

Cloud Data Security Improvement Using Steganography by Pseudo Random Number Generation (PRNG)

MSc Research Project
MSc in Cyber Security

Pooja Revanna Kumar
Student ID: 20190417

School of Computing
National College of Ireland

Supervisor: Dr Vanessa Ayala Rivera

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Pooja Revanna Kumar
Student ID: 20190417
Programme: MSc in Cyber Security **Year:** 2021-2022
Module: Internship
Supervisor: Dr Vanessa Ayala Rivera
Submission Due Date: 16th December 2021
Project Title: Cloud Data Security Improvement Using Steganography by Pseudo Random Number Generation (PRNG)
Word Count: 5252 **Page Count:** 18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Pooja Revanna Kumar

Date: 16th December 2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

| | |
|---|--------------------------|
| Attach a completed copy of this sheet to each project (including multiple copies) | <input type="checkbox"/> |
| Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies). | <input type="checkbox"/> |
| You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | <input type="checkbox"/> |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| | |
|----------------------------------|--|
| Office Use Only | |
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

Cloud Data Security Improvement Using Steganography by Pseudo Random Number Generation (PRNG)

Pooja Revanna Kumar
20190417

Abstract

The cloud is the most modern and convenient way to manage and access enormous amounts of data. The concept of cloud computing is the storage of data that is accessed and sorted over the internet rather than being kept locally on a computer. As cloud computing runs programs over the internet, it can handle a great deal of data on-demand. In the information age, cloud computing provides convenient access to online storage, which contributes to the growth of technology and communication. As cloud computing gives access to all information and allows everything to be run online, it requires strong data security. It is important to remember that several types of security problems can arise, including data security, data privacy, data integrity, and data authentication. To solve all the problems, cloud security needs to continuously improve and update. Data security is implemented and developed using Cryptography and Steganography. Steganography can be used to hide the information of communication from unauthorized users using encryption, and Cryptography can be used to encrypt data in communication. Steganography is the most effective method for securing cloud communication data. Steganography is most secure method for hiding data, including image, audio, and video. However, the best and most secure method is using image data hiding. The steganography method of cloud data securing is most secure because it handles redundant data and conceals data. When the Pseudo-Random Number Generation (PRNG) is used, the steganography method is more reliable. PRNG technology can be used to implement the steganography method.

1 Introduction

A major sensitive aspect of cloud computing is data and information security. Because cloud computing systems, data and cloud infrastructures must be protected against alteration or unauthorized access, the development of different approaches for improving data security in the cloud is needed (Ajala et al., 2019). The cloud computing system is used by businesses such as education centers, health care centres, and banks. Multiple things we use every day are private, such as ATM pins, passwords, or secret messages. Pseudo-random numbers are generated with a deterministic algorithm. This algorithm is used to sequence the data from random data.

Cryptography and Steganography (AlKhamese et al., 2019) are major components of cloud computing technology. Cloud computing also uses watermarks (AlKhamese et al., 2019).

Using steganography techniques to secure communication in the cloud is an effective way of enhancing data security in cloud computing (Sarkar and Chatterjee, n.d.). In their study, Reza, H., & Sonawane, M detailed Steganography, which is a technique of hiding information within a message in a way that only the sender and receiver are capable of understanding the content and accessing it (Reza and Sonawane, 2016). Data and messages are encrypted with this technology. Today, every image or video, and audio file on any website is stored in the cloud through a method called steganography (Brindhashree and Prakash, 2020). The use of cryptography and steganography can be used to encrypt and hide information in communications. Steganography is the most effective means of securing cloud data of communication. Whenever you use the internet or make use of online services, data security is an increasingly important concern. Using all these technologies, when any sender sends any message, any file, or anything at all, that data is already encrypted so that anyone trying to read it cannot understand it. Cryptography and steganography are used to encrypt the data from end to end. In cloud computing security, the data is always hidden from the users, but the users stay connected.

The main concern to be noticed here is how steganography will be used in cloud security with a better connection protecting data from unauthorized access and how do pseudo-random numbers work to protect the data exchange in cloud computing?

The purpose of this paper is to develop a new steganography-based approach by using pseudo-random number generation (PRNG) to improve cloud data security and also to check the better encrypted data transaction between the network protecting from the unauthorized access. The use of pseudo-random numbers, convert sequence numbers to random numbers.

An image steganography method and its applications are presented in this new technique. As the Internet continues to grow in popularity, steganography has become increasingly important. Steganography differs from cryptography in that the information is visible in cryptography, but it is undefinable, while the information is hidden in steganography. PRNG generates the random sequence which makes difficult for unauthorized person to know the secret key. And also, Steganography improves the security by pseudo-random numbers which is the least weighted bit in the number and is driven by a unique technology that is in the transform domain. Using least weighted bits, the image was encrypted with cryptography and pseudo-random numbers.

This project tries to increase data security, and this project is also more efficient than previously published projects. Through this project, cloud security performs better, because of the use of steganography technology. Cloud computing technology nowadays is an extremely useful technology, this project's security of data or sending messages is fully secure.

2 Related Work

Steganography is readily known as an excellent method of sending secret messages through photos, videos, audio, or text. The Algorithms which we have are more powerful and secure. Below points explain some of the methods used for cloud data security by Steganography using PRNG.

a. Cloud Data Security Improvement Using Steganography

The cloud security concept is based on this project that combines cryptography and steganography on the network layer to provide a comprehensive level of security. Steganographic techniques are also included in this project. Additionally, cloud computing security allows for the use of DCT and LSB techniques. The LSB technique hides all of the data from every domain. Technology that protects from external attacks always transfers data efficiently and encrypts it smoothly as well. DCT technology involves a great deal more complexity than LSB. Data encryption and data steganography have several competitors. Data encryption and data steganography are more secure than ever (Suganthi and Selvi, 2020). LSB ensures that weak data is transformed into strong data. Steganography transforms all messages or data to an encrypted format. It provides protection against external attacks. By using steganography, the sender can see everything, but the middle of the path, all the messages or data is encrypted, this is decoded after the receiver receives it. Data is hidden by a covering object coated in the middle of the path. Steganography can create connections and transform the technology in the domain.

b. Implementation of Pseudo-Random Number

Data is hidden and a connection is established with the server when pseudo-random numbers are used between steganography processes. Outsiders cannot degrade the information in the carrier image with this technology. 24 bits are available in LSB. By using pseudo-random numbers, this method creates good connections and essentializes the data. Color components from RGB pixels are mostly handled by this method. By using this technology, the data already contains all the values. Various advantages and disadvantages of the steganography method exist. With this technology, messages are converted to local images. The message and data are matched. Also, this technology maintains the quality of images or videos (Osuolale, 2017). Steganography is also based on pseudo-random numbers and MSE. Using pseudo-random numbers and steganography together converts text messages into encrypted form. Symmetric key cryptography is used to convert the long text to the encrypted version, and ASCII values and randomly generated keys are also converted to the encrypted version of the long text. Several parameters need to be improved to improve the security of cloud computing. Cloud computing uses the AES encryption standard. Image pixels are maintained by pseudo-random numbers.

c. Critical Analysis on the Protection of Cloud data from Unauthorized Access

The cloud is one of the most useful technologies of our time. We store all our data in the cloud. Physical components like hard disks, rams, and operating systems are all available in the cloud service (Dhawan and Gupta, 2021). When pseudo-random numbers and steganography work together, they encrypt data, messages, and any type of multimedia. The data is available on the internet for free and can be accessed by anyone. On the network layer of the OSI (Open Systems Interconnection) model, this steganography technology provides a very secure key-changing algorithm. Cloud computing technology is becoming increasingly secure with each passing day; when the sender sends data, messages, mail, or images, this technology turns the data into a decoded version in the middle of the path, so nobody can access the data. Data can only be received and read by the receiver. Text can be hidden using QCC and DCT. This project provides greater security in the cloud as well as being more efficient. There is no unauthorized access to research work (Jain, 2018). Unless the password is entered, any attempt to access the data in the middle of the path will result in the data being destroyed. The cloud service can be attacked by anyone or destroyed by anyone, but there are two steps of verification. Cloud data is not normally accessible by anyone.

d. Development of Solutions for Steganography model in Cloud computing

We discussed how to improve cloud security with steganography by pseudo-random number in the previous point about developing so many criticalities, and now we'll discuss how to fix all of them. It was often impossible to encrypt data when developing the project, but when using pseudo-random numbers and steganography all data was easily encrypted. Data in texting formats is sometimes not embedded but using cryptography can solve a lot of problems (Mandal and Khan, 2019). One-dimensional steganography is implemented there. When the LSB method is used, all of the images' pixel values are changed to $2n/2$. Some sections failed to maintain image processing or image value, but fuzzy logic was used in the coding section, and all images and text messages were converted using this fuzzy logic. The cloud service can secure data through steganography and cryptography.

e. Assessment of the advantages and disadvantages of Steganography model and PRNG

Pseudo-Random Numbers are used to steganography all data (BanuPriya et al., n.d.). To connect a uniform resource locator to a server, steganography technology is always used. It is a secure method to encrypt the data using pseudo-random numbers, and it is easy to make an encrypted file with the steganography method. Pseudo-Random Numbers are used in this steganography model to improve cloud security (Mustafa et al., 2018).

There are disadvantages in this project as well as a small amount of information that hides in the cloud. Steganography uses pseudo-random numbers to hide many data, files, and long texts, making them impossible to understand easily, and this is the main drawback of Steganography.

3 Research Methodology

Fresh approaches in steganography and cryptography are being introduced due to security vulnerabilities in the outcome. The field of novel approaches is critical to overcoming the weaknesses and strengths of any digital steganography technique.

To reduce software and hardware requirements, data servers should be implemented in cloud platforms (Rahman et al., 2017). It is most common for intruders to intercept messages that are hidden within the digital cover media, such as images, audio, video, or multimedia. As a result of cyber security, original approaches to steganography and cryptography have been developed to prevent hackers from intercepting confidential data. To hide secret information from an intruder, you can use these two security techniques.

- **Cryptography**
- **Steganography**

a. Cryptography Technique:

In cryptography, information is hidden within text or digital media, like images, audios, or videos. A variety of techniques are being used to generate cryptography format; for example, converting the text into an unreadable format or changing the images into a scrambled format to protect them from security attacks. In general, text files are encrypted. In plain text format, the message text is readable, and cipher text is the form of the plain text that becomes

unreadable after it is encrypted. A cipher text, also known as an encrypted text, is a series of randomized letters and digital numbers that are unperceivable to humans (Abdullah et al., 2021). The process of encrypting and decoding cipher text is known as encryption and decryption, respectively.

b. Techniques of Data Hiding:

Steganography is not part of cryptography. Data hiding emerged from steganography. Data hiding originated from the techniques of watermarking and steganography.

- **Watermarking Technique:** Watermarking involves encoding data into any digital signal and concealing it. There is no need to relate the hidden information to the image container. A watermark is used to authenticate and secure the carrier image of its owner. Watermarking protects images from copying by using a stamp to prevent unauthorized copying.
- **Steganography Technique:** Greek word steganography originated from two words meaning covered writing: steganos and graphein. Steganography is a technique for hiding data. Using a network channel, anyone with knowledge about confidential information can transmit it from the sender to the correct recipient. The recipient must have a carrier image to do all this. This image carries the secret information that will be forwarded to the recipient. A variety of countries use this technique to send confidential messages from one country to another (Dhawan and Gupta, 2021). As technology advances, steganography techniques are now being implemented in computer systems. Steganography is constructed through two steps: embedding and extraction. A bit-stream version of the secret message is embedded into the cover image during embedding.
- LSB or least significant bit of the cover image is going to be inserted into this bit-stream. The cover of this book is an RGB or color image, and therefore the three signals it contains are red, green, and blue. Image steganography can be divided into two main categories: transformation domain image steganography and spatial domain image steganography. There are two main embedding procedures: the LSB technique and PVD technique. Bitstreams are inserted using the LSB technique from the last bit of each coefficient or pixel component. Like extraction, stego-media has a hidden message that can be found only through extraction. The hidden message embedded in the input image is turned into its output image by using the stego-image or output image of the embedding image. Steganography is the full process involved (Jain, 2018). This process entails enhanced security for data transmission over insecure networks.

Steganography and cryptography techniques can be used for the protection of any secret information. Steganography differs from cryptography in that, unlike cryptography, steganography never scrambles the text, it remains unchanged with the original cover, but contains information stored within. Therefore, steganography hides the data within the cover media in such a way that changes cannot be detected.

Steganography uses a cover image and a hidden image or message that is also a cover image. Each bit of the image is inserted on the LSB portion of the pixel.

The cover media uses VoIP or voice over IP while the secret data is an audio file in any of the formats described.

c. Image Steganography Using Pseudo Random Number Generation:

The concept of image steganography is to cover an image within another image. Color or RGB images or greyscale or BMP images can both be processed this way. Monochrome images are characterized by pixel intensities within the eight bits per pixel. A RGB image consists of 24 bits per channel of pixel intensity.

The purpose of this research study is to use pseudo random number generation in order to perform image steganography. The user must therefore request that a secret message be sent to the cover image. Pseudo random number generation, or PRNG, is used to establish an algorithm. A PRNG-generated channel will be used to generate the indicator channel. Additionally, this number will be assigned to the bit that will be randomly selected by adding the number of bits to the inserted message (Mandal and Khan, 2019). In each of the channels, three bits of the MSB of the indicator channel indicate how many pixels should be suppressed. The obtained bits and PRNG of each channel are then XORed together. According to the MSB of the indicator channel, the resultant number is hiding in the LSB channel. Repeat this process until no pixels are left.

4 Design Specification

A high-security encryption method should be developed in cloud computing databases to secure data in cloud storage. Before storing data in a cloud storage server, encryption can provide an effective way to secure the data. To implement and develop data transmission in Cloud security, cryptography and steganography are use techniques for encryption of data. Steganography and cryptography are both methods of encrypting and hiding communication data from unauthorized users. For developing and designing secure cloud data solutions, steganography is a good technique to use. Images, video, text, and audio are some of the ways to hide data in Steganography but hiding data from images is one of the most effective ones. The data in this project is encrypted and hidden using the image Steganography method. In addition to the Steganography method, using the Pseudo-Random Number Generator (PRNG) algorithm can be more efficient and useful. It is possible to create more significant and reliable data security cloud storage by using the Pseudo-Random Number Generation (PRNG) process with Image Steganography.

a. Steganography Design and Implementation

Utilizing digital image steganography techniques to develop and implement a secure database for Cloud computing. The image steganography is the best digital format for steganography and the one that can hide data securely so it can be used for steganography. The implementation of image steganography gives important levels of data security redundancy. Having redundant data provides better accuracy than using and displaying data objects alone. There are many digital image formats available over the internet, but the most common is Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF), and Portable Network Graphics (PNG). These formats are implemented and developed to hide the data in encryption mode. In data encryption, some data structures must be hidden using Bitmap (BMP) format. Images on computers can include several types of light intention in various

areas. Pixels are composed of numeric values which represent individual points and forms grids. On the Internet, most of the images are in the form of rectangular maps of the image's pixels, which describe the bits from which can find the pixel's location and color. Numeric bits in an image are known as bit depth, and they contain a number of bits for every pixel. Steganography is implemented by working with a larger image instead of a normal image. Steganography posed difficulties for implementing and processing the larger image, because of its greater bit depth. It is of utmost importance that images can be displayed in a longer time than usual and that Steganography processes can be corrupted if they are not compressed.

b. Image steganography techniques

Image steganography has been implemented using Image Domain and Transform Domain types of techniques. An image domain approach is also called spatial domain, which integrates the intensity of pixels directly into the message. Using transform domain, or frequency domain, to describe images, the image will first be transformed, and a message will then be embedded. In the image domain, bit-wise methods can be applied to bit insertion and noise manipulation and can sometimes be described as "simple systems"(Hu, et al. 2019). Steganography can be manipulated in the transform domain via image transformation and algorithm. It is very much efficient and safe to use all these methods since they can hide messages in more significant parts of the cover image. The Least Significant Bit (LSB) insertion offers high simplicity and ease of use than the other insertion techniques present in the domain. The image cover is embedded with the least significant bit (LSB). This bit represents the least significant data inside an image, in other words, it is the 8th bit from some or all of the bytes that become a bit of the secret message. To represent the insertion process using a byte representation, every RED, GREEN, BLUE colour component is used in the 24-bit image. As a result, the "Pseudo-Random Number Generation (PRNG)" algorithm is used to implement all the image insertion formats, and we will create the database with encrypted and hidden data behind the images. To compile the Jupiter file, you need to run the pseudo-random number generation (PRNG) algorithm. Using Python to develop the database of secure data in the Jupiter platform, implementing and developing cloud data security. The cover image is implemented with insertion and compression, as needed, but the format of the image remains the same. As a result, the cloud storage image that we designed, implemented, and developed conceals data from public view. Figure 1 illustrates the steps followed to conduct the Image steganography using PRNG.

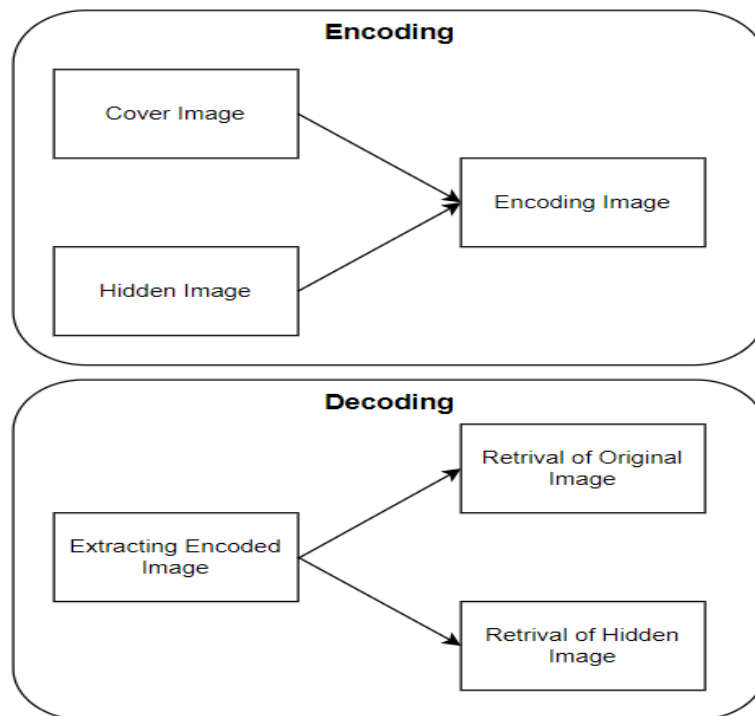


Figure 1: Flowchart of Image Steganography

For the explanation I have divided the flow of the code in to 2 section one is Encoding and second is Decoding. As name defined in the encoding section, we give 2 input images in that first data will be Cover image and the second is Hidden Image. In Cover image we will combine and merge the hidden text using the PRNG algorithm.

In PRNG the image will be turned in to binary code and loops as the matrix to add the hidden binary image column data with Cover binary image respectively. This generated the encoded binary image which is ready to transfer in the cloud system which is safe and secure to store in the cloud storage.

We need to decode the encoded image to show as original image to the use. So, we take the Encoded image which is in binary then convert it to decimal using the looping of matrix then at the end it gets the decoded image of the Hidden image and Cover image. And this decimal decoded image will be ready to view for the user.

5 Implementation

A python notebook environment with Jupyter compiler has been used for this research project. Using steganography for cloud data security, this research study aims to provide an overview on pseudo random number generation (PRNG) used for image steganography. According to the requirements of this research project, encoding and decoding methods are used for developing image steganography. Color images may be used as the message. STEGO's secret message can be found within this value. An additional decoding code is needed to extract the numerical values from stego-media to retrieve the hidden data. To do so, we need to discuss the embedding or encoding process.

Installing some of the packages required by the program must be done for the embedding process to succeed. Consider an open-source Python library such as the Image package from PIL. The PIL module is responsible for extracting pixels from images and converting them into the appropriate formats.

In the Figure 2 shows the input of the program which is Cover Image (main.png) and Hidden Image (hide.jpg).

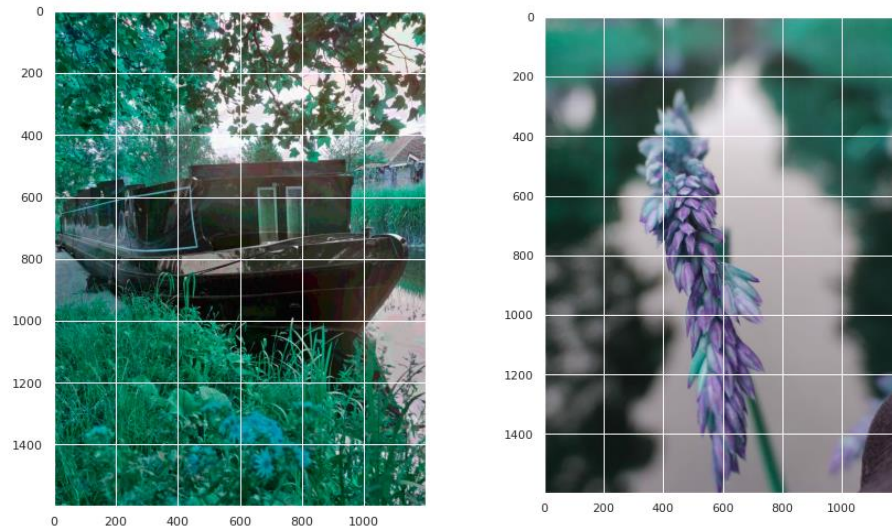


Figure 2: Cover Image (main.png) and Hidden Image (hide.jpg)

a. Image Encoding

Below section explains the encoding of the image to the stego-image.

The decoding function is used to replace the ASCII characters with a binary number. Any singular value can be added to a list without affecting the current list by applying the append operation (Hosam and Ahmad, 2019). Regardless of whether a fresh list is created, the modified values of the original list will be returned. When modifying the pixel values of an image based on 8-bit binary data, the `bincodedimage(image)` function is used.

An array of rows and columns of the cover image matrix will be created to store the binary form of the pixel stream. The images have zero-dimensional, one-dimensional, or two-dimensional shape. In this code we are using two-dimensional images, this work will be much more efficient (Ahmed and Abdallah, 2019). The image's decimal values will be converted to binary values by a for loop, and the output data will be stored in the `t` variable.

The next step in converting the binary original image to a binary coded format is encoding (SHANTHAKUMARI and MALLIGA, 2019). If a condition is implemented to verify the binary length of the secret image, this encoding will be performed on the cover image.

By this step we have a binary code of hidden and main image. A for loop will be executed from zero to the length of the binary hidden image. And this binary hidden row and column matrix will be added with respective original binary image row and column matrix. At the end of this method, we get binary image matrix contains of hidden data in it.

For the image to be displayed properly, the binary image needs to be converted into a decimal coded image following the successful execution of the encoding part. We will have the

matrix loop which runs until the rows and column size is larger or equal to the image size. At the end we will return the stego-image value that is held by the variable "t".

A method is used to show the stego-image and hide image within the console. The output stego-image is the same as the cover image which is shown in the below figure 3.

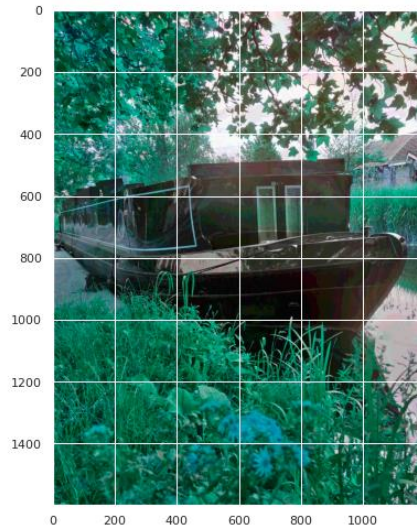


Figure 3: Output of the Stego-image (secret.png)

b. Image Decoding

In the below section we will decode the secret image generated from the encoding function.

Function to transform the image as binary image, once the transformation matrix is generated which will be passed to decode function.

Decode function will be a for loop of matrix it loops till the image size will be greater than or equal to the binary image size. In each loop the columns will be added with 0 value.

This returns the decoded binary image again a binary-to-decimal conversion is necessary during final execution in order to decode an image.

In the secret.png file, the final output of the decoded image will be stored. By decoding these lines of codes, the hidden image (figure 4) that is inserted when images are encoded will be created.

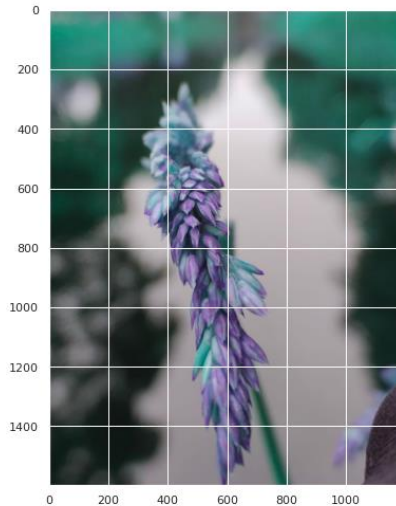


Figure 4: Output of the Decoded Image

6 Evaluation

In stenographic systems, image quality is the main objective. For evaluating the quality of an image, the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics are commonly used. PSNR is a metric used to determine if the embedded image has degraded since the cover image was created. A MSE is calculated by comparing two images. Signal-to-noise ratio (SNR) are used in imaging to assess image quality. In imaging systems, the sensitivity can be defined as the signal level that yields a threshold level of SNR.

Performance analysis of the PSNR, SNR value, and MSE value was calculated on the comparison with main and secret images and the respective values are shown in the table below.

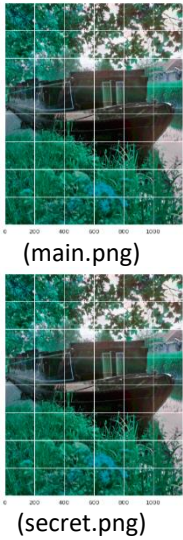
| Image Comparison | PSNR value | SNR value | MSE value |
|---|----------------|---------------|---------------|
|  <p>(main.png)</p> <p>(secret.png)</p> | 32.1537 | 7.8533 | 6.2929 |

Table 1: Performance analysis table

The table I shows the quality metrics for the cover and secret images. 'MSE' is relatively low. MSE values that are low indicate high PSNR values. This can be seen experimentally by looking at the PSNR values.

A PRNG was used to generate a sequence which tells what bit on each pixel is to be changed in (Lokhande et al., n.d.). This only affects the Blue channel. It is possible to hide data bits with the second, third, and fourth least significant bits of any given pixel. This avoids the first least significant bit. Using a PRNG, the sequence generated determines the least significant bit position to be used.

The layer selection scheme used in (M. et al., 2016) is (2-1-2). The Blue and Green channels of the first selected pixel are altered. The Blue channel of the second selected pixel is altered. Green and Blue are altered in the next iteration. This time, the secret bit is (3-2-3). The pixels were chosen using a PRNG.

The most common way to analyze a technique's security is to use histograms. The majority of steganography methods use histograms to detect hidden information. Thus, it is of critical importance that the histogram of the stego-image does not show obvious or blatant differences from the cover. The histograms of the cover image and the stego-image are shown in Table 2.


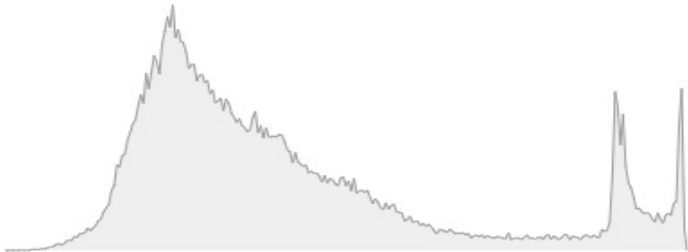

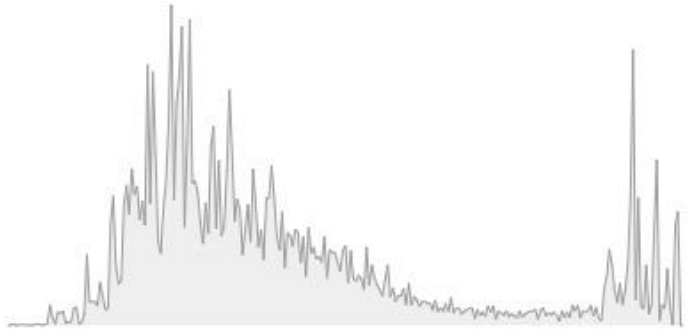
| Image Comparison | Histogram |
|---|--|
|  <p data-bbox="288 1335 411 1364">(main.png)</p> |  |
|  <p data-bbox="288 1753 411 1783">(secret.png)</p> |  |

Table 2: Histogram analysis table

As information bits are stored in a pixel, the capacity of any technique increases. Since the image's transparency depends on this decision, it is an important one. Steganography loses its

covert and stealthy qualities if the hidden bits cause blatant modifications in the image. According to the proposed method, the MSB of the indicator channel determines whether or not 6 bits per pixel should be hidden per pixel. The proposed technique can store up to three bits per pixel, which is higher than the 1-bit LSB or random bit substitution methods. As LSB substitution can hide 6 bits per pixel, its lower PSNR is compensated by its capacity.

In addition, the elaborate algorithm in the proposed method allows for both greater capacity and greater security.

7 Conclusion and Future Work

It refers to the technological development of the modern era that facilitates the growth of business models in all sectors. Many organizations, companies, and departments use this technology, such as IT, Communication, Education, banking, and health care departments. In the field of IT and telecommunications, it has the best impact on the security of online data storage. The cloud is a framework for storing data that can be accessed and sorted over the internet. Cloud security databases offer the benefit of allowing any organization to organize the database of the entire system, such as work data and employee information. As a result, cloud databases allow access to more data with less maintenance, reducing local storage requirements, and reducing the need for software upgrades. The security of online storage is vital to all aspects of Cloud Computing. Considering this, cloud storage security is a top priority over all the benefits. The more efficient and reliable way to improve data storage is through steganography and cryptography. A cryptographic system can hide data best with the help of image data hidden protection, and here we can use the same process to improve and develop a data security cloud. Audio, video and text can be used to hide data, but images are more efficient and safer. As the use of online internet communication technology grows, the privacy and security of data over the internet is a prime responsibility of cloud computing. In the following scenario, we are using the Steganography method along with the PRNG algorithm to implement and develop the best method for encrypting image data and hiding it. Users of cloud storage have full access to it over the online database storage system, which means it can be abused at any time by them or by others. Using this technique, we demonstrate to produce decent quality stego images with good PSNR values. Considering all the advantages of online cloud storage databases, privacy is the most key factor.

It is possible to implement location-based hiding in the future, as well as adding more filters and using the same Stego image with multiple filters. The embedding rate of steganography methods tends to be low. The immense capacity of video files and excellent imperceptibility of video files makes them a compelling substitute channel for images for information thrashing. The more difficult issue is to be able to embed a set of intercorrelated pictures into a compressed format in the future when the images are highly correlated.

References

- Abdullah, D.M., Ameen, S.Y., Omar, N., Salih, A.A., Ahmed, D.M., Kak, S.F., Yasin, H.M., Ibrahim, I.M., Ahmed, A.M., Rashid, Z.N., 2021. Secure Data Transfer over Internet Using Image Steganography: Review. *Asian Journal of Research in Computer Science* 33–52. <https://doi.org/10.9734/ajrcos/2021/v10i330243>
- Ahmed, O., Abdullallah, W., 2019. A Review on Recent Steganography Techniques in Cloud Computing. <https://doi.org/10.25007/ajnu.v6n3a91>
- Ajala, J.A., Singh, S., Mukherjee, S., Chakraborty, S., 2019. Application of Steganography Technique in Cloud Computing, in: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). Presented at the 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), pp. 532–537. <https://doi.org/10.1109/ICCIKE47802.2019.9004347>
- AlKhamese, A.Y., Shabana, W.R., Hanafy, I.M., 2019. Data Security in Cloud Computing Using Steganography: A Review, in: 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). Presented at the 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), pp. 549–558. <https://doi.org/10.1109/ITCE.2019.8646434>
- BanuPriya, R., Deepa, J., Suganthi, S., n.d. VIDEO STEGANOGRAPHY USING LSB ALGORITHM FOR SECURITY APPLICATION 9.
- Brindhashree, K., Prakash, S.J., 2020. Data security based on cryptography steganography combined with OTP algorithm and Huffman coding in the cloud environment. *International Research Journal of Modernization in Engineering Technology and Science* 2.
- Coverless Image Steganography: A Survey | IEEE Journals & Magazine | IEEE Xplore [WWW Document], n.d. URL <https://ieeexplore.ieee.org/document/8911367> (accessed 12.16.21).
- Deo, C.K., Singh, A., Singh, D.K., Soni, N.K., 2020. Developing a Highly Secure and High Capacity LSB Steganography Technique using PRNG, in: 2020 International Conference on Computational Performance Evaluation (ComPE). Presented at the 2020 International Conference on Computational Performance Evaluation (ComPE), pp. 136–140. <https://doi.org/10.1109/ComPE49325.2020.9200077>
- Dhawan, S., Gupta, R., 2021. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective* 30, 63–87. <https://doi.org/10.1080/19393555.2020.1801911>
- Hosam, O., Ahmad, M., 2019. Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. *International Journal of Computational Science and Engineering* 19, 153. <https://doi.org/10.1504/IJCSE.2019.100236>

Hu, D., Wang, L., Jiang, W., Zheng, S., Li, B., 2018. A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks. *IEEE Access* 6, 38303–38314. <https://doi.org/10.1109/ACCESS.2018.2852771>

Hussain, M., Wahid, A., Idris, Y., Ho, A., Jung, K.-H., 2018. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication* 65. <https://doi.org/10.1016/j.image.2018.03.012>

Jain, M., 2018. Medical Image Steganography using Dynamic Decision Tree , Piecewise Linear Chaotic Map , and Hybrid Cryptosystem [WWW Document]. URL <https://www.semanticscholar.org/paper/Medical-Image-Steganography-using-Dynamic-Decision-Jain/4cb8599146e14fff3693263a3f5cf88e8a070066> (accessed 12.16.21).

Lokhande, U., Gulve, A.K., Professor, A., n.d. Steganography using Cryptography and Pseudo Random Numbers.

M., M., A., A., A., F., 2016. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. *ijacsa* 7. <https://doi.org/10.14569/IJACSA.2016.070350>

Mandal, S., Khan, D.A., 2019. A Dynamic Programming Approach to Secure User Image Data in Cloud Based ERP Systems, in: 2019 Fifth International Conference on Image Information Processing (ICIIP). Presented at the 2019 Fifth International Conference on Image Information Processing (ICIIP), pp. 91–96. <https://doi.org/10.1109/ICIIP47207.2019.8985974>

Mary, B.F., Amalarethinam, D.I.G., 2017. Data Security Enhancement in Public Cloud Storage Using Data Obfuscation and Steganography, in: 2017 World Congress on Computing and Communication Technologies (WCCCT). Presented at the 2017 World Congress on Computing and Communication Technologies (WCCCT), pp. 181–184. <https://doi.org/10.1109/WCCCT.2016.52>

Mustafa, G., Ashraf, R., Mirza, M., Jamil, A., Muhammad, 2018. A review of data security and cryptographic techniques in IoT based devices. <https://doi.org/10.1145/3231053.3231100>

Osuolale, F., 2017. Secure Data Transfer Over the Internet Using Image CryptoSteganography. *International Journal of Scientific and Engineering Research* 8, 1115. <https://doi.org/10.14299/ijser.2017.12.002>

Rahman, M., Khalil, I., Yi, X., Dong, H., 2017. Highly Imperceptible and Reversible Text Steganography Using Invisible Character based Codeword.

Research, J.-J. for, Bandyopadhyay, S., 2018. An Ameliorate Image Steganography Method using LSB Technique & Pseudo Random Numbers | J4RV4I9001. *J4R - Journal 4 Research*.

Reza, H., Sonawane, M., 2016. Enhancing Mobile Cloud Computing Security Using Steganography. *JIS* 07, 245–259. <https://doi.org/10.4236/jis.2016.74020>

Rosalina, R., Hadisukmana, N., 2019. Implementation of Securing Data in the Cloud using Combined Cryptography and Steganography. *Jurnal Teknik Informatika dan Sistem Informasi* 5. <https://doi.org/10.28932/jutisi.v5i3.1922>

Saa, P., Costales, A., Moscoso-Zea, O., Luján-Mora, S., 2017. Moving ERP Systems to the Cloud - Data Security Issues. *Journal of Information Systems Engineering & Management* 2. <https://doi.org/10.20897/jisem.201721>

Sarkar, M.K., Chatterjee, T., n.d. Enhancing Data Storage Security in Cloud Computing Through Steganography.

SHANTHAKUMARI, R., MALLIGA, S., 2019. Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment. *Sādhanā* 44, 119. <https://doi.org/10.1007/s12046-019-1106-0>

Suganthi, S., Selvi, F.K.M., 2020. Learning of Steganography Algorithm 9, 7.

Zhang, Y., Qin, C., Zhang, W., Liu, F., Luo, X., 2018. On the fault-tolerant performance for a class of robust image steganography. *Signal Processing* 146, 99–111. <https://doi.org/10.1016/j.sigpro.2018.01.011>