International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 06, June 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Data Security on the Cloud usingImage Steganography and Convolution Neural Network

Prof. Jaya M Pattanshetti[1], Pooja Basarikatti[2], Vardafareen Mulla[3], Sneha Patil[4], Mahek Nadaf[5],

[1] *Project Guide, Department of Computer Science and Engineering, S.G. Balekundri Institute of Technology, Belagavi, Karnataka, India*

[2,3,4,5] *Student, Department of Computer Science and Engineering, S.G. Balekundri Institute of Technology, Belagavi, Karnataka, India*

ABSTRACT

Now-moment of truth,Image Steganography is the process of concealing information which maybe text, representation or image inside a cover image. The inside information is hidden in a habit that it not visible to the human eyes.Convolution Neural Network, which has arose as a powerful tool in differing applications containing image steganography, has received raised attention recently. The main aim of this paper search out explore and discuss miscellaneous deep learning designs available in image steganography field. Cloud computing confirmed its importance place it is being used by limited and big arrangements[5]. The importance of cloud computing is on account of the various duties provided apiece cloud. One of these services is storage as a help (SaaS) which admits users to store their dossier in the cloud databases[6]. The drawback of this duty is the security challenge because a third party accomplishes the data.The consumers need to feel secure to store their dossier in the cloud. Consequently, we need for models that will advance the dossier security.

Keywords: *- CNN Steganography, cloud computing, data hiding, data storage, image steganography.*

1. INTRODUCTION

Using deep convolutional neural networks, a full-sized color image is concealed inside another image (called Cover image) with minimum changes in appearance. The hidden image will then be revealed by combining a "reveal" network with the created image. Cloud estimating provides pliable services for users by joining many of resources and uses based on a pay-as-you-need concept [5]. One of the duties provided apiece cloud is store data in the cloud. This service specifies fast distribution, cheap and reliability [5]. When depositing data in cloud storage, depository devices has exposure to internal leakage, hack and other reasons that concede possibility lead to lose dossier confidentiality. Some of dossier stored in the cloud are very delicate data, such as investment and government facts, which must be protected against illegal people containing the cloud service provider. There are many researches that use cryptography methods to protect the cloud secrecy of the data , but the main loss of encryption is although the data is encrypted and enhanced unreadable, it is still survives as a

secret data. The attacker keep decrypt the dossier if he has enough time. Steganography is a way to resolve this problem because it allows the consumer to hide data into added object such as paragraph, image, audio or program, these techniques will increase the delicate data security. In this paper, we devote effort to something the image steganography to defend cloud data.

1.1 IMAGE STEGANOGRAPHY OVERVIEW

This section, provides an overview of image steganography, some techniques of image steganography and types of images. The image steganography is the process of hiding the secret data in a cover image to produce a stego image.

1.1.1 Some of Image Steganography Techniques:

• Least Significant Bit (LSB) based Steganography: Hide the bits of secret data in the LSB of the cover image. This technique is the most popular used.

• Discrete Cosine Transform (DCT): Use subdivision of quantized DCT coefficient to hide the secret data.

• Discrete Wavelet Transform (DWT): It is used to decompress the image mathematically into a set of wavelet. This technique used for medical and military applications.

1.1.2 Types of Images

• The binary images: consists of black and white pixels.

• The grayscale images: consists of pixels with shades of gray colors.

• The color images: uses some integration of red, green and blue to specify the pixels' colors.

1.1.3 Convolution Neural Network Overview

- Convolutional Neural Network is a specialized neural network designed for visual data, such as images & videos. But CNNs also work well for non-image data.
- Its concept is similar to that of a vanilla neural network– It follows the same general principle of forwarding & backward propagation.

1.3 CLOUD COMPUTING OVERVIEW

In this section, we give an overview of the cloud computing, service models, deployment models and security requirements of cloud computing. Cloud computing provides IT services to users over the Internet. The NIST defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort and or service interaction.

1.3.1 Service Model of Cloud Computing

• **Software as a service (SaaS):** User can only use the applications provided by the provider without ability to manage the applications.

• **Platform as a service (PaaS):** User creates applications on the cloud infrastructure and the user will be able to deploy and manage the applications.

• **Infrastructure as a service (IaaS):** User will provide the fundamental computing resources, such as networks, storage and processing.

• **File storage as a service (FSaaS):** The cloud provides the ability to store, manage and access the data froman interface of browser. The cloud provider holds the maintenance responsibility and oversees the infrastructure storage.

1.3.2 Cloud Computing Security Requirements

• **Audit:** It includes authentications and authorization, to ensure user's identity by implementing a strong verification process.

• **Confidentiality:** Protect data stored in the database from unauthorized users.

• **Integrity:** It is used to ensure the data consistency, and to protect data from iteration.

1.3.3 Deployment Model of Cloud Computing

• **Private cloud:**Cloud internet access provider create the possessions and uses usable to cloud consumers. The consumers must authorize get the benefits of the possessions, and they will pay established the consent.

• **Public cloud:** Users use the resources dynamically over the Internet, and they will pay based on their use.

• **Hybrid cloud:**It resides of delivered private clouds connected together and have a main administration. The fee structure in this place model is complex.

2. METHODOLOGY

2.1 Metrics used

Image steganography using CNN models is heavily inspired from the encoder-decoder architecture. Two inputs cover image and the secret image are fed as the input to the encoder to generate the stego image and the stego image is given as input to the decoder to output the embedded secret image. The basic principle is the same except different methods have tried different architectures.

The way the input cover image and the secret image are concatenated are also different in different approaches while the variations in the convolutional layer, pooling layer are expected. The number of filters used, strides, filter size, activation function used and loss function vary from method to method.

One important point to note here is the size of the cover image and the secret image has to be same, so every pixel of the secret image is distributed in the cover image.

2.1.1 PNSR& MSE

Peak Signal to Noise Ratio (PSNR) is used to decide the quality, strength and invisibility of the projected steganography method. PSNR is the percentage between the maximum character representation of the cover concept and the stego figure. In the case of steganalysis, it is the ratio of the maximum kind measurement of the original secret concept and the extracted secret figure. PSNR is used to measure the peak error of the projected method. The advantage of PSNR has to be extreme which indicates that the quality of the reconstructed stego countenance is good. Mean Squared Error (MSE) is another metric to measure the characteristic of the stego

countenance reconstructed. MSE is the cumulative regulated error betwixt the stego image and the original cover concept. For better quality concepts, PSNR has to be extreme whereas the profit of MSE has to be depressed indicating that the mistake is low. The formulas for calculating MSE and PSNR are given beneath.

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (1)$$

place, M and N is the number of rows and columns in the recommendation image individually.

After calculating MSE, its value is used in the calculation of PSNR.

$$PSNR = 10 * log_{10}\frac{(R^2)}{MSE} \qquad (2)$$

2.2 TECHNOLOGIES USED

2.2.1 VB.NET Overview

The VB.NET signifies Visual Basic. Network Enabled Technologies. It is a simple, high-ranking, object-oriented set up language grown by Microsoft in 2002. It is a successor of Visual Basic 6.0, namely implemented on the Microsoft .NET foundation. Furthermore, it supports the OOPs concept, to a degree abstraction, encapsulation, legacy, and polymorphism. Therefore, entirety in the VB.NET language is an object, containing all primitive dossier types (Integer, String, char, long, short, Boolean, etc.), consumer-defined dossier types, events, and so forth objects that inherit from allure base class. It is not a case sensitive language, when in fact, C++, Java, and C# are case impressionable language.

2.2.2 PYTHON Overview

Python is a scheming compute language repeatedly used to build websites and program, mechanize tasks, and conduct file analysis.Python is a general-purpose terminology, meaning it can be used to construct a variety of different programs and isn't specific for any specific questions. This versatility, along with allure beginner-friendliness, live well it one of ultimate-used programming languages contemporary.

3. FIGURE

3.1 Working principle of steganography and steganalysis

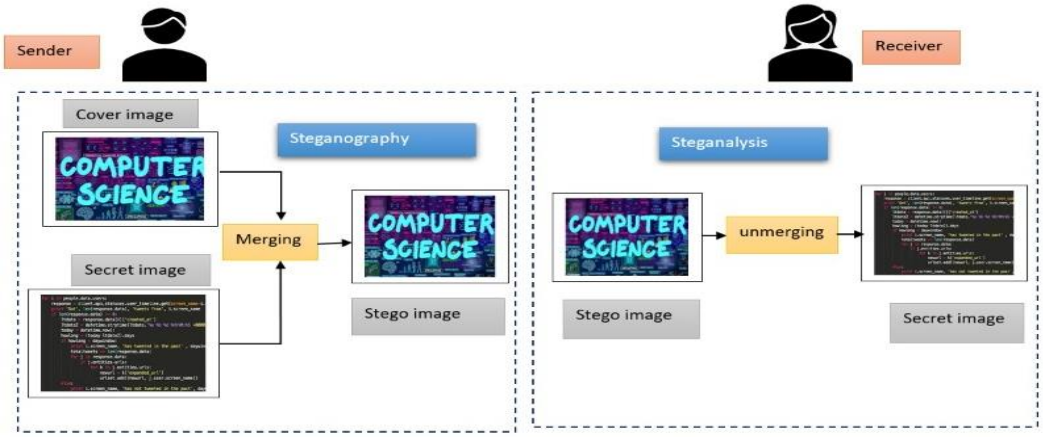

Fig 1: Working principle of steganography and steganalysis

3.2 System Design

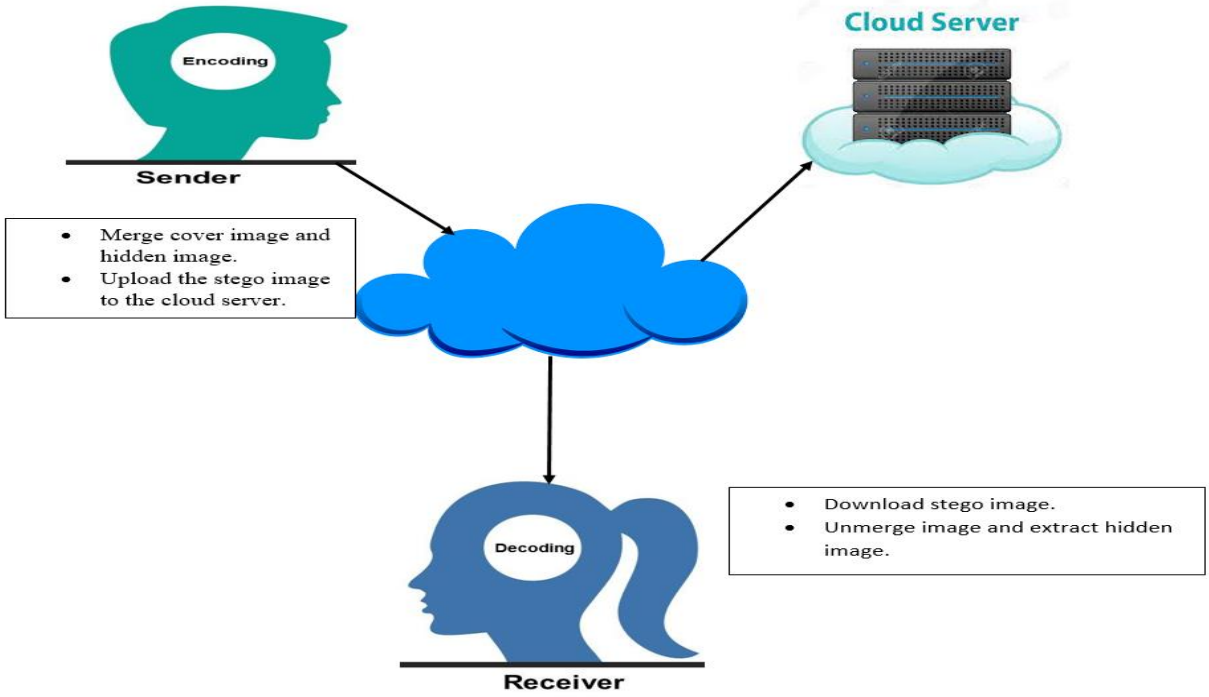

Fig 2: System Design

SENDER Module

- This module is used by the sender user
- It allows user to select cover image & hiding image
- Generates stego image.
- Then stego image is uploaded to cloud server.
- Technologies used: VB.NET & Python.

RECEIVER Module

- This module is used by the receiver user
- It allows user to download stego image from cloud server
- Applies unmerge algorithm of extracts hidden image.
- Technologies used: VB.NET & Python.

CLOUD SERVER MODULE

- The cloud server module acts as a cloud storage to store the stego image.
- It can be accessed from anywhere in the world.

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 06, June 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

3. Results

3.1 Home Page

Fig 3: Home Page

3.2 Merge File

Fig 4: Merged File

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 06, June 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

3.3 Upload File to the Cloud

Fig 5: File uploaded over cloud

3.4 Download Stego image

Fig 6: Download stego image from cloud

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 06, June 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

3.5 Unmerge stego image

Fig 7: Unmerged stego image

3.6 Final Result

Fig 8: Final Ouput

4.CONCLUSION

Cloud calculating supports many benefits to the consumers but it has security challenges. Image steganography is a habit to save secret data in the cloud by conceal the secret data in a cover image. This paper, present a review of few currently projected methods for cloud dossier safety using representation steganography. We distinguished these methods established algorithms they secondhand, advantages and disadvantages, and established the aims of steganography. We decided each method has its own benefits and defect that manage troublesome to select one method as high-quality resolution.

5. ACKNOWLEDGEMENT

It is our proud privilege and duty to acknowledge the kind help and guidance received from several persons in preparation of this Paper. It would not have been possible to prepare this paper in this form without their valuable help, cooperation and guidance. First and the foremost, we wish to record our sincere gratitude to Management of this college and to our beloved Professor, **Dr. B.R. Patagundi**, Principal, S. G. Balekundri Institute of Technology, Belagavi for his constant support and encouragement in preparation of this report and for making available library and laboratory facilities needed to prepare this report. Our sincere thanks are also due to **Dr. B.S. Halakarnimath**. Head, Department of Computer Science and Engineering in S.G.B.I.T and our guide **Jaya M. Pattanshetti**. for the valuable suggestions and guidance through the period of preparation of this paper.

REFERENCES

[1] Wikipedia. (2020). Steganography. [Online]. Available: https://en. wikipedia.org/wiki/Steganography

[2] H. Shi, X.-Y. Zhang, S. Wang, G. Fu, and J. Tang, ‘‘Synchronized detection and recovery of steganography messages with adversarial learning,’’ in Proc. Int. Conf. Comput. Sci. Cham, Switzerland: Springer, 2019, pp. 31–43.

[3] Liu, and X. Wang, ‘‘A novel quantum image steganography algorithm based on exploiting modification direction,’’ Multimedia Tools Appl., vol. 78, no. 7, pp. 7981–8001, Apr. 2019.

[4] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring data security issues and solutions in cloud computing,” Procedia Computer Science, vol. 125, pp. 691–697, 2018.

[5] A. Y. AlKhamese, W. R. Shabana, and I. M. Hanafy, “Data security in cloud computing using steganography: A review,” in 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). IEEE, 2019, pp. 549–558.

[6] Y. AlHumaidan, L. AlAjmi, M. Aljamea, and M. Mahmud, “Analysis of cloud computing security in perspective of saudi arabia,” in 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 2018, pp. 1–4.

[7] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, “A comparative study of recent steganography techniques for multiple image formats,” International Journal of Computer Network and Information Security, vol. 11, no. 1, p. 11, 2019.

[8] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299–326, 2019.

[9] A. Beroual and I. F. Al-Shaikhli, "A review of steganographic methods and techniques," International Journal on Perceptive and Cognitive Computing, vol. 4, no. 1, pp. 1–6, 2018.