

School of Built Environment, Engineering and Computing

Leeds Beckett University

**Applications of** **Steganographic Technique for better cloud security**

By:

Dr. Pooneh Bagheri Zadeh

Submitted to Leeds Beckett University in partial fulfilment of the requirements for the degree of MSc Information Technology

**May, 2023**

# Candidate’s Declaration

I, Steve Tauro, confirm that this dissertation and the work presented in it are my own achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

I have read and understand the penalties associated with Academic Misconduct.

Signed: Steve Tauro

Date: 1st May 2023

Student ID No: 7730129

# Acknowledgements

Many people have played an important role in the compilation of my dissertation, either directly or indirectly.

I am grateful to Dr. Pooneh Bagheri Zadeh for her guidance, feedback and constant support and motivation.

I would like to thank all the researchers who contributed to the field and assisted in expediting my knowledge of the subject.

I would like to extend a heartfelt gratitude Ms. Chaitali Chandwani, who has been a constant source of support and encouragement.

Lastly, I would also like to thank my mother, my father, Ms. Anushka Chiplunkar, and Mr. Raj Dandekar who kept me going through the tumultuous time that was conducting my research and writing my dissertation.

You all continue to be the foundation that guides and encourages me to be my best self and strive for excellence.r

# Abstract

In today’s age of digitalization where more and more individuals as well as businesses store their sensitive data in cloud systems, it is important to ensure that these cloud systems are secure. However, the information technology sector has been witnessing a constant rise in data breaches and cyber-attacks. Though there has been tremendous advancement in cloud services, the industry is still faced with some pressing security problems. Some of these issues include source location, multi-tenancy problems, validation of data obtained and its dependence on the owner, system observing, etc. This calls for implementation of strategies that can enhance cloud security. One such popular technique is steganography. In this research, four steganography techniques (LSB, DCT, PVD, and SST) have been compared with one another on the basis of time taken, CPU utilisation, and image compression in order to determine the most effective technique that helps in enhancing cloud security. It was found the LSB has one of the fastest algorithms, low CPU utilisation, and least image compression, making it an ideal steganography technique.

***Keywords:*** *Cloud computing, Cloud security, Steganography, Least Significant Bit, Discrete Cosine Platform, Pixel Value Differencing, Spread Spectrum Technique.*

Contents

[Candidate’s Declaration ii](#_Toc134436930)

[Acknowledgements iii](#_Toc134436931)

[Abstract iv](#_Toc134436932)

[List of Figures vii](#_Toc134436933)

[List of Tables 8](#_Toc134436934)

[Abbreviations 9](#_Toc134436935)

[Chapter 1: Introduction 10](#_Toc134436936)

[1.1 Overview 10](#_Toc134436937)

[1.2 Rationale 20](#_Toc134436938)

[1.3 Aim and Objectives 21](#_Toc134436939)

[1.4 Outline 23](#_Toc134436940)

[Chapter 2 : Literature Review 24](#_Toc134436941)

[Chapter 3 : Methodology 33](#_Toc134436942)

[3.1 Ethical Considerations 33](#_Toc134436943)

[3.2 About the application 34](#_Toc134436944)

[3.2.1 Basic steganography model 34](#_Toc134436945)

[3.3 Dataset description 40](#_Toc134436946)

[Chapter 4 : Product/Research Design and Implementation 42](#_Toc134436947)

[Chapter 5: Research Outcomes/Results/Discussion and Evaluation 49](#_Toc134436948)

[5.1 Research outcomes and Results 49](#_Toc134436949)

[5.2 Research outcomes/ Discussion 58](#_Toc134436950)

[Chapter 6: Project Management 59](#_Toc134436951)

[Chapter 7: Conclusion and Future Work 60](#_Toc134436952)

[Limitation 60](#_Toc134436953)

[Future Work 61](#_Toc134436954)

[Recommendation 61](#_Toc134436955)

[References 63](#_Toc134436956)

[Appendices 68](#_Toc134436957)

# List of Figures

[Figure 1.1 : Overview  …………………………………………………………….10](#_Toc24785726)

# List of Tables

[Table 1.1 : Data……………………………………………………………………………12](#_Toc24580679)

# Abbreviations

CDMA Code Division Multiple Access

Figure 1

# Chapter 1: Introduction

## 1.1 Overview

**1.1.1 Cloud computing**

With the evolution of technology, there have been various advancements in the field of Information Technology. One such innovation is cloud computing systems. In simple words, a cloud is a system consisting of computers and servers which are accessible globally through the internet. The hardware in this system is usually owned, operated, and monitored by a third party in a manner which integrates one or more data centres (Mirashe and Kalyankar, 2010). Though there is no universally accepted definition of cloud computing, Gens (2008) defines it as “an emerging IT development, deployment and delivery model, enabling real time delivery of products, services and solutions over the Internet (i.e., enabling cloud services).”

**History of cloud computing**

In the late 1960’s, when implementation of the internet brought an advancement in society, McCarthy conducted a seminar at MIT where he quoted “if computers of the kind I have advocated become the computers of the future, then computing may someday be organised as a public utility just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry” (Arora and Bajaj, 2013). After a decade, the growth of the internet was increasing rapidly which resulted in developers to create the first virtualization and multi-processor unit through which programmers could implement different processes in a single machine simultaneously. As an upscaling technology, the users had a major concern as to whether it could satisfy the computational needs at such high value. Therefore, the concept of “renting” was introduced where organisations could purchase or subscribe to the resources at a lower value (Davies, 2004).

The evolution of cloud computing came into notice in 1999 when a company named Salesforce became the first global organisation which provided a cloud-based Consumer Relation Management (CRM) software. This software, based on the “Platform as a Service” (PaaS) such as Microsoft Azure as a platform model, helped businesses to maintain analytical insights of the customers by providing services through a cloud-based application (Surbiryala and Rong, 2019). By 2005, Amazon launched Amazon Web Services (AWS) as an investment to provide a largely distributed IT structure so that it would maintain the growth of the firm (Varia and Mathew, 2014). In 2007, many universities and schools began to avail the services provided by big tech companies like Google and IBM which helped them in reduction of cost and resources shared with students. These services benefited the institutions by constructing a powerful computational platform which can be deployed over the internet (Sultan, 2010). In July 2010, NASA and Racksapce initiated a non-profit organisation collaborating with companies such as IBM, Dell, Microsoft. This organisation focuses on developing an open-source platform where users can contribute their technical abilities to the community. Till date, this organisation integrates more than 100 companies and above 500 developers who managed to release six successful softwares in less than 2 years (Sell, 2019). Soon after, Cloud Security Alliance (CSA) published a paper which helps the cloud providers to implement services in order to meet the basic industry requirement (Orea, 2011).

**Benefits of cloud computing**

The demand for cloud computing services is growing rapidly in the area of distributed computing which leads to an increase of data processing and storage in the community.  There are various advantages of using such technologies which increase the ease of conducting business among other uses in organisations. The National Institute of Standard and Technology has defined five essential benefits for the computing system which are as follows:

* On-Demand Service: These include cloud services that can be delivered to the users at their convenience without the requirement of any authorization. Some examples of on-demand services are web hosting services, storage, network infrastructure, etc.
* Maintainability: Cloud services providers assure less maintenance by the clients of the computerware, including software as well as hardware, as compared to traditional computing methods.
* Collaboration: It aids by creating a platform where developers can collaborate with other developers in order to construct an effective workflow within the organisation.
* High Performance: Owing to the cloud computing technology, users experience a high-performance computing environment such as increased storage, reduced processing time, and enhanced availability of resources.
* Subscription-based Billing: This feature enables the customer to buy the services as per requirement. The user has full control over availing the services whenever they are required and can discontinue them when they are not required. The subscription model has various options such as monthly, quarterly, or annually billing cycle which provides customers with a range of choices.

**Applications of cloud computing**

Since its development, cloud computing systems have been adapted in various fields. Some of its applications are discussed below:

* Cloud computing for e-learning: The use of cloud computing technology in e-learning provides a solution to overcome challenges faced in traditional education. This technology can provide scalability, cost-effectiveness, and flexibility in delivering educational resources and can help improve the interaction between students and teachers. It was found that implementing private clouds for educational institutions can enhance the services and resources by providing services like email, class recordings, surveys, virtual labs, etc. for the students. However, there might be potential challenges faced such as data security, authorization, hardware and software incompatibility etc. (Alshwaier, Youssef and Emam, 2012).

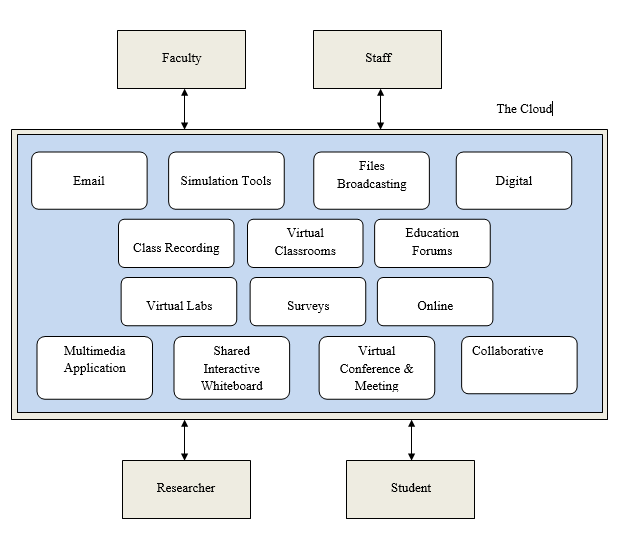


Figure 1.1:  Services provided by cloud in e-learning

* Cloud computing for Enterprise Resource Planning (ERP): Business organisations face challenges in terms of purchasing, installing and maintaining various types of applications. Enterprise Resource Planning (ERP) systems have limitations in terms of user accessibility, availability of resources and performances. ERP cloud is the latest cloud provider service which instals the ERP application on cloud frameworks such as data centres. This enables access to the application anywhere through an internet connection and also reduces the cost of capital and results in a higher Return Of Investment (ROI).

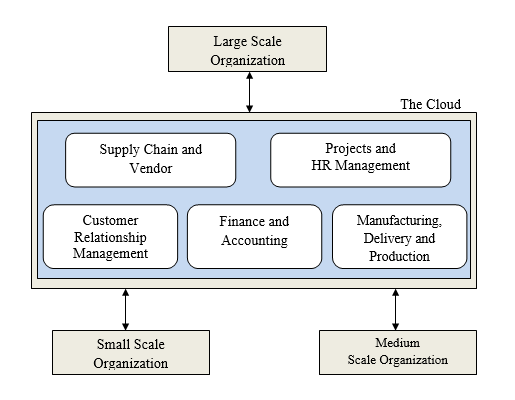


Figure 1.2: Services provide by cloud in ERP

* Cloud computing for E-government: E-Government refers to the use of cloud computing technology to provide government services and resources to the citizens. It offers a pay-as-you-go pricing model which allows the agencies to pay only for the resources they use. It also enables real time data analysis and sharing, which can improve decision making and delivery of services.

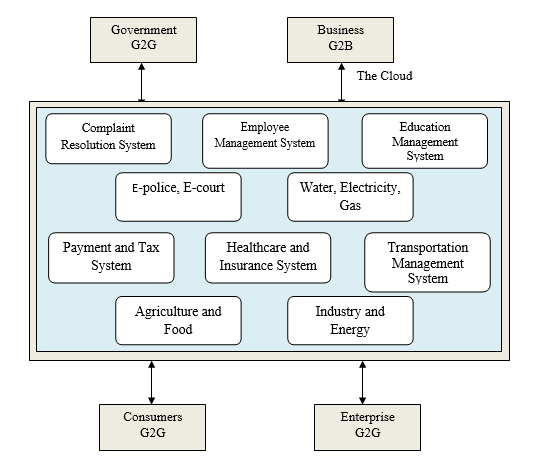


Figure 1.3: Services provided by cloud in Government

**Types of cloud**

The deployment model of cloud computing are segregated as follows:

* Private Cloud: It refers to a cloud infrastructure operational for a single organisation irrespective of whether it is managed by the organisation itself or by a third party. Private clouds are more secure compared to public clouds because the hosting is implemented within the organisation.
* Public Cloud: It refers to cloud infrastructure that is accessible to the general user over the internet
* Hybrid Cloud: It refers to sharing of information by various organisations and supporting a specific community that has shared uses of the system.
* Community Cloud:  This is a collaborative effort between two or more private organisations, often in the same industry, to develop an infrastructure which benefits the firms mutually (Goyal, 2014).

**Types of cloud systems**

* Software as a Service (SaaS): In this model, the responsibility of running and maintaining application and computing resources is handled by the cloud service provider (CSP).  Unlike the traditional software, SaaS benefits the customer in certain ways such as licences, low maintenance and upgrade of software.

Example: Google Maps, Salesforce.

* Platform as a Service (PaaS): PaaS provides a platform for developing, running, managing, configuring the infrastructure.

Example: Windows Azure, Google App engine.

* Infrastructure as Service (IaaS): IaaS provides virtualized computing resources over the internet such as server, storage, and networking.

Example: Amazon Web Services, Dropbox (Joint and Baker, 2011).

**1.1.2 Steganography**

In the modern era, the Internet has become an important source for securing data in the IT sector.  To assure that the data is well protected, an encryption technique was implemented to keep the data confidential. This technique was known as Cryptography, a method which is used to encrypt and decrypt secret messages. As the content of the private message was secured, it was also required to keep the original message as confidential as the secret message. The method which was implemented for this purpose was named Steganography.

Steganography is a method which secures information by hiding it in a multimedia format (Image, Audio, Video). In simple words, steganography is the art of hiding confidential data. The motivation to use steganography is to make sure the data which is embedded into multimedia should be hidden from both user ends (encryption and decryption) to make it difficult for the hackers if it is discovered. The word steganography has its roots in the Greek language, “Stegos” meaning hidden/covered/ or roof, and “Graphia” simply meaning writing (Dickman, 2007).

**History of steganography**

Steganography owes its discovery to a Greek ruler in 440 BC, Histaeus. This was a revolution for Greece where the soldiers had to shave their head, carve the message on their heads, and wait till the growth of hair to ensure the message was hidden. This method involved carving of the head with the help of wax protected wooden slabs. The message was engraved on the wood and a layer of wax was poured to cover it. To receive the message, the receiver had to shave off the soldier’s head in order to decrypt the message. This same procedure was repeated to reply (Silman, 2001).

As time evolved, the technique of steganography brought hope for adapting new methods. During World War II soldiers used to send the message with the help of invisible ink. The message was decrypted only when the receiver had the appropriate chemical compounds in order to reveal the hidden message (Dickman, 2007). In other parts of the world, a French photographer used to send large chunks of messages with the help of pigeons. While Paris was in major attack by the troops in 1870, they used microfilm to send messages via pigeons. This technique led to the invention of microdot. During the world war, microdot was used as a steganographic technique for transmitting messages. In this technique, the message can be in the form of paper or picture which can easily shrink as small as a dot from a pencil. It helped ensure authenticity and security of the message (Siper, Farley and Lombardo, 2005). However, a major drawback of this method was noticed by the countries when it was easy to detect the covered message. A suggested principle was implemented to keep the cover message undetected. It was proposed that a key should be generated between the cover file and original file to make sure the message has not been accessed by the hacker. This key had the functionality of cryptography which maintains the information secured (Lakshmi and Latha, 2013).

**Steganography techniques**

Images have been a strong source for data hiding which was used as the basic principle in steganography. In different domains, images can be of different sizes and formats depending on the application. A suitable algorithm can be used as a steganographic technique for images. The image is specified as a graphical representation in the world of computers.  These images are arranged in a grid pattern with every grid having a point referred to as “pixel (bits)”. A computer inspects these pixels as an array of numbers formed in a two-dimensional structure which represents different intensities of light across the grid.  Each pixel represents binary digits indicating the colour and location arranged in a row by row from left to right to form an image.

As the evolution of steganography made a mark in the world of information technology, the majority of digital files started using different methods of steganography. However, it is only effective if the digital objects have a high degree of redundancy. Redundancy is defined as the object bits that produce a precise rate than the original digital fill in which the user can see and use. Most of the images and audio files imply redundancy for information hidden. The main key of redundancy is that these bits can be changed without any detection of alteration (Morkel et al., 2005). There are 4 types of steganography which are as follows (Ahsan and Kundur, 2002):

* Text Steganography: A technique which allows to hide information in the form of text. This method involves data encoding of each letter of the hidden information.
* Image Steganography: A technique which uses different images as a cover where every pixel is a key to reveal the hidden information in an image.
* Audio Steganography: This refers to a technique in which a secret message is concealed in an audio signal which is modified according to the binary sequence of the audio file.
* Video Steganography: It can also be called as the combination of image and audio steganography where large amounts of information can be hidden. The data can be embedded in two forms such as embedding the data in raw video and compressing it later or embedding the data directly into the compressed data stream.
* Network Protocol: In this technique the message is hidden within the network. TCP/IP (Transmission Control Protocol/Internet Protocol) header packets can be a great example to store the data during the time of transmission.

**Image steganography**

As image steganography is widely used, implementation of the steganography algorithm depends on various cover objects used and various domains employed for embedding or modifying the cover object. Images have a high level of redundancy and can offer increased capacity and resilience to distortion. In image steganography techniques, the hidden text was stored in an image referred to as noise which can be undetectable for Human Visual System (HVS). Data hiding can be a concern because images represented in static form can be subjected to a range of manipulation, which can lead to non-linear operations such cropping, blurring, filtering and compression that can impact on the result of loss of data (Bender et al., 1996). For the purpose of this research, image steganography will be the chosen method to assess its effect on cloud computing security.

**Domain structures**

The most common and widely used domains for image steganography are as follows:

* Spatial Domain: This domain represents a two-dimensional matrix where the secret information is embedded at the pixel level. The manipulation of the image is applied by modifying the pixel value and encrypting the secret message. Since the Human Visual System (HVS) cannot detect the changes of pixels, the domain can be used to hide the message without being noticed. This technique includes operations such as colour values, modifying the pixel location, and adjusting the intensities of the light on the grid. Least Significant Bit (LSB) is the most common technique to encode the message once modification of the pixel is successfully altered.
* Transform domain: This domain presents a mathematical transformation of the image from its original spatial domain to a different domain such as a frequency domain or wavelet domain. Transformation of the image can be performed on the basis of transformed coefficient to apply the secret message. Comparatively, the Wavelet domain can also be applied to decompose the image into different frequency sub-bands. The highest frequency band can be altered to encode the secret data, as it will be undetectable for human vision. As it requires more computational resources and knowledge to extract the data from the modified coefficient, Discrete cosine transform (DCT) and Discrete Fourier transform (DFT) can transform the image into frequency components (Chedda et al., 2010).

Steganography is a process in which information and data is hidden in multimedia files like images, texts, audios, and videos. It embeds secret data using specific algorithms which are then decoded at the end of the receiver. The following steganography techniques will be employed for the purpose of this research:

1. Least Significant Bit (LSB)

LSB is the most widely used steganography technique and also the most difficult. It is an insertion technique used in image steganography to hide a secret message within an image file. It works by replacing the least significant bit of the pixel value in the image with a bit from the secret message. This involves masking, filtering, and transforming. It works on the principle of replacing the Least Significant Bits (LSB) of the cover image with the Most Significant Bits (MSB) of the information that is to be hidden without significantly hampering the properties of the cover image (Raja et al., 2006).

2. Discrete Cosine Transformation (DCT)

DCT is a steganography technique which implements breaking of image into 8x8 block of pixel. After breaking down the image, a general equation is added to the multidimensional block which executes the equation from left to right and top to bottom. DCT converts the image into a frequency which is divided into regions such as High Frequency (FH), Low Frequency (FL), Middle Frequency (FM).

3. Pixel Value Differencing (PVD)

In this steganography technique, information is hidden within digital images. It is mostly performed in the spatial domain. Essentially, PVD modifies the least significant bit (LSB) of each pixel in the image on the basis of the difference between the current and neighbouring pixel value. After calculating the difference between each pixel and its adjacent pixel, if the value surpasses a predefined threshold value, the LSB of the pixel is transformed to encode a part of the secret message. If the value is lesser than the threshold value, the LSB of the pixel remains unaltered (Fridrich et al., 2001). Though it is a simple and effective technique, it is vulnerable to attacks such as those involving statistical analysis of the data in the image. Additionally, if a large amount of bits are encoded, it may result in noticeable visual artefacts i.e. it has a low embedding capacity (Luo et al., 2011).

4. Spread Spectrum Steganography (SSS)

This steganography technique spreads information over a broad frequency range in order to hide information within digital signals. It uses a spreading code to embed the secret information into the host signal. This host signal can be a digital image, audio, or video. In this technique, first the secret message is converted into a binary sequence. Then, the sequence is multiplied with a pseudorandom spreading code, resulting in its spread over a wide frequency range. This spread signal is then added to the host signal. The host signal may contain interference in various forms such as noise. The same spreading code which is used to embed the secret message is deployed to despread the signal in order to decode the secret message from the spread signal. To extract the secret message, the despread signal is processed (Marvel et al., 1999).

## 1.2 Rationale

In today’s age of digitalization where more and more individuals as well as businesses store their sensitive data in cloud systems, it is important to ensure that these cloud systems are secure. However, the information technology sector has been witnessing a constant rise in data breaches and cyber-attacks. Though there has been tremendous advancement in cloud services, the industry is still faced with some pressing security problems. Some of these issues include source location, multi-tenancy problems, validation of data obtained and its dependence on the owner, system observing, etc. This calls for implementation of strategies that can enhance cloud security. One such popular technique is steganography. Previous research has shown that steganography techniques have been useful in providing extra security to cloud computing systems (Singla and Bala, 2018). However, there is still ambiguity over which steganography technique is the most effective in preventing attacks on cloud systems. Majority of existing literature focuses on the integration of cryptography and steganography techniques which poses limitations in terms of availability, costs, complexity, and time (Adee and Mouratidis, 2022). This paper aims to identify the most efficacious steganography technique which successfully adds extra layers of security in cloud systems. By doing so, the researcher also aims to contribute to identifying the strengths and weaknesses of various steganography techniques in order to have a better understanding of how they can ameliorate performance. Essentially, this study will aid in the development of measures that are effective in enhancing the security of cloud computing systems along with a reduction in the risks synonymous with data breaches and cyber-attacks. Additionally, it will provide helpful insights for individuals and businesses that rely on cloud systems for storing confidential data.

## 1.3 Aim and Objectives

**Aim**

The purpose of this project is to investigate the uses of steganographic methods for the improvement of cloud security and to construct a Convolutional Neural Network (CNN) based model in Python for the efficient discovery of information that is concealed inside cloud data.

**Objective**

* To conduct an in-depth review of the literature on steganography and cloud security, to understand the key concepts and techniques involved.
* To identify the potential applications of steganography in enhancing cloud security, such as secure data transfer, secure storage, and secure sharing of data.
* To design and implement a steganographic technique in Python, for embedding secret data into cloud data without affecting its integrity and confidentiality.
* To develop a Convolutional Neural Network (CNN) based model in Python for effective detection of hidden information within cloud data, using various steganographic techniques.

**Research question**

Which steganography technique is the most useful and efficient in reducing attacks on cloud system security?

**Research objectives**

1. To conduct a thorough literature review to identify potential research gaps in research revolving around the use of steganography techniques to improve cloud security
2. To determine the weaknesses in the security of cloud computing systems
3. To identify the current trends in steganography techniques that can be used to enhance cloud security
4. To perform a comparative analysis of steganography techniques in order to ascertain which technique is the most effective in preventing attacks on cloud systems

The present research aims to identify the contribution of steganography on security in cloud computing systems. Thereafter, it will determine which steganography technique is the most effective in enhancing the security of cloud computing systems. It also aims to contribute to the field by providing recommendations to overcome the present problems in the area.

## 1.4 Outline

The research is organised according to the following structure:

Chapter 1 of the report provides an overview of the research including the introduction, rationale, and research aims and objectives.

Chapter 2 comprises a thorough review of the pre-existing literature on cloud computing and steganography techniques being used in this research. It also summarises related work.

Chapter 3 of this dissertation report includes the methodology.

Chapter 4 provides a brief explanation of the application developed to conduct the research and its implementation in the context of this study.

Chapter 5 reports the findings and results of the research.

Chapter 6 provides a timeline of the project.

And finally, chapter 7 imparts a conclusion along with the scope of future work that can be done in the field.

# Chapter 2 : Literature Review

Though the innovation of cloud computing systems brought about a revolution in the field integrating IT services and the business sectors, it poses significant security issues from various perspectives including stakeholders, architecture, characteristics, etc. (Almorsy et al., 2016).  Cloud Security refers to the risk and vulnerabilities associated with storing and processing the data in the cloud. It is a part of computer security and encompasses a set of technologies, policies, and control methods which assist in protecting the data in the cloud and the services that it provides. The fact that cloud systems provide various benefits like flexible access to data, omnipresence of data, and resilience allows cloud providers to allocate their funds in improving security (Ryan, 2013). But due to the nature of the system itself, when the data is uploaded onto the cloud it is inevitably put out of reach of the clients, leading to the rise of significant security issues. Singh and Chatterjee (2017) identified the following challenges that are currently faced by the cloud industry:

This brings many advantages, including data ubiquity, flexibility of access, and resilience.

1. Problems regarding security of stored data and computing

Data is central to any cloud computing service. After the data is in the cloud, the clients are unaware of what happens to it, making it isolated and inscrutable to them. This problem is evident in two situations i.e. before the data is computed and after the data is computed.

* Issues with data storage: A critical issue that occurs is the confidentiality of data stored in the cloud servers by the clients. For example, big companies like Google and Amazon have physical servers located in various countries and they store the data based on a feature called multi-location which causes security and legal problems because different countries have different policies.
* Un-trusted computing: The overarching aim of many security services is to provide a front end interface for SaaS applications when users request a web service. These applications adapt and change according to the pattern of usage and behaviour displayed by the user. Such computing frameworks may produce unwanted, false, or inaccurate results caused by malicious or misconfigured servers.
* Availability of data and services: Though cloud resources and services are highly available, both virtual and physical, they require changes to be made at the application as well as infrastructural level. A potential solution to this is multiple alive servers supporting the applications, however, this makes the cloud system vulnerable to Denial-of-Service (DoS) attacks. Such attacks involve flooding the target system or application with information, or sending information triggering an attack, resulting in the user being shut out of their network or machine. Partial or complete failure of the system and availability of services and data may result from even a single fault in the cloud system environment. Additionally, cloud outages may be the resultant of unavailability of hardware resources. Such problems can cause immense distress to the business availing the cloud services.
* Cryptography: This mechanism is deployed to secure the information stored in cloud systems. It involves converting plain text into cipher text. However, if the algorithm is implemented in an ineffectual manner or uses a weak key during the encryption process, it makes the data susceptible to attacks, for example, brute force attacks.
* Recycling of cloud data: It is essential for the cloud service providers to sanitise the cloud space once data has been utilised and deleted by the user. Improper sanitization can lead to data leaks and losses.
* Malware: Malware has the ability to harm cloud services and devices by deleting or corrupting data stored in the cloud. It spreads to all other files which are synchronised with the file containing the malware.

1. Problems with security of virtualization

A major factor which has contributed to the widespread adoption of cloud technology in the business industry is the virtualization of services. Though it contributes positively by reducing costs and increasing profit, it is still vulnerable to threats and attacks.

* Image management in virtual machines: Features like elasticity and service orientation create a dynamic and volatile environment for the users to create, modify, and copy virtual machine (VM) images and even allows for the usage of previously created images. This poses severe security problems, for example, a malicious user has the ability to upload corrupted images in the repository containing malware, or can even find possible attack points by finding the codes of images. Improper management of VM images can result in breach of confidentiality of users, VM sprawls, or wastage of resources.
* Virtualization of networks: Attackers can access sensitive information of the clients or network providers as virtualization of networks paves the way for limited administrative access to the cloud and network tailoring caused by instability in network characteristics, abnormal packet delays, and unstable OSI layers. It also leads to other security issues like spoofing, packet sniffing, and network based VM attacks.
* Mobility: The process of copying or moving a VM to other servers is known as VM cloning or template image cloning. This process can lead to multiple errors in security like misconfiguration as the mobility of VM aids for quick development of VM images, hampering the process of transferring and increasing deployment time.

1. Security issues related to internet and services

Along with services and resources, the cloud infrastructure requires a carrier to transmit data between senders and receivers. This carrier is the internet. In the form of digital data, the internet transmits a large number of data packets from the source to the destination passing through a number of nodes, making it unsafe for the end users.

* Venomous outsiders and Advanced Repeated Threats (ARTs): ART refers to an attack model with consists of the three phases i.e. information gathering via public or private intelligence sources aka Open Source Intelligence (OSINT) gathering phase, threats modelling phase, and finally, the attack phase. Hence, it is important for businesses to keep essential information private and keep a tab on what type of information and how much of it is provided publicly.
* Web services: Data integrity is a critical problem in a distributed system. The Service Oriented Architecture (SOA) provides a solution to maintain integrity of data in clouds. Extensible Markup Language (XML) and Application Programming Interface (API) are used to improve functionality of clouds. However, APIs do not provide any transactional reports which can exacerbate data integrity issues.
* Availability of safe web services: Majority of cloud services are accessed via web based agents like web browsers. There are vulnerabilities like malicious web links and websites which constantly increase the malware in cloud systems, therefore, attracting attackers to attack vectors.

1. Security issues in networks

Networks are fundamental to cloud computing systems; hence, network level issues have a direct negative impact on cloud environments. Due to the dynamic nature of cloud networks, these issues are considered internal as well as external. DoS attacks on networks do not only affect the availability of the services but also affects the bandwidth of networks and can cause congestion in networks. Network security issues lead to vulnerabilities through mobile platforms and circumference security.

1. Problems with access control

Protection from unauthorised permissions is called access control security. A combination of an e-mail address or username and password is used to authenticate the identity of users in order to maintain access security in order to prevent attacks via web technologies or websites. This includes physical access, user credentials, authorization, authentication of entities, management of user identities, and anonymization.

1. Problems regarding software security

A major concern in the present day is that of software security. This is because of the wide array of programming languages available. Cloud computing systems are composed of thousands and millions of lines of code. Due to this, there is a lack of a single universally accepted system to measure the levels of security in cloud systems. Security issues can arise by a single bug in the code, which can occur at a framework level as well as user interface level.

1. Problems with management of trust

A relationship built on trust is essential between the client and the cloud service provider. It acts as a basis to access various resources and services such as storage, web-based access, visualisation mechanisms, and computational algorithms. Trust is also imperative in peer-to-peer networks, sensor networks, and distributed networks. Therefore, it is important that the human aspect be emphasised while handling security.

1. Problems regarding compliance and legal issues

An essential document in the cloud-business model is the Service Level Agreement (SLA). It is signed by both parties i.e. the client and the service provider, and it outlines the services or resources which will be delivered, the terms and conditions of usage, the metrics by which effectiveness of the processes for monitoring, etc.

* Digital forensics: The recent years have witnessed a boom in the field of digital forensics which are used to audit tasks in cloud computing with an overarching aim of identifying potential threats. Issues arise when resources cannot be located and isolated, called data locality issues. Seizing of data and disclosure of data can compromise the privacy and confidentiality of clients.
* Legal problems and cyber laws: Cyber laws are backdated and also may potentially breach the confidentiality and privacy of users as these cyber laws do not provide complete security to cloud systems. As the physical servers used by cloud systems are located in different countries all around the globe, the laws are not universal and change from country to country. This can lead to breaches in the SLA and nonconformity on the part of providers due to the feature of data migration.

Steganography has been found to be a useful tool by many researchers which enables covert transmission of information through overt communication channels. It combines encryption methods with cryptography techniques which allows for the user to send information hidden inside a multimedia file in plain view. When combined with pre-existing encryption algorithms, the hidden data becomes difficult to detect as well as decipher (Dickman, 2007). Current researches have proven that cloud security can be enhanced using a combination of methods like steganography, encryption and decryption techniques, compression and splitting techniques, digital signature algorithm, data encryption standard algorithm, etc. in order to bypass the limitations of previously used traditional data protection methods (Awadh et al., 2019). It has also been found that steganography techniques can be employed without the interference of a third party (Ahmed and Abduallah, 2017).

One of the most widely used steganography techniques is Least Significant Bit (LSB). This technique involves encoding a secret message within the least significant bits of a multimedia file in image or audio format. As the least significant bits of a digital file represent the least important information of the file, altering them to encode the message does not have a significant effect on the overall quality of the file. LSB has been used in various areas such as digital forensics, military communications, medical imaging, etc. It was found that LSB has several advantages like it minimises the error rate in the process of embedding the secret message and that it has greater criterion reliability (Rahman et al., 2022). It has a high capacity of carrying information and is a simple method to implement (Goli and Naghsh, 2016). Additionally, the information can be retrieved without any loss of quality of the media file (Ali et al., 2020). However, despite its advantages, it also has certain limitations. LSB was also found to be vulnerable to attacks, for example, compression, cropping, and salt and pepper noise (Goli and Naghsh, 2016). Another challenge is that the storage capacity of the LSBs may not be enough to hide large amounts of confidential information. Unauthorised users may also be able to detect secret messages which jeopardises the confidentiality of the data (Cheddad et al., 2010).

Another popular steganography technique is Discrete Cosine Transform (DCT) which works on the principle of modifying the coefficients of an image's frequency domain in order to embed secret data. The least significant coefficients are modified to ensure that data is hidden while ensuring minimal damage to the quality of the digital file. It also involves applying a secret key in the process of encoding and decoding the secret message from the image. This key controls the positions of the coefficients that have been altered (Patel and Dave, 2012). Over the years, studies have found DCT to be an effective and reliable steganography technique which can be used to transmit information confidentially. A study in which DCT was implemented in different image formats like JPEG, PNG, and BMP, it was found that the technique is effective in embedding secret messages while maintaining the integrity of the original images (Zhang et al., 2019). Another study analysed DCT on the basis of data hiding capacity, image fidelity, and security. The results indicated that DCT was more effective than other steganography techniques (Wang et al., 2017). At the same time, DCT has its limitations. It was found that DCT steganography is susceptible to attacks like histogram analyses which aids in the detection of hidden information. Also, DCT is a time taking and computationally intensive procedure (Zhu et al., 2021).

Another established steganography technique is Pixel Value Differentiation which involves modifying the pixels surrounding those pixels holding the least value based on the difference of values between the pixels in order to embed secret messages. A secret key, which controls the positions of the pixels that have been altered, is required in order to encode and decode the message. The modification is done in a manner which is undetectable to the human eye. Studies have shown that PVD is preferred over LSB as the process of embedding is smoother in PVD steganography. A major advantage of this technique is the imperceptibility of the modification of the image. However, at the same time, this method lacks security, for example, it is susceptible to histogram analyses which can lead to the detection of secret messages in the altered images (Kadhim et al., 2019). To overcome these weaknesses, modified versions of PVD were also introduced such as Adaptive PVD, a combination of PVD and LSB, improved rightmost digit replacement (iRMDR) and parity-bit pixel value difference (PBPVD), etc. (Hussain et al., 2017).

Coming to the last well known steganography technique known as Spread Spectrum Technique. It is a technique which involves the data to be hidden within a digital signal. This technique makes it difficult to detect the secret information. An application was deployed where the technique generates a key to encrypt the secret message before embedding it in the image. The advantage of the key is to decode the message from the image. The system proposed by the research was to divide the message into small blocks. These blocks use a pseudo random sequence to select specific blocks to embed the secret data. The messages are spread all over the signal so that the authorised users have access to decode the information. Digital signature can be great example authentication for verifying the integrity of the watermarked image  and copyright protection (Zhelezov and Kordov, 2020).

Steganography has been found to be the most effective technique to enhance the security of cloud computing systems. This is because it makes it difficult for attackers to breach confidentiality and compromise the integrity and authenticity of data. Discussed below are the characteristics of steganography techniques which aid in improving cloud security (AlKhamese et al., 2019; Ahmed and Abdullah, 2017):

1. Confidentiality - It can prevent unauthorised access to attackers by embedding confidential information in multimedia files, hence, concealing sensitive data.
2. Integrity - Checksums or digital signatures can be integrated within data files which maintain the integrity of data stored in the cloud systems. By doing so, cloud providers can ensure that the data has not been tampered with in the process of transmission or storage.
3. Authentication - Cloud service providers can also use steganography techniques to demonstrate authenticity and veracity of the data being stored in their system. They can also detect any alterations. This is done by embedding digital signatures like watermarks into the files.
4. Detecting unauthorised access - Steganography techniques can be employed to embed “triggers' ' in the form of data in files that alert the administration of cloud service providers if the files are accessed without authorisation and authentication. This enables cloud service providers to take immediate preventive or corrective actions in case of a security breach.

However, there is ambiguity over the efficacy of different techniques of steganography and their usage in different scenarios relating to cloud computing. Furthermore, present literature outlines various limitations like the fact that current techniques and schemes are only able to tackle a limited number of security issues which arise in cloud computing environments and that too in a small environment. The aim of this research is to identify the most effective steganography technique which can be used to enhance cloud computing security. Additionally, recommendations will be provided on the basis of the findings in order to bring improvement in steganography and encryption-decryption techniques on a large scale to solve multiple security problems in a wider environment.

# Chapter 3 : Methodology

The main aim of this chapter is to present the description of the research methods used in this study.

## 3.1 Ethical Considerations

The applications of steganographic procedures for better cloud security raise a few moral contemplations. Here is a portion of the key moral contemplations that are taken to be considered.

**Privacy**

The utilization of steganography should be visible as an infringement of security, as it includes concealing data without the information or assent of the picture proprietor. There might be worries that steganography could be utilized to cover delicate information, like individual or monetary data, and possibly lead to security infringement.

**Security**

The utilization of steganography can likewise have security suggestions, as it very well may be utilized to conceal vindictive code or different sorts of malware. The likely abuse of steganography to stow away malware could prompt security breaks or digital assaults, which can have sweeping ramifications for people and associations.

**Legal considerations**

The utilization of steganography might be unlawful in specific settings, for example, when used to conceal data is dependent upon lawful or administrative prerequisites. In this way, considering the lawful ramifications of involving steganography in some random context is significant.

**Moral contemplations in research**

Specialists involving steganography in their examinations ought to think about the likely moral ramifications of their work, like the chance of hurting people or associations. They ought to guarantee that they have acquired the essential endorsements and authorizations prior to directing their examination.

**Transparency**

It is vital to be straightforward about the utilization of steganography, especially in situations where it is being utilized for security purposes. Straightforwardness assists with building trust and guarantees that clients know about the possible dangers and advantages related to steganography.

while steganography can be a valuable instrument for better cloud security, it is vital to consider the moral ramifications and potential dangers related to its utilization. It is fundamental to guaranty

that steganography is utilized in a moral and dependable way and that proper shields are set up to safeguard the protection and security of people and associations.

## 3.2 About the application

## 3.2.1 Basic steganography model

With the rise in information security risks, image steganography has become an important technique for data transmission as it guarantees the secrecy, security, and confidentiality of the information. Explained below is how steganography simply works:

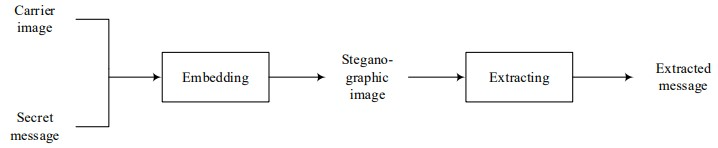


Figure 3.1: Basic Steganography model

There are two major steps which ensure the confidentiality of the information. They are as follows:

* Embedding:The process of hiding a secret message into the carrier image.
* Extracting**:** The process of accessing the information from the encoded steganographic image.

**3.2.2 Application**

After a thorough analysis of the present literature on the different approaches for image steganography, an application was developed to understand and analyse which steganography technique is most suitable for data hiding. In this study, four methods have been implemented to assess the efficiency of the steganography technique with respect to data security. They are as follows:

**Least Significant Bit (LSB)**

This algorithm is categorised into two scripts i.e. LSB\_Encoding and LSB\_Dedcoding.

1. LSB\_Encoding: This script defines a function called “encode\_image” which takes an image and a secret message as an input parameter. The function encodes the secret message into the image by converting the messages into bytes, checking the size of the messages, converting the message from bytes to binary, and embedding the binary message into the image. Once all the conditions are satisfied the function returns the encoded image.

The algorithm requires importing of necessary python libraries which provides access for the functions. These libraries are hosted by the python interpreter. They are as follows:

* SYS: This module is used to interact with the python environment. It grants access to various variables and functions to maintain and manage the arguments accessed through the command line by the interpreter.
* PSUTIL: Process and system utility is a cross platform library which is used for monitoring the system and utilisation of the resource. For the purpose of this research, the application retrieved information on the running processes and gathered information such as CPU utilisation, time taken to encode the message, and file size after and before compression.
* PIL:Python Image Library enables the interpreter to deal with images.

Once all the necessary libraries had been imported, “time” and “image” modules were imported from the python image library. The “time” provides functions related to time and functions to analyse the time taken to encode the secret message. Once the secret message is embedded into the carrier image, the image converts into RGB colour space by implementing the “convert” method. It converts the steganography file and stores it in “.jpeg” format in the same directory where the encoded message is saved. Finally, the algorithm calculates the parameters in order to analyse this technique.

1. LSB\_Decoding: This script describes a function called “decode\_image” which fetches the file path of the image and returns the hidden message encoded in the image. This function opens the encoded image and converts into an RGB format.  Image function extracts the least significant bit of each pixel to reconstruct the binary message after extraction of the image into a binary format. Character Detection which is also known as “chardet()”, this package helps to detect the hidden text and extracts the encoded message  from the steganography image.

* Discrete Cosine Transform (DCT):

This algorithm is categorised into two scripts i.e. Endcode\_DCT and Decode\_DCT.

1. **Encode\_DCT:** This technique uses two arguments; the first argument is the path file for the cover image, and the second argument is the secret message encoding. In this study, “cv2.dct()” function was implemented to perform the arguments. The secret message was converted to binary using ASCII encoding. Meanwhile, the carrier image was converted to grayscale image. The function was implemented using 8X8 block grid structure. The image was allocated a block  by calculating the height, width of the image. Thereafter, the secret message was embedded in a sequential manner. To fetch the steganography image, inverse DCT function was applied to the modified DCT using “cv2.idct()” function. Predefined libraries were accessed from the python interpreter. They are as follow:

* **SYS:** This library grants permission to maintain the variable and performance of  the function “cv2.dct()”
* **CV2:** It is known as the OpenCV library which performs computer vision tasks and aids in image processing.
* **PSUTIL:** This is a hybrid library which retrieves the data from the process and system.
* **Time:** Provides time related functions.
* **Numpy:** It is a predefined library which solves large and complex matrices and arrays with the help of high level mathematical functions.

1. **Decode\_DCT:** For retrieving the steganographic image, the image was formatted to grayscale by using the “cv2.cvtColor()” function. The converted image performs a DCT function where the image were converted from frequency domain to spatial domain by passing the “cv2.dct()” function. The secret message was retrieved by analysing each block on the basis of the height and width of the block using array slicing. After converting the messages into bits, “str()” was implemented to convert the bits into binary. Hence, the “chr()” function was used to extract the secret message from the binary message. The libraries that were used for the “encode\_dct” step were used for this step as well.

* Spread Spectrum Technique: This algorithm is categorised into two scripts i.e. SST\_Encoding and SST\_Dedcoding.

1. SST\_Endcoding: A function known as “embed\_sst”  is implemented which plays an important role in encoding procedures. This function is used to find the image path, the secret message, and embeds two parameters i.e. “alpha” and “beta”. This function was implemented to find the strength of embedding the secret message into the carrier image. The code uses a function “str2bits” which enables a string message as input and returns a binary string message of 0’s and 1’s. The strength was calculated by a threshold value based on the “alpha” parameter. “Embed\_coeffs” is an array which was implemented for storing the strength values. Initially, the value was set to zero using the “np.zeros\_like” function which sorts the values in an ascending order using the “np.sort” function and compares it with a formula which involves the parameter of beta. After calculating the strength, it embeds the secret message into the cover image using a technique called spread spectrum steganography. Libraries implemented for the working of this technique are as follow:

* “Sys” was imported to maintain and manage variables and methods for the function “embedd\_sst”.
* “Psutil” was imported to measure and monitor functions such as CPU utilisation, processing time, etc.
* “Numpy” was imported to perform the numerical operations on array.
* “Scipy.fftpack” was imported to perform an important mathematical expression of fourier transformation.
* “PIL.image” was imported to handle complex procedures of image processing.

Thus, after the completion of implementing the function and libraries, the stego image was stored in a local database labelled as “encoded.jpeg”. A report was also generated on the basis of CPU utilisation, file compression, and time taken.

1. SST\_Decoding: A function was implemented known as “extract\_sst” which passes three parameters: “stego\_image\_path”, “alpha”, “beta”.  Alpha is an integer representing the number of DCT coefficients which was used for embedding messages. Beta is a scaling factor to detect the embedding strength of the array. DCT computes the images in rows and columns by implementing “T” which is known as “threshold” to transpose the array. In this study, the secret message was extracted from the image by iterating over 8X8 clocks of the “embed\_coeffs” array.  The messages were computed and examined in such a way that the bits were linked with the binary string named “secret\_msg\_bin”. The binary string message was converted using the “char” function to store the secret message. After the completion of the function, the message was extracted from the stego image. The extraction of the message was printed on the basis of alpha and beta where the value was set to “1000” and “0.01” with respect to the image path**.**

* Pixel Value Differencing (PVD):  This algorithm is categorised into two scripts i.e Encode\_PVD and Decode\_PVD.

1. Encode\_pvd:  This script performs a function known as “encode” where two arguments are implemented; the path of an image file and a secret message to be hidden within the image. “PIL” Python Image library was  used to load the image and obtain the dimension of the image with respect to height and width. For embedding the secret message, Format() function was implemented to convert it into a binary format which was stored in a variable named “binary message”. This function checks the length of the message and employs a parameter which checks the length of the binary message and pixels of the image. Meanwhile, it performs an if-else statement which checks each block from top to bottom positioning with respect to (0,0). If the condition is found to be true, the message will be encoded. If the condition executes a large value as compared to the pixel value, it passes a ValueError which does not allow the message to be encoded. The modified image is then stored with the original filename\_encoded.jpeg. Predefined libraries were accessed from the python interpreter. They are as follow:

* SYS: This library was imported to maintain and manage variables and methods for the function “encode\_pvd”.
* CV2: It is also known as the OpenCV library which performs computer vision tasks and image processing.
* Numpy: It is a predefined library which solves large and complex matrices and arrays with the help of high level mathematical functions.
* Pywt: It is also known as PyWavelets which is a mathematical technique that allows signals and images to be broken into different frequency components to support multi-level reconstruction of images.

**Decode\_pvd**: The predefined libraries used in the “encode\_pvd” step were used in this step as well. “Extract\_text\_from\_image” function was used which hides text based on high frequency bands. These bands contain detailed information about the image and the message. This function was performed in a loop to extract the least significant bit (LSB) from a “binary\_text”. The loop terminates only if the eighth consecutive LSB is equal to 1. As a part of extraction, “chr()” function was implemented to convert the binary\_text to ASCII characters. In the end, the functions return the embedded secret message.

**Basis of analysis**

The identification of the most suitable technique was analysed on the basis of the following technical parameters:

* **CPU Utilisation**: Central Processing Unit Utilisation refers to the amount of resources  utilised to execute a task or processing of  the data.
* **Time**: It refers to the amount of time taken to encode and decode the message from the image.
* **Image Compression**: Image Compression refers to redundancy of the size of image and protecting the essential information to be hidden inside the image.

## 3.3 Dataset description

This dataset is a collection of 44,000 512x512 pixels pictures that are installed with various sorts of noxious payloads utilizing the Most un-Huge Piece (LSB) method. The payloads incorporate JavaScript, HTML, PowerShell, URLs, and Ethereum addresses, and they are implanted in the principal piece of each variety channel, bringing about a limit of 512x512x3 bits per image.

The dataset is intended for applications of steganographic procedures for better cloud security, where steganography can be utilized to conceal malignant payloads in blameless-looking pictures. The device utilized for the LSB steganographic strategy is the LSB-Steganography, which is a famous steganography apparatus that empowers clients to conceal messages or documents in computerized pictures.

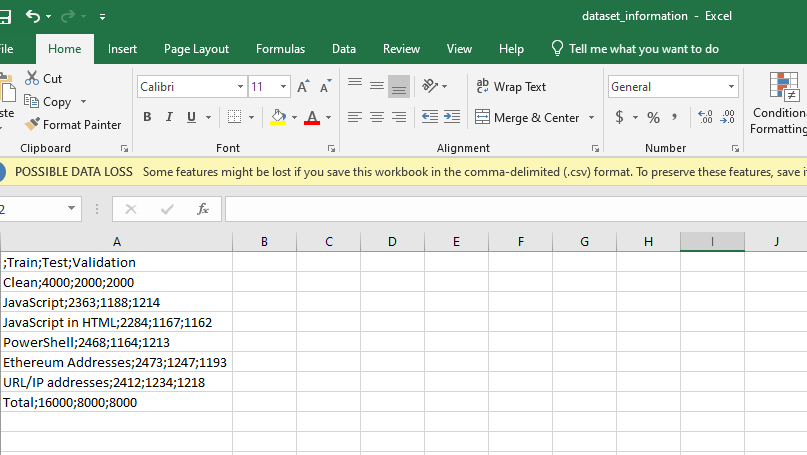


Figure 3.3.1: Dataset description

Source: self-created

The dataset comprises 16,000 images in the preparation set, 8,000 images in the test set, and 8,000 images in the approval set. The images in the preparation set contain various sorts of payloads, including the malevolent JavaScript’s acquired from the JavaScript Malware Collection, the malicious JavaScript’s jumbled in HTML acquired from the Noxious Javascript Dataset, the pernicious PowerShell scripts acquired from the PowerDrive repository, the vindictive URLs acquired from the Ethereum-records archive, and the Ethereum addresses acquired from the URLhaus data set.

In the preparation, test, and approval sets, the dataset likewise incorporates two extra test sets: stego\_b64 and stego\_zip. These sets contain 8,000 images that are "obfuscated" with the base64 and zip calculations, separately, this dataset can be helpful for specialists and professionals who are keen on creating steganographic methods for better cloud security, especially for distinguishing and forestalling the implanting of malignant payloads in digital images.

# Chapter 4 : Product/Research Design and Implementation

Graphical user interface, application, Teams

Description automatically generated

Figure 3: Login Page

The different steganography techniques were implemented using a web based application which was developed by the researcher. This web application creates a space where all the four steganography techniques were  performed simultaneously. These algorithms were then analysed on the basis of three parameters such as CPU utilisation, Time Chart and  image compression.

This application was designed with a highly user friendly interface that facilitates the user's understanding of each algorithm separately. As a user, the individual would first have to register with the system using an email address and create a password. Once authentication is done, the user can see a dashboard with each technique listed, namely Least Significant Bit, Discrete Cosine Platform, Pixel Value Differencing, and Spread Spectrum Technique.

Graphical user interface, application

Description automatically generated

For instance, the user starts with the LSB technique. They then need to write a secret message and upload any image provided from the data set which will be used for encrypting the secret message. Thereafter, the user has to select the name of the receiver for whom the secret message is meant for. The system will give a list of all users who are registered on the application. Therefore, the encoded image can only be viewed by the selected user and the logged-in user themselves. Once all the required details are filled in, the user has to select the encode button, and they will get an option to download an encoded image. This image contains the secret message.

Graphical user interface, text

Description automatically generated

Figure 4 : Encoding process

**The encoding processes**

The website was developed using HTML, CSS/ JS, and the backend is written using PHP and Python. Once the user enters the details in the HTML form, an asynchronous call (AJAX) is made to the PHP file. This asynchronous call is facilitated by JQuery, which collects the data inputted in the form and sends a POST request to the PHP file. An asynchronous call reduces the wait time and enables the transport of data without the need to redirect the page, which in turn enhances the user experience.

The PHP script now has the required data, which is the secret message, image, current user details, and the username for which the message is intended. The PHP script first uploads the image on the server, before which it checks if the image format is valid (png, jpeg, jpg, etc.) and if the image is less than 5kb. Post this, a Python script is executed, which will pass two parameters as arguments i.e. the image path and the secret message. The researcher has developed a Python script that encodes the image to store the secret message with the use of libraries like Pillow, Chardet, CV2, etc. The Pillow library contains all the basic image processing functionality, and CV2 helps in image processing and performing computer vision tasks.

The output of the Python script returns an encoded image, time taken, CPU utilised, and image name. These, when received by the PHP script, send the encoded image back as a response to the previous asynchronous call, which then facilitates the download. The rest of the information received by the Python script, namely, the image, time taken, CPU utilised, and image name, is stored in the database, which is used for the purpose of analysis.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| id | current\_user | msg\_for(recv) | img\_name | time\_taken | cpu\_percent | img\_loss\_in\_kb |

**Figure 5 :** Database Schema

This is a sample demonstration of a database schema which stores all data into blocks of parameters.

**The decoding process**

In the web application, below the encode module, the user can find the decode section as well. There, the user has to upload the encoded image, and in response, the secret message will be decoded and displayed. Similar to the encoding process, an asynchronous call is executed, which carries the uploaded image along with the logged in user’s details. The PHP script first determines if the uploaded image is intended for the logged-in user by cross-checking the details stored in the database during the time of encoding. If the user is authorised, a Python script is executed with the image path as the parameter in order to decode the secret message. On successful decoding the image, the Python script returns a text to the PHP script, and in turn, the PHP script sends the text as a response to the asynchronous call and displays the secret message to the user.

Graphical user interface, text, application, email

Description automatically generated

Figure 5: Decoding process

As many cloud services have Multi-Factor Authentication (MFA) to enhance system security, a security layer can be added to a cloud framework using image steganography. The concept is to implement image steganography to recover forgotten passwords. This feature has been added to the existing application, allowing a registered user to retrieve their password with the aid of image steganography Multi-Factor Authentication (MFA)  can be a way to improve the security of the data. A thorough analysis on different researchers on how their ideas are implemented to prevent the security risks in cloud computing.

Multi-Factor Authentication (MFA)  can be a way to improve the security of the data. A thorough analysis on different researchers on how their ideas are implemented to prevent the security risks in cloud computing.

Graphical user interface, application, Teams

Description automatically generated

Figure 8 : Retrieving the password from login page

If a user forgets their password, they can use this feature by clicking on the 'forgot password' link/button. This will redirect the user to a page where they can enter their registered username and email ID and click on the 'Receive Encoded Image' button. This action will trigger an email to the specified email address, which will include an attached encoded image. The password of the registered user will be encoded in this image using the LSB technique.

Graphical user interface, application, Teams

Description automatically generated

Figure 9 : Stego image sent to the registered email

Once the user downloads the image received via email, they can upload it to the appropriate page and click on 'Decode.' If the user and the image are valid, the password will be displayed in text format, which can then be used to log in again.

Graphical user interface, application

Description automatically generated

Figure 10 : Pasword decoded

Graphical user interface, text, application, email

Description automatically generated

Figure 11: Email received to decode the password

By practically applying image steganography to the application, the security has been significantly enhanced.

If a user forgets their password, they can use this feature by clicking on the 'forgot password' link/button. This will redirect the user to a page where they can enter their registered username and email ID and click on the 'Receive Encoded Image' button. This action will trigger an email to the specified email address, which will include an attached encoded image. The password of the registered user will be encoded in this image using the LSB technique.

Once the user downloads the image received via email, they can upload it to the appropriate page and click on 'Decode.' If the user and the image are valid, the password will be displayed in text format, which can then be used to log in again.

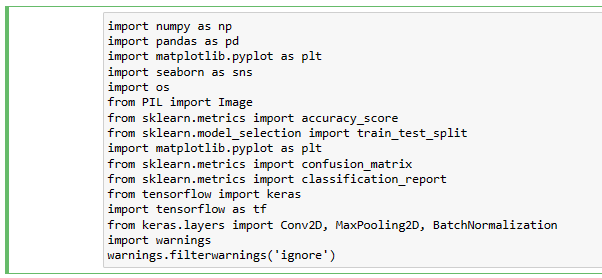
By practically applying image steganography to the application, the security has been significantly enhanced.

The additional security layer provided by MFA is challenging for cyber attackers to gain unauthorised access to the data even if they have the users credentials. It is the easiest way to implement this security layer where the user only requires to provide some additional authorization layers. It resolves major attacks such as:

* Brute-Force Attacks:  Auto Generated tools are accessed by the attackers to try a vast variety of username and password combinations to gain an unauthorised entry to an account. MFA can fight such an attacker as it would still require a second authentication factor to access the account.
* Phishing Attacks: Attackers use fraud web sets or spam emails to manipulate the user into giving the credentials to access the account.
* Man-in-the-middle: Intercepting the communication between the user and the cloud system can be a possibility to leak the credentials
* Data & Security attacks: A biometric factor like fingerprint generated like fingerprint generated from an app can be a task for the attacker to access or steal the stored data.
* Virtualization Attacks: These threats are usually inside the infrastructure of a virtual machine. To ensure the authenticity a onetime code can be generated as a layer to protect the privileges and resources accessed by the virtual machine. Even if the unauthorised users try to abuse the resources, MFA will alert for an authentication code to grant entry.

# Chapter 5: Research Outcomes/Results/Discussion and Evaluation

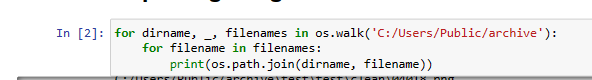
## 5.1 Research outcomes and Results

steganography can be utilized as an information increase procedure to work on the exhibition of grouping models. By implanting extra data in the preparation information, steganography can expand how much information is accessible for preparing and working on the precision of the model. For instance, steganography can be utilized to implant extra elements or marks in pictures that are utilized to prepare a grouping model. This can assist the model with learning more complicated designs in the information and working on its exactness. The utilization of steganography in requires cautious thought of safety and moral issues, for example, the potential for pernicious entertainers to utilize steganography to implant vindictive code or information in the preparation of information. It is essential to guarantee that the utilization of steganography is in consistence with significant regulations and guidelines and that suitable safety efforts are set up to safeguard the privacy and trustworthiness of the information.

**Figure 5.1.1: Importing libraries**

(source: self-created)

This is a code piece written in Python involving a few libraries for machine learning and data visualization, including NumPy, Pandas, Matplotlib, Seaborn, Scikit-learn, and TensorFlow.The code begins by bringing in these libraries and fundamental modules from them. In particular, it imports NumPy as np, Pandas as pd, Matplotlib.pyplot as plt, Seaborn as sns, the os module, the Picture module from the PIL library, the accuracy\_score capability and train\_test\_split capability from Scikit-learn, and different modules from TensorFlow and Keras.The code then, at that point, characterizes a capability or a progression of capabilities for information preprocessing, model structure, and assessment. Without seeing the full code, it is hard to decide the particular undertakings and work process the code performs.



**Figure 5.1.2: Importing image folder**

(source: self-created)

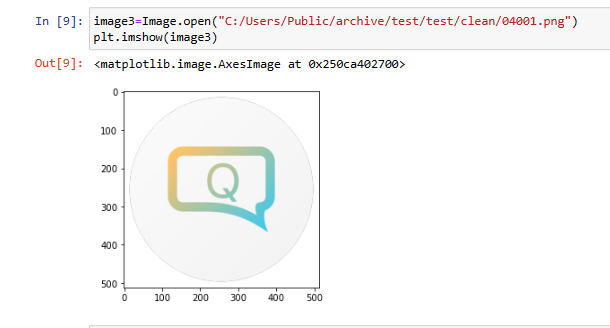
This code utilizes the os module to navigate through the registry design of the predetermined way ('C:/Clients/Public/document') utilizing the os.walk() technique.The os.walk() technique produces the record names in a registry tree by strolling the tree either hierarchical or base up. For every registry in the tree, including the root catalog, it y a 3-tuple. Here, the for loop iterates over the os.walk() generator, unloading the tuple into the factors dirname, \_, and filenames. The variable dirname addresses the way to the ongoing registry being crossed, filenames is a rundown of the record names in the ongoing catalog, and the variable \_ is a rundown of subdirectories in the ongoing registry (which are not being utilized in this code).Inside the inward for circle, the os.path.join() technique is utilized to join the ongoing registry way (dirname) with every filename in the filenames list. This outcomes in a full document way for each record in the predetermined catalog and its subdirectories. The full document ways are then printed to the control center utilizing the print() capability.



**Figure 5.1.3: Image plot folder**

(source: self-created)

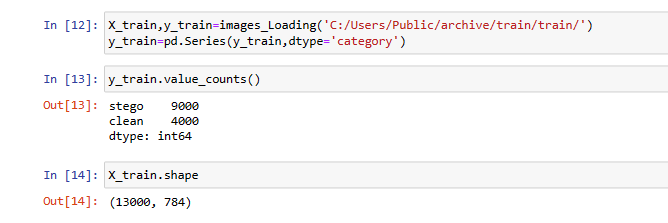
This code opens a image record situated at the predefined document way (C:/Users/Public/file/train/train/clean/00001.png) utilizing the image module from the PIL library. The Image.open() strategy is utilized to open the picture record, and the subsequent Picture object is appointed to the variable image1.Then, at that point, the plt.imshow() capability from the matplotlib.pyplot module is utilized to show the picture in a plot. The imshow() capability takes the image1 object as info and shows the picture as a plot in the ongoing figure.This code expects that the picture record at the predefined way exists and is a substantial picture document that can be opened by the image module.



**Figure 5.1.4: Image folder plot**

(source: self-created)

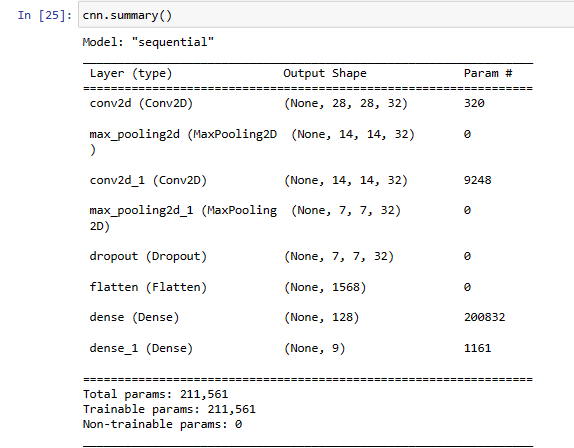
This code opens a image document situated at the predefined record way (C:/Clients/Public/file/test/test/clean/04001.png) utilizing the Picture module from the PIL library. The Image.open() strategy is utilized to open the picture document, and the subsequent Picture object is relegated to the variable image3.Then, at that point, the plt.imshow() capability from the matplotlib.pyplot module is utilized to show the picture in a plot. The imshow() capability takes the image3 object as info and shows the picture as a plot in the ongoing figure.This code expects that the image document at the specified way exists and is a substantial picture record that can be opened by the Picture module.



**Figure 5.1.5: Train test image load**

(source: self-created)

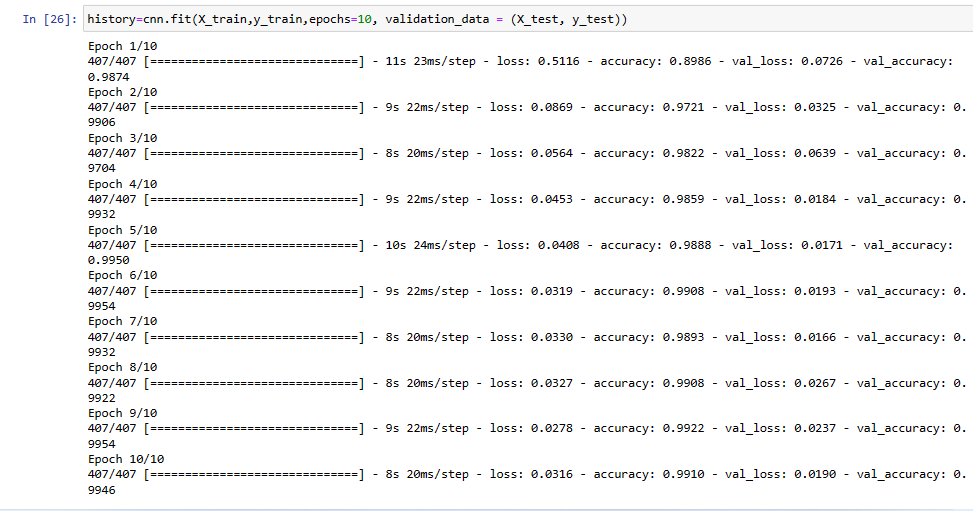
This code calls a function or technique named images\_Loading() that is excluded from the gave code piece. Without the execution of this capability, figuring out the thing this code is doing specifically is troublesome.The variable names, almost certainly, this code is stacking pictures and their related marks for the preparation informational collection from a predetermined registry (C:/Clients/Public/file/train/train/).The stacked pictures and their marks are alloted to the factors X\_train and y\_train, individually.The second line of code changes over the information kind of the names to a class information type utilizing the pd.Series() capability. A class information type is helpful while managing all-out information, like marks, as it can decrease memory use and accelerate specific tasks contrasted with a normal item data type.



**Figure 5.1.6: CNN summary**

(source: self-created)

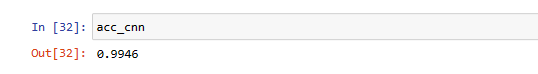
The above figure which is showing the summary of CNN This code calls the outline() strategy on a Keras Consecutive model item named cnn.The summary() strategy creates an intelligible synopsis of the model engineering, including the layers, their result shapes, the number of teachable boundaries, and other pertinent data.The result of this strategy is printed to the control center, giving a speedy method for investigating the model and guaranteeing that it has been built as planned. The outline can likewise be valuable for investigating issues connected with model design and for recognizing overfitting or underfitting issues.



**Figure 5.1.7: CNN summary**

(source: self-created)

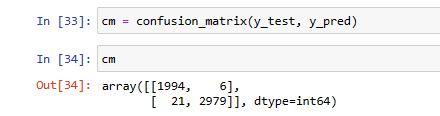
This code prepares a Keras Successive model item named cnn utilizing the fit() strategy.The fit() technique is utilized to prepare the model on a predefined set of info information X\_train and compare marks y\_train. The epochs parameter determines the number of epochs (complete goes through the whole preparation dataset) that the model ought to be prepared for.The validation\_data boundary indicates a tuple containing the approval information X\_test and comparing marks y\_test. During preparation, the model is to be assessed on this approval set after every age, permitting the client to screen the model's exhibition and forestall overfitting.The fit() technique returns a set of experience object that contains data about the preparation cycle, like the preparation and approval exactness and misfortune at every age. This set of experiences object is relegated to the variable history.In general, this code prepares the cnn model on the preparation information for 10 ages and uses the approval information to screen the model's presentation.



**Figure 5.1.8: CNN accuracy**

(source: self-created)

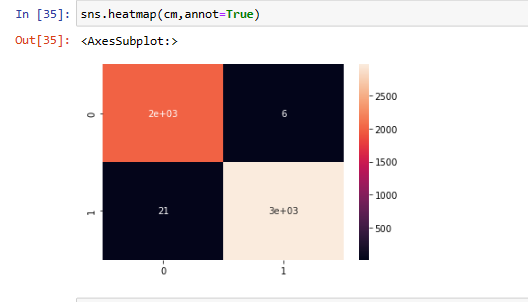
The code bit provided doesn't contain a definition for the variable acc\_cnn, so it is hard to give a depiction of what it does.almost certainly, acc\_cnn is a variable used to store the accuracy 0.9946.The estimation of this exactness might be performed utilizing the accuracy\_score() capability from sci-kit-get the hang of, contrasting the anticipated marks for the test set to the genuine names. On the other hand, it very well may be determined utilizing a Keras technique, for example, assess ().Without more data on how acc\_cnn is characterized or determined, giving a more point-by-point portrayal of the code is beyond the realm of possibilities.



**Figure 5.1.8: Confusion matrix**

(source: self-created)

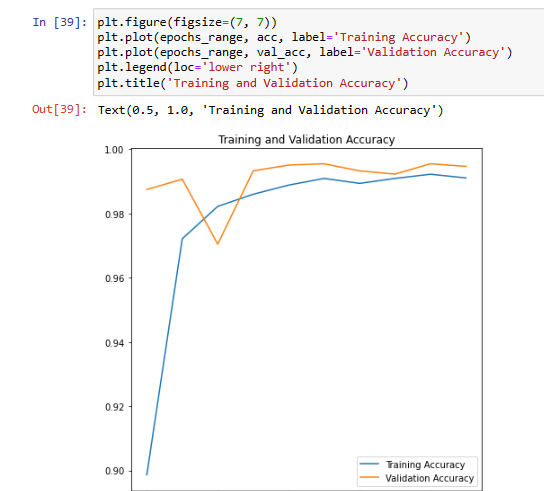
This code creates a disarray lattice utilizing the sci-kit-learn confusion\_matrix() capability. The capability takes two sources of info: the genuine marks y\_test and the anticipated names y\_pred. The confusion\_matrix() capability then, at that point, computes and returns the disarray network as a two-layered exhibit.The resulting confusion matrix is relegated to the variable cm. The network is displayed in the result of the code, and it has two lines and two segments.The components in the slanting from the upper left to base right address the number of genuine up-sides (TP) and genuine negatives (TN), which are the accurately characterized occasions for each class. For this situation, there are 1994 genuine negatives for the top of the line and 2979 genuine up-sides for the second class.The components in the off-slanting positions address the quantity of misclassifications. For instance, there are 6 misleading up-sides (FP) for the top notch and 21 bogus negatives (FN) for the second class.speaking, the disarray network gives important data about the presentation of the grouping model, including the quantity of right and erroneous expectations for each class.



**Figure 5.1.9: Heatmap**

(source: self-created)

This code produces a heatmap perception of the disarray grid utilizing the heatmap () capability from the seaborn library. The heatmap() capability accepts the disarray lattice cm as info and creates a shaded network addressing the qualities in the grid.The annot=True boundary adds the mathematical upsides of the lattice to every cell of the heatmap, giving more point-by-point data about the number of genuine up-sides, genuine negatives, bogus up-sides, and misleading negatives in each class.The resulting heatmap gives a visual portrayal of the disarray network that can assist with distinguishing examples and patterns in the information, for example, classes that are habitually misclassified or classes that have high exactness. This can be a valuable instrument for assessing the exhibition of a grouping model and distinguishing regions for development.



**Figure 5.1.10: Training and validation accuracy**

(source: self-created)

This code produces a plot of preparing and approval exactness over different ages of preparing for a brain network model. The plt.figure() capability sets the size of the figure, which is 7 creeps by 7 crawls for this situation.The plt.plot() capability is called two times, once to plot the preparation exactness (acc) over the quantity of ages (epochs\_range), and once to plot the approval precision (val\_acc). The name boundary is utilized to set the marks for each line in the plot.The plt.legend() capability adds a legend to the plot that distinguishes which line relates to the preparation exactness and which line compares to the approval precision. The loc boundary sets the area of the legend to the lower right corner of the plot.At long last, the plt.title() capability sets the title of the plot to "Preparing and Approval Exactness".This kind of plot is normally used to envision the presentation of a brain network model during preparing. It can assist with distinguishing issues, for example, overfitting or underfitting, where the preparation exactness might increment while the approval precision doesn't, or where the approval precision begins to diminish as the model turns out to be excessively complicated.

## 5.2 Research outcomes/ Discussion

The above code isn't straightforwardly connected with steganography or cloud security, yet the ideas of picture characterization and profound learning are pertinent to these areas.Image classification using CNN is a typical procedure for distinguishing objects inside pictures, and it has numerous applications in regions like computer vision clinical imaging, and remote detection. Via preparing a model on an enormous dataset of marked pictures, for example, the dataset utilized in the code above, it is feasible to make a classifier that can precisely distinguish new images.With regard to steganography and cloud security, picture arrangement procedures can be utilized to distinguish pictures that contain stowed-away data. For instance, assuming that an assailant was to insert delicate information inside a picture and transfer it to a cloud administration, a picture grouping calculation could be utilized to distinguish that the picture contains more data than is evident from a visual investigation. This could assist with recognizing potential security breaks and keep touchy information from being compromised. Image classification, there is progressing investigation into steganographic methods that can be utilized to conceal information inside pictures and different media. A portion of these methods are intended to be more impervious to location than customary steganography, making them possibly more helpful for cloud security applications. While the above code isn't straightforwardly connected with steganography or cloud security, it shows the utilization of AI procedures for picture grouping, which can be a significant apparatus here. Progressing examination into both picture arrangement and steganography will probably prompt new and creative ways of upgrading the security and protection of cloud-based information.

# Chapter 6: Project Management

Cloud computing is becoming more popular as individuals realise its advantages in terms of convenient data storage and access. The following is a possible explanation for this phenomenon. Using cloud storage, however, is fraught with peril since it's possible for unauthorised parties to get access to sensitive data stored there. The usage of cloud storage introduces this risk. Information may be concealed in a picture or a clip using a technique called steganography. There are several methods to do this. This means it's a good tactic for shoring up the security of cloud-stored information. The option to use steganography is there here. To that end, we suggest using steganography to cloak private information inside a picture, with a convolutional neural network (CNN) providing additional security. The information will be hidden using steganography. To accomplish the intended outcome of hiding the data within the image, steganography would be utilised. Project management is going to be employed to help with the smooth running of this system's growth.

The project will be overseen using agile project management techniques, and its primary objective is to provide a working prototype quickly and effectively. Python will be used for both the steganography-based system's construction and the CNN model's development. The system's performance will be evaluated using a cloud storage service, and the results will be compared to real-world conditions.

The project will be successful if a steganography-based solution is developed to improve cloud security, with the data embedded encrypted using a convolutional neural network model. The constructed system will be tested in various ways to see how well it functions. The objective of these evaluations is to provide the highest possible degree of security with as little effect as possible on the system's functionality. The project management plan will guarantee on-time completion within the allocated budget and to the complete satisfaction of all parties involved.

The goal of the presented research is to develop a steganography-based system that, when used in tandem with a Python-based convolutional neural network (CNN), improves cloud security. This system's creation will be guided by the principles of project management. Doing so will guarantee that the project is finished on time and to the satisfaction of everyone involved. This project will significantly advance the rapidly expanding subject of cloud security by creating a novel method for safeguarding private data stored in the cloud.

# Chapter 7: Conclusion and Future Work

The above code gives off an impression of being connected with picture characterization utilizing convolutional brain organizations (CNNs) and assessing the presentation of the model utilizing different measurements like exactness and disarray framework. While this code doesn't straightforwardly connect with steganography or cloud security, steganography is a method that can be utilized to conceal data inside computerized pictures or different media to upgrade security and protection. By implanting information inside a picture, for instance, a client can send delicate data in a manner that is less inclined to be distinguished or caught. As far as future work, there are numerous possible applications for steganography and related procedures in cloud security. For instance, steganography can be utilized to conceal delicate information inside pictures or different media prior to transferring to a cloud administration, giving an extra layer of safety past encryption and other conventional safety efforts.Other possible regions for future work incorporate growing further developed steganographic procedures that are less powerless to location or creating calculations to recognize steganography and other incognito correspondence methods. Also, exploration could be directed to investigate the expected dangers and tradeoffs related with involving steganography in cloud security, like the potential for expanded computational above or decreased picture quality. Generally speaking, steganography can possibly be an important instrument in cloud security, and further innovative work in this space could prompt superior security and protection for clients.

## Limitation

* Cropping, resizing can potentially remove the information in the image which can be easily detected by the attackers.
* If the technology is properly implemented, the image can result in the loss of data.
* Size of the information matters as it limited with the size of the image and complexity of the algorithm applied. This causes loss of data storage within an image.
* As application is user-friendly, the user cannot be authorized to download the encoded image if he/she is not registered.

## Future Work

Based on the findings, here are some suggestions for the future scope of the study:

1. A master key to be generated in order to authenticate the user to decode the following password for login credentials.
2. The application lacks machine learning algorithm. So, implementing Convolutional Neural Network (CNN) can be a best fit because it learns the pattern and structure of images to detect the presence of the information.
3. The created application can also be tested with different techniques for better cost-effective solution to prevent attacks on the information (eg: Visual Cryptography)
4. Deploying into a cloud service platform such as Amazon Web Services (AWS) and accessing certain services and policy provided such as Key Management Services (KMS) and Identity Access Management (IAM) and Cloud trail to explore and monitor the technique and risk involved for better security requirements.

## Recommendation

Based on the results and findings of the supplied research, it is suggested that more investigation into steganography as a strategy for increasing the amount of information to better the performance of machine learning models be conducted. This suggestion was made since the provided research included both results and findings. This strategy could enhance the amount of data used to train models, resulting in models that are not only more accurate but also more sophisticated. However, while incorporating steganography into machine learning, it is crucial to keep security and ethical considerations in mind.

The offered code snippets also serve as a solid groundwork for actual data preprocessing, model creation, and result evaluation in machine learning. NumPy, Pandas, Matplotlib, Seaborn, Scikit-learn, and TensorFlow are just some of the libraries and modules used by these processes, which encompass a wide range of applications. Furthermore, a wide range of Python packages are used in these processes. Some examples of operations that come under this heading include importing data, browsing directories, presenting visuals, and describing model architecture. Researchers and developers in the field of machine learning would do well to familiarise themselves with the aforementioned libraries and code snippets, as doing so would streamline their processes and improve the quality of their final products.

Finally, it's important to underline the significance of understanding the need for greater study on the ethics, safety, and regulation of machine learning to ensure the responsible creation and dissemination of machine learning models. The topics of ethics in machine learning, safety in machine learning, and regulation of machine learning should all be central to this study. Privacy, objectivity, fairness, and accountability must all be taken into account, as well as the fulfilment of any and all applicable laws and standards. Experts in the field of machine learning, both in academia and in industry, should pursue ongoing training and education in the areas listed above. This will contribute to the development of a culture in which machine learning is used in a responsible and ethical manner.

# References

Ahmed, O.M. and Abduallah, W.M., 2017. A review on recent steganography techniques in cloud computing. *Academic Journal of Nawroz University*, *6*(3), pp.106-111.

Ahsan, K. and Kundur, D., 2002, December. Practical data hiding in TCP/IP. In *Proc. Workshop on Multimedia Security at ACM Multimedia* (Vol. 2, No. 7, pp. 1-8). New York: ACM Press.

AlKhamese, A.Y., Shabana, W.R. and Hanafy, I.M., 2019, February. Data security in cloud computing using steganography: a review. In *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)* (pp. 549-558). IEEE.

Almorsy, M., Grundy, J. and Müller, I., 2016. An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

Alshwaier, A., Youssef, A. and Emam, A., 2012. A new trend for e-learning in KSA using educational clouds. *Advanced Computing*, *3*(1), p.81.

Arora, R. and Bajaj, K.S., 2013. Highly Effective Advanced Technology" HEAT" Re-defining Technology for Hospital Management. *International Journal of Management & Behavioural Sciences, Special Edition*, pp.68-73.

Awadh, W.A., Hashim, A.S. and Hamoud, A., 2019. A review of various steganography techniques in cloud computing. *University of Thi-Qar Journal of Science*, *7*(1), pp.113-119.

Bender, W., Gruhl, D., Morimoto, N. and Lu, A., 1996. Techniques for data hiding. *IBM systems journal*, *35*(3.4), pp.313-336.

Bohn, R.B., Lee, C.A. and Michel, M., 2020. The NIST cloud federation reference architecture.

Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P., 2010. Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), pp.727-752.

Dickman, S.D., 2007. An overview of steganography. *Department of Computer Science, James Madison University Infosec Techreport*, *2*, pp.305-315.

Davies, A., 2004. Computational intermediation and the evolution of computation as a commodity. *Applied Economics*, *36*(11), pp.1131-1142.

Fridrich, J., Goljan, M. and Du, R., 2001, October. Reliable detection of LSB steganography in color and grayscale images. In *Proceedings of the 2001 workshop on Multimedia and security: new challenges* (pp. 27-30).

Gens, F., 2008. Defining cloud services and cloud computing. IDC eXchange.

Goli, M.S. and Naghsh, A., 2016. A comparative study of image-in-image steganography using three methods of least significant bit, discrete wavelet transform and singular value decomposition. *Bulletin de la Société Royale des Sciences de Liège*, *85*(1), pp.1465-1474.

Goyal, S., 2014. Public vs private vs hybrid vs community-cloud computing: a critical review. *International Journal of Computer Network and Information Security*, *6*(3), pp.20-29.

Hussain, M., Wahab, A.W.A., Ho, A.T., Javed, N. and Jung, K.H., 2017. A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. *Signal Processing: Image Communication*, *50*, pp.44-57.

Joint, A. and Baker, E., 2011. Knowing the past to understand the present–issues in the contracting for cloud based services. *Computer Law & Security Review*, *27*(4), pp.407-415.

Kadhim, I.J., Premaratne, P., Vial, P.J. and Halloran, B., 2019. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, pp.299-326.

Lakshmi, P.N.S. and Latha, C.N., 2013. A Novel Syndrome Coding Scheme For Embedding And Minimizing Distortion in Steganography.

Luo, W., Huang, F. and Huang, J., 2011. A more secure steganography based on adaptive pixel-value differencing scheme. *Multimedia tools and applications*, *52*, pp.407-430.

Marvel, L.M., Boncelet, C.G. and Retter, C.T., 1999. Spread spectrum image steganography. *IEEE Transactions on image processing*, *8*(8), pp.1075-1083.

Mirashe, S.P. and Kalyankar, N.V., 2010. Cloud computing. *arXiv preprint arXiv:1003.4074*.

Morkel, T., Eloff, J.H. and Olivier, M.S., 2005, June. An overview of image steganography. In *ISSA* (Vol. 1, No. 2, pp. 1-11).

Orea, J., 2011. Quick guide to the reference architecture: Trusted Cloud Initiative. *Cloud Security Alliance*.

Rahman, S., Uddin, J., Khan, H.U., Hussain, H., Khan, A.A. and Zakarya, M., 2022. A novel steganography technique for digital images using the least significant bit substitution method. *IEEE Access*, *10*, pp.124053-124075.

Ryan, M.D., 2013. Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, *86*(9), pp.2263-2268.

Sell, L., 2019. Openstack launches as an independent foundation, begins work protecting, empowering and promoting openstack.

Silman, J., 2001. Steganography and steganalysis: an overview. *Sans Institute*, *3*, pp.61-76.

Siper, A., Farley, R. and Lombardo, C., 2005. The rise of steganography. *Proceedings of student/faculty research day, CSIS, Pace University*, p.D1.

Sultan, N., 2010. Cloud computing for education: A new dawn?. *International Journal of Information Management*, *30*(2), pp.109-116.

Surbiryala, J. and Rong, C., 2019, August. Cloud computing: History and overview. In *2019 IEEE Cloud Summit* (pp. 1-7). IEEE.

Varia, J. and Mathew, S., 2014. Overview of amazon web services. *Amazon Web Services*, *105*.

Wang, W., Guo, Y., Li, L., & Li, X. (2017). Steganography algorithm based on discrete cosine transform and human visual system. *Multimedia Tools and Applications*, 76(15), 16279-16294.

Zhang, X., Shi, Z., Liu, X., & Zhang, X. (2019). A DCT-based steganography method with high image quality. *Multimedia Tools and Applications*, 78(9), 11151-11170.

Zhelezov, S. and Kordov, K., 2020. Method for Spread Spectrum Steganography with Cryptographic Algorithm.

KHAN, L.S., KHAN, M., HAZZAZI, M.M. and JAMAL, S.S., 2023. A novel combination of information confidentiality and data hiding mechanism. Multimedia Tools and Applications, 82(5), pp. 6917-6941.

KOPTYRA, K. and OGIELA, M.R., 2023. Steganography in IoT: Information Hiding with Joystick and Touch Sensors. Sensors, 23(6), pp. 3288.

MAGDY, M., HOSNY, K.M., GHALI, N.I. and GHONIEMY, S., 2022. Security of medical images for telemedicine: a systematic review. Multimedia Tools and Applications, 81(18), pp. 25101-25145.

MANDAL, S. and KHAN, D.A., 2023. Enhanced-Longest Common Subsequence based novel steganography approach for cloud storage. Multimedia Tools and Applications, 82(5), pp. 7779-7801.

MAWGOUD, A.A., TAHA, M.H.N., ABU-TALLEB, A. and KOTB, A., 2022. A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system. Journal of Cloud Computing, 11(1), pp. 97.

NGUYEN, T.D. and LE, H.Q., 2022. A secure image steganography based on modified matrix encoding using the adaptive region selection technique. Multimedia Tools and Applications, 81(18), pp. 25251-25281.

PANCHIKKIL, S., SIVA, P.V., MANIKANDAN, V.M., DONTA, P.K., PRAVEEN KUMAR, R.M. and THIPPA, R.G., 2023. An Ensemble Learning Approach for Reversible Data Hiding in Encrypted Images with Fibonacci Transform. Electronics, 12(2), pp. 450.

PHIPPS, A., OUAZZANE, K. and VASSILEV, V., 2022. Securing Voice Communications Using Audio Steganography. International Journal of Computer Network and Information Security, 14(3), pp. 1.

SELVARAJ, J., WEN-CHENG, L., BALASUBRAMANIAN, P.K., KAVITHA, C. and GAN, H.S., 2023. Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security. Electronics, 12(7), pp. 1636.

SHAWKAT, S.A. and AL-BARAZANCHI, I., 2022. A proposed model for text and image encryption using different techniques. Telkomnika, 20(4), pp. 858-866.

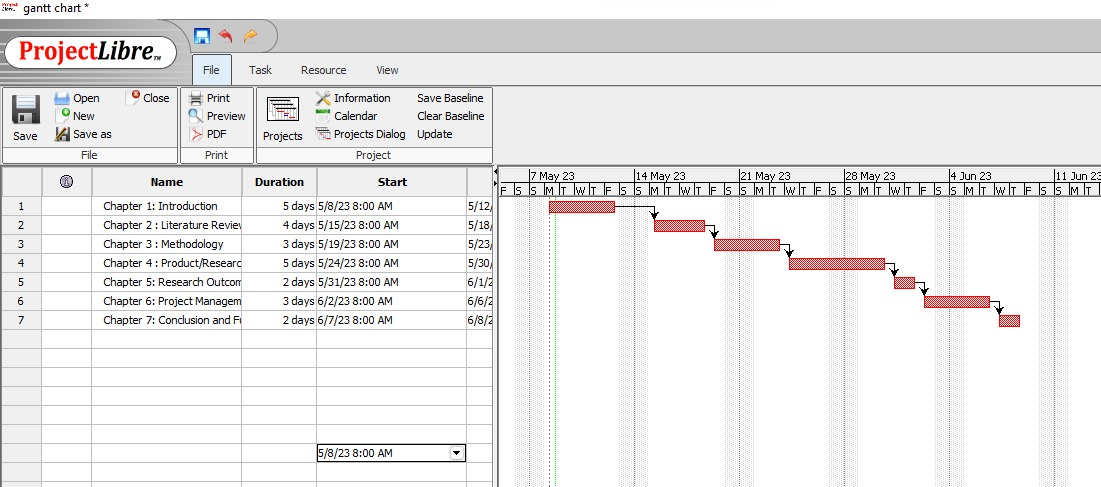
TAHA, M.S., RAHEM, M.S.M., HASHIM, M.M. and KHALID, H.N., 2022. High payload image steganography scheme with minimum distortion based on distinction grade value method. Multimedia Tools and Applications, 81(18), pp. 25913-25946.

WANG, J., TAN, F.S. and YUAN, Y., 2023. Random Matrix Transformation and Its Application in Image Hiding. Sensors, 23(2), pp. 1017.

YADAV, G.S., MANGAL, P., PARMAR, G. and SOLIYA, S., 2023. Genetic algorithm and hamilton path based data hiding scheme including embedding cost optimization. Multimedia Tools and Applications, 82(13), pp. 20233-20249.

# Appendices

**Gantt chart**

****

**GitHub Link**