Shades of Secrecy: The art of Image Steganography

Lakhan Parashar
Department of Computer Science and Engineering
Chandigarh University
Chandigarh, India
lparashar02@gmail.com

Prakhar Nigam
Department of Comouter Science and Engineering
Chandigarh University
Chandigarh, India
prakharnigam222@gmail.com

Deeptesh Jyoti
Department of Computer Science and Engineering
Chandigarh University
Chandigarh, India
deeptesh182000@gamil.com

Rajiv Ranjan
Department of Computer Science and Engineering
Chandigarh University
Chandigarh, India
rajivranjan2304@gmail.com

***Abstract*— Image steganography is the process by which we can hide our information which could be in nay form such that text, image or video in another or cover image. This process is used to increase the security of data and secure and reliable transfer of information over the internet. As security is considered on of the most important factor in the IT world, thus image steganography is an effective way to do so. In this paper, a detailed process of steganography is explained and practical approach for the same is also given.**

Keywords—Image steganography, Security, Data hiding.

I. INTRODUCTION

The world is growing significantly in the terms of technology as almost everyday a new form of tech invention is happening, the need for security is more than ever. Almost every other organization is dependent of their security teams for their protection of data and securing their information from cyber theft. Steganography has been used for over centuries, but as the world became modernized and data became digital, steganography also changed its form to help the digital data to be secured.

Cryptography was the method to secure the communication between the two parties which involved encrypting and decrypting the data. But sometimes these encryption methods are not sufficient to keep the contents of the data secure. For this purpose, the technique of steganography was developed [1].

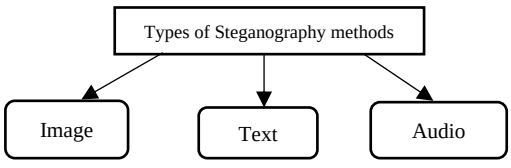

Figure. 1.1

1.1 Types of steganography methods

Image steganography is the practise of concealing information inside photographs. In order to make the alteration less obvious and make it easier to conceal the information, the noisy parts of the cover picture are changed with a wide range of colour changes. Several methods of picture steganography include masking, filtering, and transformations [2], as well as the use of least significant bits.

Text Steganography: It is done by altering the text characteristics. This is done by various coding methods in such a way that it does not seem suspicious or altered to the user. Line-shift coding, Word-shift coding, and Feature coding are the three coding methods that may be employed for text steganography [2].

Audio steganography is a method for concealing information in digitalized audio signals, which may cause a tiny change in the binary order of the audio file. The following are many methods for audio steganography: Spread spectrum, LSB coding, phase coding, echo hiding [2],

1.2 Steganalysis

The art and science of detecting hidden information/data is called steganalysis. It can be used by the hackers to steal the information. But also steganalysis can find its uses in cyber forensics, tracking of criminal activities and much more. It could also be used to improve the methods of steganalysis so that it could become hard to decode by the attackers [3].

Thus, image steganography is a useful approach in the world or we can say in the domain of technology and security. This paper discusses the ways to perform steganography and also the future scope of steganography.

II. LITERATURE REVIEW

Image steganography is a technique of hiding secret data inside an image without changing its visual appearance. The process includes changing the pixels' least important bits, or those that contain the least amount of information. Least Significant Bit (LSB), Pixel-Value Differencing (PVD), and Spread Spectrum are only a few of the methods utilised in picture steganography (SS)

Nowadays many steganography methods were discovered by researchers. They are trying to maximize the quality of image as

when the data is stored in the image the quality of the image is getting lower and the image becomes blurry

In this section several state of the art and methods are discussed.

1. A.H.M Almawgani [4] used the concept of hybrid steganography method. They suggested an approach that uses an extraction algorithm and an embedding algorithm. The embedded method divides the picture into n*n non-overlapping blocks, and then breaks each block down into 4 subbands. After that they use GA (genetic algorithm) algorithm which helps to retain the quality of the image as previous. At last, they use LZW (Lempel Ziv Welch) algorithm for data compression. They use LZW because it compresses all types of data.
   The first row consist of normal iamge and their histogramof the quality of the pictureand in the second row we can see the image with hidden data and their histogram.

2. Verma el al.[5] is used the method for converting the secret data into a set of two digits decimal values. A digit in the set is hidden in RGB cover pixel as each pixel has some bits value, so they modified the pixels digit nearest to pixels value. This method provides higher payload and good imperceptibility. But there is a major drawback seen in this method that is when they change the pixels value nearest to pixels digit the color of the original image will slightly changed.
3. MIT, Cambridge, USA[6], Kevin A. Zhang, Alfredo Cuesta-Infante, and Lei Xu have created an active payload with 4.4 bits per pixel, which is 10x greater than prior methods. The effectiveness of traditional methods is up to 0.4 bits per pixel. Beyond that, it is clearly visible to the naked eye. Even with an image that has been encoded with > 4 bits per pixel, the majority of conventional steganalysis programmes can only discover steganomes with an auROC of 0.6. Steganography, for instance, may be used in medicine to cover up confidential patient data in photographs. such as X-rays or MRIs, as well as biometric information (Srinivasan et al., 2004). (Douglas et al., 2018). in the world of media.

Steganography can be used to regulate content access and embed copyright information (Maheswari & Hemanth, 2015).
Residual connections have been found to increase model stability and convergence in their model, thus we believe that their employment will enhance the steganographic image's quality.
The success of an image steganography project depends on the proper implementation of the chosen technique, as well as the effectiveness of the decoding process used to extract the hidden information. Proper testing and validation of the project should be carried out to ensure that the embedded information is successfully retrieved and that the project meets its goals.

Overall, image steganography is a powerful technique that can be used in a variety of applications, including digital watermarking, secure communication, and data hiding. Its importance in the field of information security and privacy cannot be overstated, and as technology continues to evolve, so too will the techniques and algorithms used in image steganography

Literature Review Summary:-

Author	Origin	Year	Name of the Paper	Theme
Kevin A.Zhang	USA	2019	SteganoGAN: High Capacity Image Steganography with GANs	Neural and deep learning. And Hiding arbitrary data in images using generative adversarial network.
A.H.M. Almawagani	Saudi Arabia	2020	Hybrid Image Steganography Method Using LZW and Genetic Algorithm for Hiding Confidential Data	Hybrid Steganography and Non-overlapping blocks of n*n pixels.
Verma el al	South Africa	2005/2018	An Overview OF IMAGE Steaganography	High degree of redundancy and Audio steganography using masking.

Table 1.1

III. METHODLOGY

The steganography preparation system consists of three parts, the hidden tissue and the revealed tissue. We will put these three parts together to form the ultimate system to hide and reveal hidden images

i. Preparatory system:

Take part in the hidden photo contest. This element has two functions. First, the training method progressively increases the size of the hidden picture to the size of the cover, dispersing the secret image bits across all N N pixels, for nations where the hidden image (size M M) is smaller than the cover image (size N N). The proper encoding of the picture is a more critical objective of all latent image dimensions than converting color-based pixels into more usable characteristics (such as edges).

ii. Hiding system:

produces the Container image using the preparation network's output and the cover image. This mesh receives as its input a N N pixel area that contains the deep composite RGB channels of the overlay picture and the converted channels of the concealed image.

iii. Network Reveal

This is the correct network and image used by the recipient. This is a decoder. This only captures the Container image (not the

cover or hidden image). The decoder system outputs the cover image to reveal the hidden image.

Here we are using Tiny Image net Dataset which consist of 2000 images of measurement 65x65. These images will be used for cover image and secret image. Basically, we will divide there 2000 image into half first half will be used for cover image and second half for secret image.

What we are going to do is that we are going to hide our secret image in a plain sight as our cover image that what steganography stands for.

Very first thing we are going to do is to calculate the total number of pixels of both the cover image and secret image. Once the calculation is done now, we move to the main part where we have to hide our secret image in cover image. For this we will take the pixels of secret image and try to place these pixles between the pixels of cover image. This is our preparatory system.

Once our preparatory system is complete, we move to hiding system where we take the input as the output of preparatory network and concatenate it to RGB channels using a formation of 5 density layer that has 50 layers each and al last we mix all the pixels of cover image and secret image to make it difficult decode without proper process. Up to this step we can say that out secret is hidden successfully.

Lets come to the part where we have to decrypt or reveal the secret image this is where we are going to use our revel system. In this using the cover image container we take the pixels of secret image and try to put it back together. During this process there is loss of pixels due to which our secret image comes out to be blurry and out of colors. But by using our methodology we are going to try to n=make this loss as minimum as possible.

We are going to train our machine to make the loss factor as low as possible by applying a optimized model of hyperparameters. By using this we will make the reconstruction process of secret image loss less. Converting the activation function from relu to tanh makes the optimization system of our model very volatile at high education charges (proven through two strong strains in the plot). After halving the schooling rate, the model begins to perform better in optimization, but it outperforms the model with relu as an activation characteristic.

IV. RESULTS AND OUTPUTS

In this study, we have evaluated the performance of various image steganography algorithm for hiding secret and crucial data within a cover image. We use a dataset of images of different sizes and different pixels, and embedded the secret message of various length into the cover image.

We have study the various algorithm for the image steganography and found that the loss in their cover image is high, so we use some algorithm to minimize the loss of pixel and loss of resolution in the stegano image, so that it looks more realistic.

Our experimental results showed that the algorithm that we have outperformed and in comparison to other algorithm our results are more realistic. The algorithm that we have performed will able to minimize the loss of pixels and resolution. We have taken an input of different pixels and different resolution and found that the results are more realistic than others.

Here is the graph in which we can clearly see that the loss in pixels is too low.

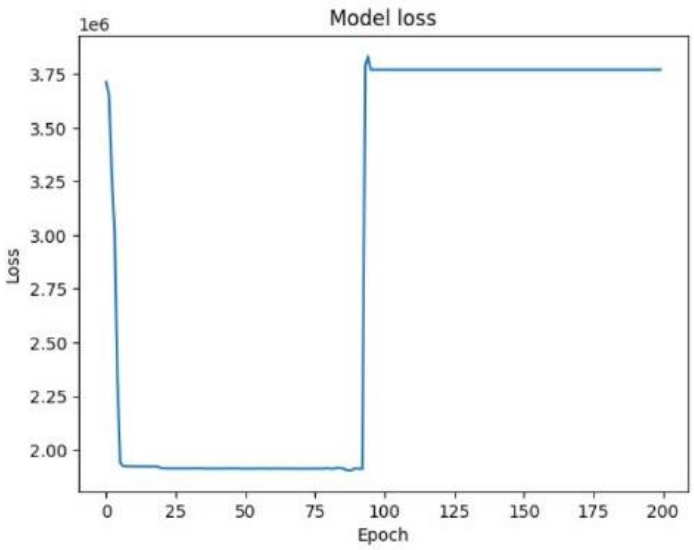

Figure. 1.2

The figure 1.2 represents the graph that was generated by our algorithm which shows that the relation between loss and Epoch.

At the output phase of our model, we have six rows which are as follows:

- Cover image (input image)
- Secret image (input image)
- Encoded cover
- Decoded cover
- The difference between encoded original cover
- The difference between encoded secret and original secret image.

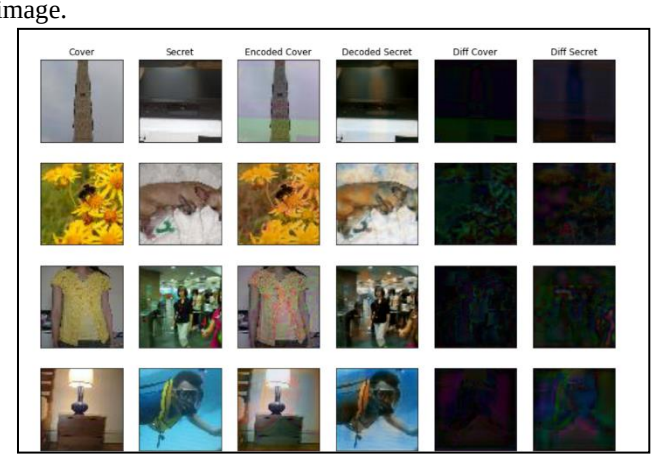

Figure 1.2

Here figure 1.3 represents the final results that our algorithm gives.

After the 300 epochs, we have trained our machine in such a way that secret image is somewhat embedded in the cover image. But still the changes are visible to naked eye. That means we have to increase the epochs for training the data along with some changes in the learning rate.

Learning rate is used as a tuning parameter for optimizing the algorithm so that loss is minimum. Various “lr” used in this algorithm is 0.001, 0.003, 0.005.

We can see that the cover image and secret image and the final result as Encoded cover. After embedding the secret image in cover image the final result is generated which looks like much more simmilar to the cover image.

Overall, our research demonstrate the trade off between capacity , visual, PSNR value and pixels in image steganography, and provide insights for appropriate techniques depending on the specific requirements of the application.

FUTURE SCOPE

The future scope of the project image steganography is promising as there are many new techniques and technologies are emerging year by year which can be applied to improve the security and enhancement of steganography.
Some of the potential areas of development are:

i. Deep Learning Techniques : As deep learning algorithms have been applied to improve the security and robustness of image. In future techniques of deep learning are become more developed and it can help to improve the performance of steganography systems.
ii. Mobile Applications : With the increasing popularity of mobile devices, steganography can be applied to mobile applications to provide more security as compared to now. It provides an additional layer of security to the mobile devices.
iii. Multi-Media Steganography : Steganography can be applied on various forms of multimedia that is on video, audio, and on Image also. In future more techniques and methods are developed to embed these type of files.

There is still more potential for future work in steganography domain. The model which we have researched upon of embedding one image into another, can be further be taken one step ahead with other levels of steganography.

We can develop such algorithms which are resistant o attacks. Also, the amount of information that can be embedded can also be increased to increase the efficiency of security. Steganography has also many other applications such that copyright protection, authentication etc, which could be worked upon.

CONCLUSION

Our results for embedding the hidden picture in the cover image have been optimised utilising image steganography with Python and deep learning. This study demonstrates that picture steganography is a reliable method for maintaining data security. To improve the effectiveness of our model and the clarity of our study, we employed several iterations, Python libraries, and deep learning in our project.

Due to its capacity to stop the transmission of sensitive information, image steganography is a method that has gained a lot of interest in recent years. Without affecting the image's visual quality, the procedure entails masking hidden information in photographs. Since it prevents an attacker from being discovered, this approach is superior to encryption.

Image steganography deals with many issues such as securing confidential messages, maintaining image quality and ensuring messages are deciphered by their recipients. However, various techniques and algorithms have been developed to solve these problems, including least bits (LSB) embedding, spread-spectrum steganography, and adaptive steganography.

Developing powerful steganographic algorithms, increasing the capability and security of steganographic systems, improving the detection and protection of steganographic systems, and evaluating the performance of steganographic systems are the important research objectives of image steganography.

In general, image steganography is an important technique with many applications, including security and law enforcement. With further research and development, it can offer effective solutions for secure communication in many ways.

REFERENCES

I. "AN OVERVIEW OF IMAGE STEGANOGRAPHY," by T. Morkel, J.H.P. Eloff, and M.S. Olivier.
II. "An introduction to steganography methods," by Mehdi Hariri, Ronak Karimi, and Masoud Nosrati.
III. Themrichon Tuithung, Yambem JinaChanu, and Khumanthem Manglem Singh, "Image Steganography and Steganalysis: A Survey."
IV. Lempel Ziv Welch and genetic algorithms are used in this hybrid picture steganography technique to conceal sensitive information.
V. Luo, W., Huang, J., & Qiao, L. (2010). A novel adaptive steganographic algorithm based on syndrome-trellis codes. IEEE Transactions on Information Forensics and Security
VI. Avcibas, I., Memon, N., & Sankur, B. (2011). Steganalysis based on image quality metrics.
VII. Kumar, A., & Sharma, R. (2017). A review on digital image steganography techniques. Procedia Computer Science
VIII. Yadav, R., & Rajpal, N. (2018). A comprehensive review on image steganography techniques. Procedia Computer Science
IX. Chandrakala, S., & Selvi, S. T. (2020). A review on image steganography techniques
X. Singh, S., & Kumar, M. (2021). A survey on image steganography and its techniques
XI. Fridrich, J., Kodovsky, J., & Holub, V. (2012). Rich models for steganalysis of digital images
XII. Das, A., Kundu, M. K., & Das, A. (2012). High capacity data hiding in digital images using reversible texture synthesis
XIII. Zhang, J., Xu, L., & Zhang, X. (2011). A novel reversible data hiding scheme based on SMVQ and modified entropy coding. Signal Processing