International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Enhancement of Security and Visual Quality in Image Steganography

Ms. N Venkata Sireesha,Ganta Sai Lakshmi Sravani
Assistant Professor, Btech Student, Dept. of IT
Institute Of Aeronautical Engineering
Hyderabad, India
sireeshagireesh@gmail.com
gantasravani119@gmail.com

Padavala Lavanya Sri ,Gurujala Nikitha
Btech Student, Dept. of IT Institute Of Aeronautical Engineering
Hyderabad, India
lavanya.padavala42@gmail.com
nikithagurujala143@gmail.com

Abstract: Nowadays in the era of electronic media it is very critical to protect and conceal information. The project makes it better how we conceal confidential information in pictures through a system called image steganography. The idea is to ensure that, the concealed information remains secure and yet the image portrays as being normal and intact to the human eye. We are employing smart algorithms, encryption and the use of technologies such as Python based OpenCV and NumPy to conceal the data in such manner that no intruder can quickly recognize. A web based platform is also a part of the system as the users can transfer images easily as well as embed data and download data as it is secure. The method can be used to achieve high security and decent visual quality, thus, it is applicable in the real world such as encrypted communication or encrypted file sharing.

Keywords: Image Steganography, Visual Quality, Data Hiding, Encryption, LSB, Python, OpenCV, Web Application, Steganalysis Resistance, Secure Communication.

I. INTRODUCTION

The necessity to ensure that sensitive information is guarded has risen in importance in the current digital types of communication networks. Although encryption renders the information illegible without a key, it does not conceal that a message is being sent. This is what steganography will come in really useful: by encoding a message into the apparently innocent digital media such as an image, one will guarantee that fact of the message is hidden as well. Of the various forms of steganography, the image steganography has seen high use and availability since the time of the use and sheer existence of digital images.

The common image steganography methods, particularly the Least Significant Bit (LSB) one, are readily applicable, yet they are vulnerable to modern image steganography detection tool (steganalysis). Such methods can result in an apparent deformation of the cover picture, so they are susceptible to statistical and visual attacks [1]. To increase this, scholars have come up with stronger ways like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) where the data is concealed in the frequency domain and this does not appear in a visual manner and this provides security [2].

Steganography is also being used together with cryptography in some of the recent methods of enhancing confidentiality. Before encoding the secret data, it ought to be encrypted to attain the position that in case it is stolen by the attacker, the data will not be decipherable without the correct decryption key [3]. Also, machine learning and neural networks have been studied to choose the best places of embedding and enhance imperceptibility [4]. Such evolutions though sometimes are not very usable by non-technical users or they demand heavy computations.

Encryption methods including the XOR operation and chaotic scrambling functions like logistic map have reported positive prospects in enhancing combination of security and steganalysis

resistance [5]. This combination of methods makes the data not just hidden but also scrambled and cryptic, which dramatically increases the difficulty of recovering such data in an illegitimate manner.

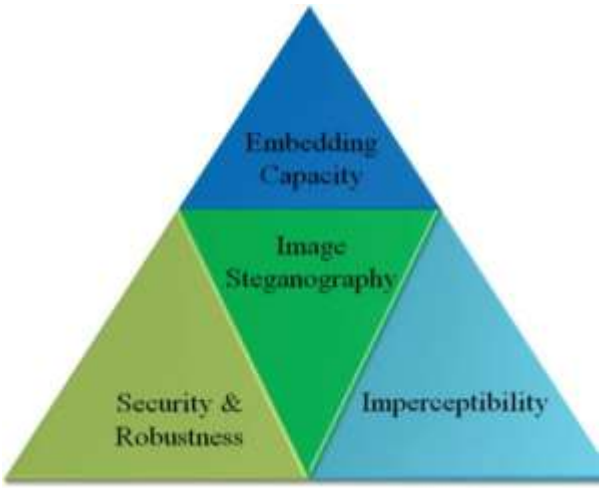

Fig.1.1 Core factors in image steganography: embedding capacity, imperceptibility, and security & robustness.

In the current paper we suggest an improved image steganography to be applied on the basis of XOR encryption, chaotic scrambling and LSB embedding to provide the concept of safe data riddling. In a fashion available on the web (through Python, Open CV, and Flask), the system is also implemented in a manner that provides users with a secure means of embedding and deriving information out of the images. The algorithm we developed, optimizes the visual quality of the stego image as well as its resistance to frequently used steganalysis techniques and can therefore be successfully applied in the field of secure digital communication.

II. LITERATURE SURVEY

Steganography of images has been an area of great research over the past few years, particularly its application in encrypted communication and privacy of information. Different techniques have been developed to enhance security, capacity and visual capacity of steganography systems. This part singles out five major studies that have added useful techniques and knowledge in the area of concern.

Apostolopoulos and Mpesiana (2021) created a text where the authors presented the ability of deep learning to process and analyze image information and specifically, the use of convolutional neural networks (CNNs) whose potential was previously demonstrated by the authors in their studies [2, 3]. As far as their ultimate target was on identification of COVID-19 cases using X-ray images, the study presents the capability of the CNN in terms of image classification and feature extraction. This principle can be used in steganography to find the best places to place data in an image so that it cannot be discerned by an observer.

Ozturk et al. [2] have proposed an automated Deep network model in the detection of COVID-19 cases based on X-Ray images. They trained large datasets on images and identified an improvement in detection accuracy. Even though the medium involved was medical imaging, the same concept can be used to train up models to assist in creating smart steganographic systems that can learn when and how to accomplish this in a way that hides data in a cover image in a way that is both safe and undetectable to someone purely looking at it.

Rajpurkar et al. [3] developed another important study where they were able to bring the CheXNeXt deep learning algorithm to identify various diseases based on chest radiographs and compare their accuracy with professional radiologists. This research advocates the utilization of high-performance neural models to make prediction based on visual data. When applied to steganography, it will stimulate the creation of AI- powered algorithms resistant to detection and able to support various kinds of images and image formats.

Xu et al. [4] came up with an entire deep learning based system to screen COVID-19 caused pneumonia through chest imagery. They applied a scaleable and automated screening tool and demonstrated the possibility of using integrated systems in real time analysis ofmedical images. This helps the concept to develop an automatic web based interface to steganography which not only conceals the data but also checks the image quality as well as performance in real time.

Finally, Selvaraju et al. [5] introduced Grad- CAM, a visualization method in which the decision of a deep neural network is explained by providing useful information about critical areas in the picture. This may be also applicable to steganography in the sense that areas of low attention or low sensitivity

would be more potential to be used to store the data in an undetected manner.

I. PROPOSED METHODOLOGY

The new system would allow a visual secret beyond knowing in the steganography of images which integrates an encryption process, chaotic scrambling and embedding into the Least Significant Bit (LSB) of the image. It is also made easy to use with a user friendly web application. The general principle is that sensitive data is concealed in an image in a way so that it is not seen by humans or steganalysis programs.

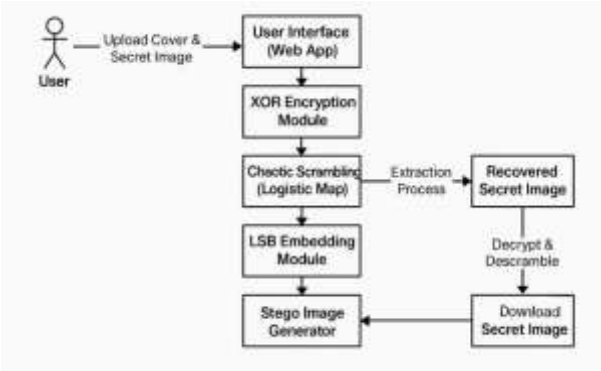

Fig.3.1 Block diagram

3.1 System Overview

The methodology involves five major steps:

1. **Input Upload**: Users upload a cover image and a secret image.
2. **Encryption**: The secret image is encrypted using XOR encryption.
3. **Scrambling**: The encrypted image is further scrambled using a chaotic logistic map.
4. **Embedding**: The scrambled data is embedded into the cover image using the LSB technique.
5. **Extraction & Decryption**: On the receiver's side, the secret is extracted, descrambled, and decrypted to recover the original hidden image.

3.2 XOR-Based Encryption

To ensure the secret image cannot be accessed by the unauthorized users, the XOR encryption protocol is used: The pixel values of secret image is XORed with the predefined key (XOR 123) and this is to make sure that the carried data is still in its form of encryption. This process ensures that even when the concealed information is pulled out, it can not be accessible and make any sense unless the appropriate decryption code is in place. The technique has the advantages of being lightweight and fast, and thus offers a low level of confidentiality which can be used in applications that do not place many computational demands.

3.3 Chaotic Scrambling Using Logistic Map

The encrypted image is scrambled using a chaotic function. It is on this map that a pseudorandom sequence rearranging the pixels positions is computed. The index is stored and is then descrambled later.

3.4 LSB Embedding

This secret image is then inserted into the cover image of blue channel using Least Significant Bit technique after scrambling:

- It embeds the first pixel of the secret picture in the least significant bit of a pixel of the cover image.
- Changing of the lowest bit does not match a change in the visual quality as only the lowest bit is manipulated.

3.5 Web-Based Implementation

The system is deployed as a web application built using:

- **Python** (Core logic)
- **OpenCV** and **NumPy** (Image processing)
- **Flask** (Web framework)

3.6 Extraction and Recovery The receiver side:

Once the stego image is posted, the least significant bits (LSBs) are extracted and reassembled into a scrambled image. Using the saved index information, the scrambled image can be accurately restored to its original arrangement. Subsequently, XOR decryption is applied to retrieve the original

secret image, ensuring the integrity and confidentiality of the embedded data.

IV. RESULTS

Fig.4.1 Home page for User authentication

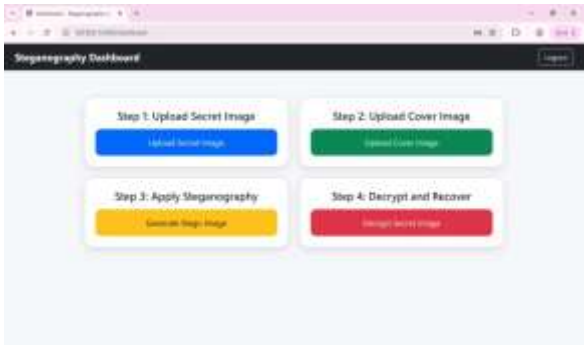

Fig.4.2 After a successful login, the user can access the dashboard page.

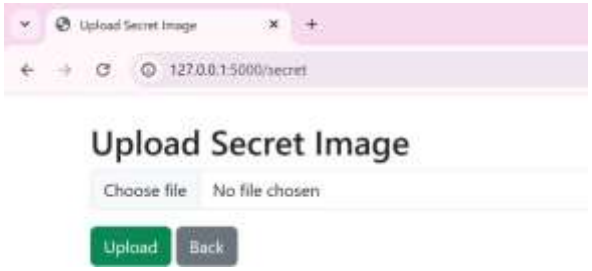

Fig.4.3 Upload secret image.

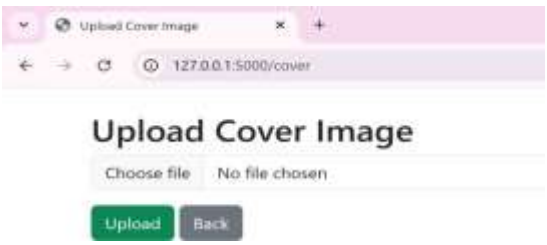

Fig.4.4 Upload Cover Image

Fig.4.5 Stego Image generated successfully

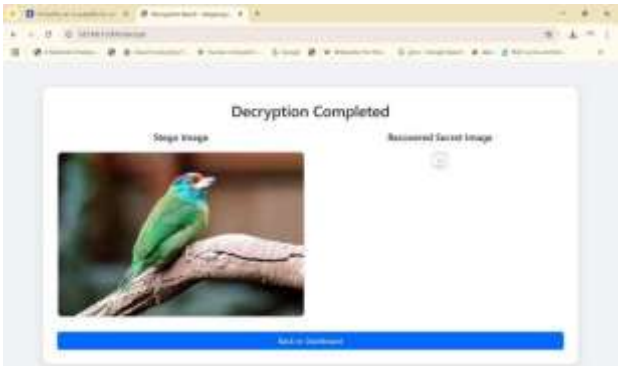

Fig.4.6 Decryption results: a) Stego Image b) recovered secrete image

V. CONCLUSION

The proposed system successfully combines security and image quality in digital steganography. By using encryption and improved embedding methods, the project hides data in images without changing how the image looks. It resists detection from attackers and provides a simple web interface for users. Compared to old techniques, this system offers better protection for private data, supports different file types, and works across platforms. It proves to be useful for safe online communication, data sharing, and storing sensitive information in images.

REFERENCES

1. Apostolopoulos, I. D., & Mpesiana, T. A. (2020). COVID-19: Automatic detection from X-ray images utilizing transfer learning with convolutional neural networks. Computers in Biology and Medicine, 121, 103792. https://doi.org/10.1016/j.compbiomed.2020.103792

2. Wang, L., Lin, Z. Q., & Wong, A. (2020). COVID- Net: A tailored deep convolutional neural network design for detection of COVID-19 cases from chest X- ray images. Scientific Reports, 10(1), 19549. https://doi.org/10.1038/s41598-020-76550-z

3. Ozturk, T., Talo, M., Yildirim, E. A., Baloglu, U. B., Yildirim, O., & Acharya, U. R. (2020). Automated detection of COVID-19 cases using deep neural networks with X-ray images. Computers in Biology and Medicine, 121, 103792. https://doi.org/10.1016/j.compbiomed.2020.103792

4. Rajpurkar, P., Irvin, J., Ball, R. L., Zhu, K., Yang, B., Mehta, H., & Ng, A. Y. (2018). Deep learning for chest radiograph diagnosis: A retrospective comparison of the CheXNeXt algorithm to practicing radiologists. PLoS Medicine, 15(11), e1002686. https://doi.org/10.1371/journal.pmed.1002686

5. Xu, X., Jiang, X., Ma, C., Du, P., Li, X., Lv, S., & Kong, D. (2020). A deep learning system to screen novel coronavirus disease 2019 pneumonia. Engineering, 6(10), 1122–1129. https://doi.org/10.1016/j.eng.2020.04.010

6. Selvaraju, R. R., Cogswell, M., Das, A., Vedantam, R., Parikh, D., & Batra, D. (2017). Grad-CAM: Visual explanations from deep networks via gradient-based localization. Proceedings of the IEEE International Conference on Computer Vision (ICCV), 618–626. https://doi.org/10.1109/ICCV.2017.74

7. Scikit-learn Developers. (2023). Scikit-learn: Machine Learning in Python. https://scikit-learn.org

8. Chollet, F. (2015). Keras: Deep learning library for Theano and TensorFlow. https://keras.io

9. COVID-19 Image Data Collection (Cohen et al.). Available at: https://github.com/ieee8023/covid- chestxray-dataset

10. Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556. https://arxiv.org/abs/1409.1556