.org/)DOI:10.5815/ijcnis.2019.01.02

[3] Siddharth Singh and Raaghavv Devgon," Analysis of Encryption and Lossless Compression Techniques for Secure Data Transmission", 2019 IEEE 4th International Al Conference on Computer and Communication Systems.

[4] Masumeh Damrudi and Kamal Jadidy Aval, "Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019

[5] Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. Ahamed, Hamdy M. Kelash, Ashraf A.M. Khalaf and Hanafy M. Ali, "Hiding data in images using steganography techniques with compression algorithms", TELKOMNIKA, Vol.17, No.3, June 2019, pp.1168~1175ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018DOI:10.12928/TELKOMNIKA.v17i3.12230

[6] Rashmi Kasodhan and Neetesh Gupta, "A New Approach of Digital Signature Verification based on Bio Gamal Algorithm", Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Xplore Part Number: CFP19K25-ART; ISBN: 978-1-5386-7808-4

[7] Christy Atika Sari, Giovani Ardiansyah, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography", TELKOMNIKA, Vol.17, No.5, October 2019, pp.2400~2409 ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018DOI:10.12928/TELKOMNIKA.v17i5.9570

[8] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, and Ahmed Bouridane, "Image Steganography: A Review of the Recent Advances", IEEE Access, volume: 9, Jan 2021

[9] Chitra Biswas, Udayan Das Gupta and Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", International Conference on Electrical, Computer and Communication Engineering (ECCE), Feb 2019

[10] Vikas Singhal, Yash Kumar Shukla and Navin Prakash, "Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256",International Journal of Innovative Technology and