



**Title:**

**Concealing Existence of Secret Message through a  
Novel and Secure Image Steganography Algorithm  
Appertaining to Arithmetic Subtraction.**

Supervised By

**Md Maruf Hassan**

**Associate Professor**

Department of Software Engineering

Submitted By

**Jyoti Chandra**

Student ID: 201-44-194

A thesis submitted in partial fulfillment of the requirement for the degree  
of Masters of Science in Software Engineering

**Department of Software Engineering  
DAFFODIL INTERNATIONAL UNIVERSITY**

Fall – 2022

### APPROVAL

This thesis/project/internship titled on "Concealing existence of secret message through a novel and secure image steganography algorithm appertaining to arithmetic subtraction", submitted by Jyoti Chandra, ID: 201-44-194 to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Masters of Science in Software Engineering and approval as to its style and contents.

#### BOARD OF EXAMINERS




Chairman

Dr. Imran Mahmud  
Associate Professor and Head  
Department of Software Engineering  
Daffodil International University



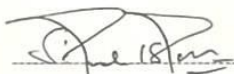
Internal Examiner 1

Dr. Md. Fazla Elahe  
Assistant Professor and Associate Head  
Department of Software Engineering  
Daffodil International University



Internal Examiner 2

Afsana Begum  
Assistant Professor  
Department of Software Engineering  
Daffodil International University



External Examiner

Dr. Md. Saiful Islam  
Professor  
The Institute of Information and Communication Technology (ICT)  
Bangladesh University of Engineering and Technology (BUET)

## DECLARATION

I announce hereby that I am rendering this study document under the supervision of **Md. Maruf Hassan**, Associate Professor, Department of Software Engineering, Daffodil International University. I, therefore, state that this work or any portion of it was not proposed here therefore for Master's Degree or any graduation.

Certified by:

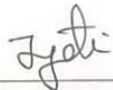


---

**Md. Maruf Hassan**  
Associate Professor

Department of Software Engineering  
Faculty of Science & Information Technology  
Daffodil International University

Submitted by:



---

**Jyoti Chandra**  
Id: 201-44-194

Batch: 12  
Department of Software Engineering  
Faculty of Science & Information Technology  
Daffodil International University

## ACKNOWLEDGEMENT

I had several difficulties when writing my thesis. Whatever the case, it would not have been possible without the kind support and aid of several people. Each of them can make me want to widen my attention. I am very appreciative of Daffodil International University's direction, **Md. Maruf Hasan's** constant monitoring, and their aid with the project. They also gave me important information concerning the trip. I want to explicit my grace to my parents, classmates, and DIU members for their kind assistance and comfort in helping us to do this task. I want to sincerely thank everyone for their contributions and acknowledge their efforts. My thanks and appreciation are also extended to my adventure companion, as well as to those who have faithfully helped me with their skills.

## TABLE OF CONTENT

<b>APPROVAL</b>	<b>iError! Bookmark not defined.</b>
<b>DECLARATION</b>	ii
<b>ACKNOWLEDGEMENT</b>	iv
<b>TABLE OF CONTENT</b>	v
<b>LIST OF TABLE</b>	vii
<b>LIST OF FIGURE</b>	viii
<b>ABSTRACT</b>	ix
<b>CHAPTER 1: INTRODUCTION</b>	1
1.1 Background	1
1.2 Motivation of the Research	5
1.3 Problem Statement	6
1.4 Research Questions	7
1.5 Research Objectives	6
1.6 Research Scope	6
1.7 Thesis Organization	7
<b>CHAPTER 2: LITERATURE REVIEW</b>	8
<b>CHAPTER 3: METHODOLOGY</b>	10
3.1 Encrypting Secret Message	11
3.2 Pixel Filtering Algorithm	12
3.3 Steganographic processes	13
3.4 Algorithm for embedding and retrieving.	16
<b>CHAPTER 4: RESULTS AND DISCUSSION</b>	18
4.1 Result Discussion	18
4.2 Implementation on Desktop App	23
<b>CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS</b>	23
<b>REFERENCES</b>	24

## LIST OF TABLES

Table 1:Quality measurement metrics of the projected method <b>Error! Bookmark not defined.</b>	
Table 2: Comparison among recent steganographic techniques	21
Table 3: Comparison among recent steganographic techniques	
<b>22Error! Bookmark not defined.</b>	

## LIST OF FIGURES

Figure 1: General Block Diagram of Steganography	2
Figure 2: Types of Steganography	2
Figure 3: AES encryption	3
Figure 4: Even pair-based pixel filtering system	13
Figure 5: Odd pair-based pixel filtering system	13
Figure 6: Embedding Process	15
Figure 7: Retrieving Process	16
Figure 8: Cover Images	19
Figure 9: Desktop Application	23

## ABSTRACT

Currently, information represents one of the most crucial instruments, and it must properly address the rising information security threat. Additionally, when data is delivered, it is tracked and modified remotely through the internet. As a result, cryptography or even steganography are two main methods for enhancing security during transmission. In cryptography, data is encoded to cipher texts using a non-public key, but regardless of how effective the encryption is, the message's corporeality is apparent to others. Contrarily, steganography keeps many secret information hidden through a common-secret file to thwart visual inspection. In this study offered a fresh data-concealing method based on LSB image steganography, in which only the reader picture pixels are used to hide sensitive information. An LSB steganography-secured word is used together with image pixel intensities to filter the whole picture and identify the seeker pixel in order to do this. To increase security, secret data is embedded using the subtracting method, as well as the hidden message is then encrypted, and using the AES encryption before applying steganography. In order to control the generated stego image quality, MSE as well as PSNR measurements are scaled in the experiment. The stego image has an increased PSNR but a smaller MSE value when compared to other evaluated styles, highlighting the rigidity of the proposed approach.

**Keywords:** YCbCr, AES, Image Steganography, SHA3-512, Pixel selection technique, LSB



# CHAPTER 1

## INTRODUCTION

### 1.1 Background

The usefulness of the internet is now enriching quickly. The internet's utility is currently growing. Security on the internet and communication space is one of the most essential subjects that people are interested in. Humans communicate with one another constantly because they are social animals. Every person has a unique communication style, and sometimes they want to discuss private information with the intended person [1]. However, it couldn't communicate data or information to the specified recipient on a constant basis in order to remain safe and secure. To protect actual data, data must be supplied covertly. Consequently, data encryption is required for secure communication between two entities. Cryptography is the most widely used method of data encryption. However, as is well known, relying only on encryption has security risks since nonpublic information may be linked to it [2]. In contrast, steganography hides the secret communication using the cover medium so that no one can see it. The fundamental advantage of steganographic rendering is that it conceals the data beneath a cover medium, keeping it hidden from everyone save the beneficiary. Steganography is an important and effective technique that furthers high-level security, particularly by breaking encryption [3]. Steganography conceals the genuine character of the message, disabling the assumption of communication on the part of outsiders. In this approach, information containing sensitive data is transferred into an unanticipated channel [4].

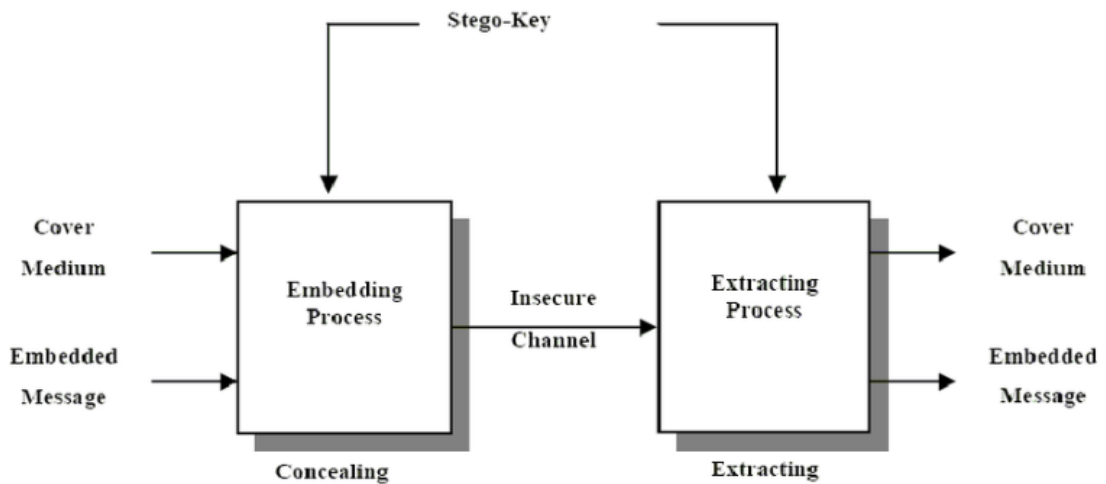


Figure 1: General Block Diagram of Steganography [5]

Figure 1 depicts the contours of the steganography technique. The many types of cover media that we may employ steganography on are numerous. Sensitive information is hidden via steganography methods in carrier media including images, sounds, data, and film lines [6].

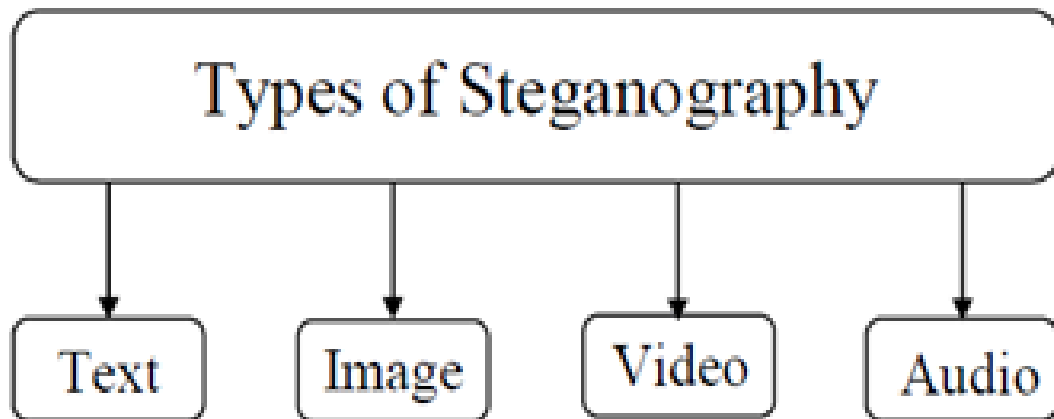


Figure 2: Types of Steganography

Figure 2 shows a variety of potential cover media where steganography may be used successfully. The most comprehensive and varied medium for protecting educational content is, however, the image. The human eye becomes more sensitive to brightness

than chrominance as we become older. Steganography uses this flaw in the eye's ability to see image lines to exchange data. We used to a 24-bit hue image by way of the publication's concealment image. The frequency sphere and the spatial sphere are the two components of the image steganography system [7]. The original image is used, and a mathematical procedure is used to convert the image into a substitutive domain in the frequency domain [8]. However, the spatial domain is adequate to instantaneously direct ahead and change the original image [9]. The most popular and fundamental kind of spatial sphere steganography is the least significant bit (LSB) approach, in which the secret communication bits are used in lieu of the picture's LSB bit [10]. There are two categories of LSB photo steganography: non-filtering and filtering. Each cell in the picture is utilized to lack of standardization obscure information in the non-filtering approach., whereas not all pixels in the filtering method are. The filtering algorithm takes into account image quality and chooses seeker pixels to hide data [11]. In this work, we used LSB filtering photo steganography. In such circumstances, the secret information can only be secured using steganography. As a consequence, we combined the recommended steganography with the most sophisticated AES encryption technique. The core principles of AES encryption are shown in Figure 3.

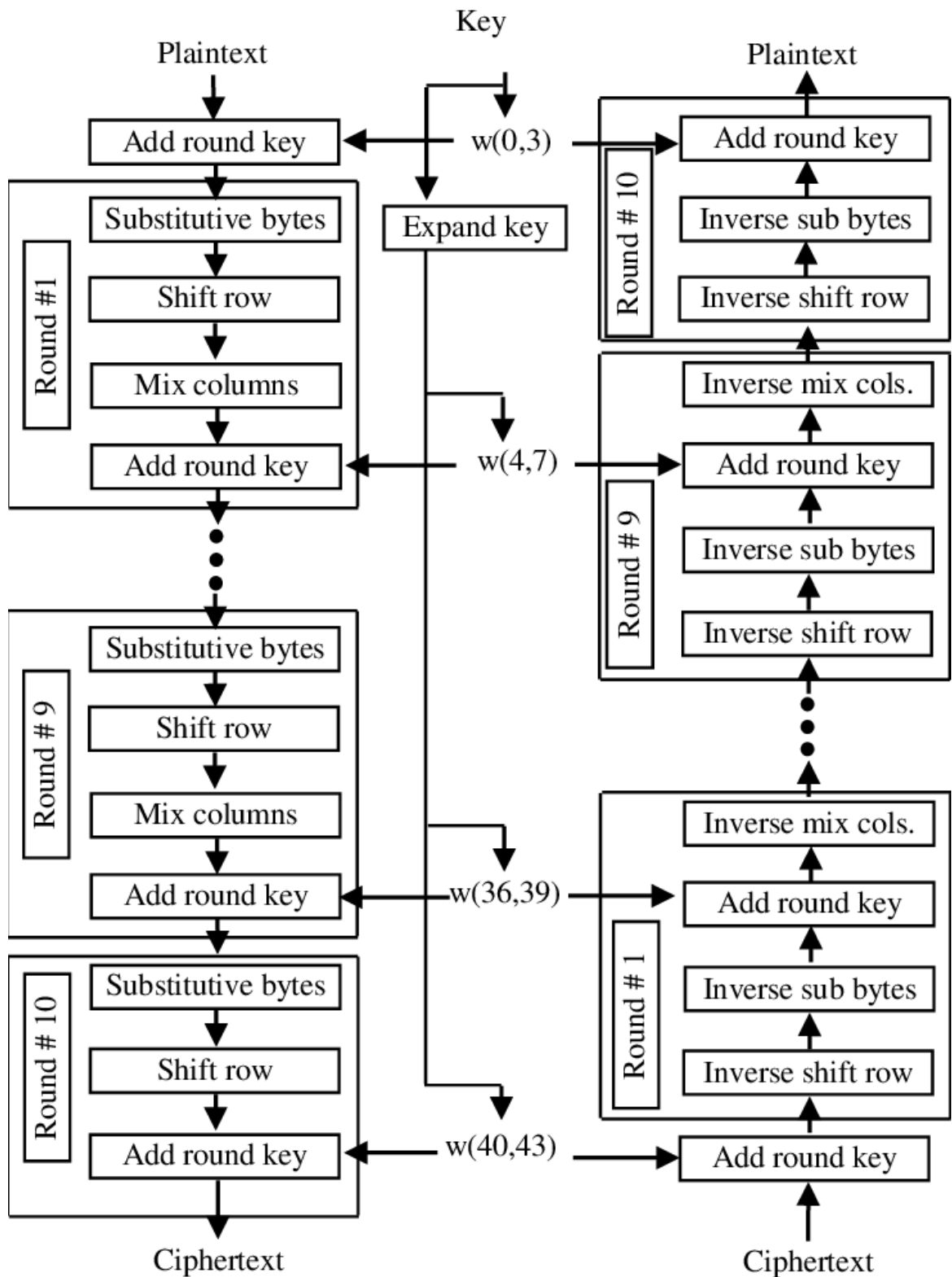


Figure 3: AES encryption [13]

In this study, we use a user-defined term to qualify the conventional LSB technique.

The certification shows of encryption as well as obfuscation techniques that is presented in this paper is done by conducting a Subtraction procedure on a document text communication module with an LSB slot, making it both easy to use and very efficient. The bits that represent any key. Key Benefits From our proposed scheme as follows -

- 1) The most powerful symmetric algorithm on a Subtraction operation with critical arbitrary automatic extraction of LSB for pixel values for the cover photo.
- 2) Expansion and improvement of the old-style LSB masking system meanwhile the gratified of the clandestine annuity book is being interpreted.
- 3) Expand and improve capacity Several confidential textbook submissions have been withdrawn since our proposal. The system can be applied to altered proportions of painted images.

The remaining portion of this paragraph is organized as follows: The Related Research is presented in Section 2, the Justification for the Proposed Approach is described in Section 3, the Outcomes are simulated in Section 4, and Interactions are described in Section 4. The completion of the job is presented in Section 5 as a whole.

## **1.2 Motivation of this Research**

Over the past few years, the internet has developed into a large technological backbone for cutting-edge industrial activities. Online hosting has lately replaced organizing software in colorful organizations. Internet users and drug users who access such websites for data have access to their services. To identify drug users affiliated with a

certain group, they have used the word-based authentication approach, which is currently weak. A number of techniques have been created by interlopers to defeat authentication systems, which might lead to theft, abuse, or loss of private data. Picture steganography, which is hard to detect and may close the gap in pixel selection manner, is the main driving force behind the development of a security strategy that would give redundant sub caste in authentication system.

### **1.3 Problem Statement**

The process of hiding data or material in a digital file or medium, such as a picture, audio, or video file, is known as information hiding in digital media. The purpose of information concealing is to guard against unwanted access to and alteration of the data. Numerous techniques, including as steganography, cryptography, watermarking, and digital signatures, may be used to achieve this. Making ensuring that the data is secure and hidden from unauthorized users while yet allowing authorized users to access the data is tricky when it comes to information concealment. Although cryptography is a crucial component of security, it is insufficient on its own. Data and communications are protected by cryptography, but additional security concerns like authentication, access control, and vulnerability management are not covered. Additionally, cryptography does not defend against nefarious parties that are able to access the data or communications. Therefore, in order to offer a complete security solution, cryptography should be used in concert with other security methods like authentication, access control, and vulnerability monitoring. While evaluating the primary data was collected, it was noted that different experimenters have combined cryptography and steganography for authentication, but in steganography, they used traditional pixel

selection techniques that are easy to detect and particular behavior may be able to recognize the existence data using steganalysis, and in cryptography, they used a hash function like Sha-256, SHA-0, BASE64, or SHA-1 that has some areas of weakness that can be exploited by dazzling table attack. In addition, data protection using steganography is effective against unwanted access. It may be used to conceal sensitive data so that no one can see it, making it impossible for anybody to discover the data's existence. As it is difficult for other parties to intercept the data, it may also be used to securely transport data across the internet or other networks. Steganography may also be used to watermark digital material to indicate the source of the information, which is another way it can be used to protect intellectual property.

#### **1.4 Research Questions**

Question 1: Is the anticipated increased data concealing model operational?

Question 2: Is the completed authentication approach as effective as the other authentication procedures in terms of results?

#### **1.5 Research Objectives**

1. The most powerful symmetric algorithm on a Subtraction operation with critical arbitrary automatic extraction of LSB for pixel values for the cover photo.
2. Expansion and improvement of the old-style LSB masking system from the time when the gratified of the clandestine pension book remains translated.

3. Expand and improve capacity several confidential textbook submissions have been withdrawn since our proposal. The system can be applied to different sizes of colored images.

## **1.6 Research Scope**

Numerous groups offered their assistance to drug users online. As a result, identification of their stoner depends on verification. In recent years, hackers have devised a number of techniques for disabling authentication systems. We must keep enhancing this sector's security. There are thus several exploratory compasses in this area.

## **1.7 Thesis Organization**

The analysis in this work makes use of the IEEE representation system. The five chapters that make up the article are addressed below-

Chapter 1: An overview of the exploration setting, provocation, problem statement, and objects is given in this chapter.

Chapter 2: This chapter covers affiliation with a project and identifying the exploration gap.

Chapter 3: The exploration methodology and approach will be used throughout the trip.

Chapter 4: The experimental results are compared to being methodologies.

Chapter 5: The exploration expansion, research restrictions, and the direction of the forthcoming exploration endeavor are all presented.



## CHAPTER 2

### LITERATURE REVIEW

While doing the research, numbers on image steganography and cryptographic hash for authentication were discovered. The following is a discussion of those interconnected mechanisms. Combining obfuscation techniques with cryptography may result in a more reliable and resilient medium since it has been observed that using either one alone is insufficient for full or adequate information security, in this segment, colorful lessons for perfecting in addition ornamental Secret dispatches hidden in cover image lines will be banded

The application of steganography principles to cover different media has been shown in a number of ways. A technique that combines image steganography and encryption was presented by Islam et al. [14]. Before overlaying the image, the secret message is first encrypted using the AES encryption procedure. They also applied the concept of filtering, which involves using some of the image's pixels to obfuscate information rather than all of them. A technique for hiding private information during communication that combines data encryption and visual concealment was put out by Mukhedkar et al. [15]. Data bits were concealed in the LSB position and the Blowfish Algorithm was used to encrypt the picture. An LSB method that Singh et al. [16] described, involves hiding peek data in non-adjacent pixel regions of the chosen image. The attacker is unable to identify the corporality of secret data bits on the edges because the pixels on the edges are brighter and more dark than their neighbors. A unique technique for fusing grayscale image steganography in the spatial realm with encryption was put out by Joshi and Yadav [17]. This method encrypts the secret message using

the Vernam cipher algorithm. Furthermore, the LSB bit positions of the pixels include the ciphered data. The left shift and XOR procedures are also performed. The pixel valuation-based measurement method employed in the LSB steganographic methodology was looked at by Li et al. [18]. A photo encryption method based on the Rubik's cube was created by Loukhaoukha et al. [19]. The XOR technique is then applied in rows and columns once the image has been scrambled. The link between the original and the ciphered image becomes unclear as a consequence. An method to text medium steganography was put out by Majeed et al. A simple steganographic method is suggested by Ghosal [21] in which the number of 1s and 0s in the red building block are first counted. Additionally, the technique calculates their tyrannous difference, and the outcome is disassociated by 2. The resultant number of bits is therefore hidden in another color building block (Green and blue). Using the higher LSB bit is a method for data concealment that was put out by Kaur et al. [22]. Additionally, data size was decreased by using the LZW compacting technique. The LSB image steganography approach was introduced by Ren-Er et al. [23], in which the secret data is encrypted using DES before embedding. Actual test results are used in a grayscale image that serves as the cover spitting image as well as an RGB paints that serves as the concealed image in a steganography approach developed by Raniprima et al. [24]. An undisclosed image is ciphered by means of the Rubik's chop method, which modifies the positions of pixels in a digital image, for even more realistic security. The method Phadte and Dhanaraj [25] developed combines Steganography and Cryptography. To hide critical information, this system uses the chaotic proposal to encrypt this performing stego image. The method developed by Broda et al. [26] employs an image color model to hide information in textbook form. During the conversion from RGB to YCbCr, there

is no loss of confidential information. Charan et al. [27] developed a method for obscure secret information in a color image using the LSB replacement technique. The confidential data is first expressed in code by means of the Caesar code method, and then the put into code data is embedded into the image. A hybrid approach that combines segmentation and data hiding was described by Khalaf and Sulaiman [28]. Two RGB channels are used to mask the third channel's private information. Using one channel as an indicator route, the other channels calculate the number of ones along the chosen index path. A steganography method was developed by Emad et al. [29] to conceal a data bitstream in the LSB bits. The system approximates grayscale images using the integer wavelet transform (IWT). Digital watermarking using LSB and ANN systems to conceal concealed information was proposed by Deeba et al. [30]. A digital image is concealed within another digital image using the LSB approach, and the hidden data is revealed using ANN. In [31], Alam et al. proposed a technique for pixel identification that are used to include concealed data by using an 8-directional pixel selection algorithm. They used 1 bit LSB for embedding, which produces good PSNR, however the pixel selection method is static, which might be a weakness in the model. The LSB replacement strategy was first presented by the authors in [32], and it is also the most straightforward and widely used system when compared to the other varieties. The cover image looks less hazy with this technique since the only modification made at the LSB position is "1". The main drawback of the model is that the LSB technique used a standard zig-zag strategy, which is very well-liked by invaders but results in greater PSNR and lower MSE values. Information concealment and digital image encryption by Chaudhary and Paras [41] make secret data and digital photos more secure by using LSB technology and the Advanced Encryption Standard (AES) algorithm. We use the

AES encryption technique to encipher the embedded image and the LSB technology to hide data in pictures. Many picture data concealing strategies are included in the spatial domain method. The LSB substitution technique is the most straightforward and widely used of the other techniques. This reduces blur on the cover image since there is only one alteration at the LSB location, "1." A greater PSNR and a lower MSE value are produced by the LSB method. We found several ways to hide data using colored images. The HLSB method for the RC4 stream cipher is used in M.H. Abood's [42] efficient image encryption approach, where steganography and a hash function are used to encrypt and decode the RGB pixels. His LSB insertion method has an MSE of 0.03 and a PSNR of 63 dB. A method for transferring information covertly using grayscale image steganography was created by J. Baek et al. a bit was shown on a particular pixel using XOR. M. Sengupta, J.K. Mandal, and [44] Based on fidelity, the data integration technique with the minimum variance is recommended. In this instance, the byte's two bits between the LSB and the fourth bit toward the MSB are modified through the use of random replacement sites. In order to conceal text in color images with greater PSNR and lower MSE values for a variety of images, Deepak Kumar [45] adopted the YCbCr color model.

The outcomes were improved by effectively enforcing a feline Map (ACM) synthesis with RSA and afterwards overlaying the coded outcome in a cap picture using a 2 different LSB steganography technique. By initially shortening the transmission and then including the AES technique, Sofyane et al. [46] improved picture steganography. Since the messages are divided into two corridors and transmitted individually, De Rosal et al. [47]. employment of maximum and exponent functions improves communication security. The Arindam et al. [48] simple XOR binary grounded

technique is mandated. They modified various LSB procedures in their research by including a sequence method for pixel choosing. Three bits of MSB were utilized as the encrypt key by Yani et al. [49] and a three-time XOR procedure was suggested for textbook deliveries. In this research, a straightforward and efficient method of a double XOR operation with a genuinely random key is carried out prior to bedding the text employing key elements of this system's essential production idea without the requirement to generate or transmit a crucial. The most significant bits (MSB) of cover and stego-image picture pixels will automatically generate a key that is utilized by both the recipient and the sender parts; the only information we need to shoot is the duration of stoner simple textbook conversation. We suggested saving several initial bytes (always the first 32 bytes) of the cover image for this purpose in order to extend the length of stoner textbook transmission and to detect alternative LSBs in order to prevent the washing of secret classroom dispatches. The HLSB system for the RC4 sluice cipher is used in M.H. Abood's [50] efficient image encryption scheme, and the RGB pixel is translated and deciphered via steganography using a hash function. His LSB insertion technique has a 0.03 MSE and a 63 dB PSNR. A covert information transfer system utilizing argentine-scale image steganography was introduced by J. Baek et al. [51]. A bit display on a particular pixel bit was carried out using XOR. J.K. Mandal, M. Sengupta, and [52] proposed minimal friction for the integration of data, based on commitment. In this instance, two bits by the byte between the LSB and up until the fourth bit towards MSB are modified using random relief places. Deepak Kumar [53] implemented color picture caching using the YCbCr color model, which has superior PSNR and lower MSE values for various images. In the spatial realm of picture steganography, T. Bhuiyan et al. [54] described a method for concealing information

that included taking the message bit, doing an XOR operation with each RGB element's seventh bit, and thereafter embedding the result in the RGB material's 8th couple of moments. They did, however, employ a zig-zag pixel selection approach, which is a conventional pixel selection technique that selects pixels from the beginning of images, perhaps making it simpler to detect the existence of hidden data.

To address these issues, we used the subtractions operation with the LSB technique with a basic pixel selection technique to reduce time, where we used [33] Peak Signal-to-Noise Ratio (PSNR), Mean Absolute Error (MAE), Signal Noise Ratio (SNR), Mean Square Error (MSE), Root Mean Square Error (RMSE), and embedding time metrics, which can provide us with a better technique than various techniques, There Our suggested technique also produces higher-quality images than existing ways .

## CHAPTER 3

### RESEARCH METHODOLOGY

Image cryptography is an image transformation process to ensure its security. The safety of images has become increasingly important because of the rapid evolution of the Internet in today's digital world. Increased attention has recently been paid to the safety of digital images and many different techniques for encrypting images have been introduced for this purpose. An automated two-layered safe data hiding technique for picture steganography employing 1-bit LSB and a zig-zag pixel selection approach has been shown in this study, with the encryption system and steganography perpetration discussed in depth in the following subsections.

#### 3.1 Encrypting the Secret Message

The user must enter the secret data into our suggested tool, which will decrypt it automatically when it is entered. It is translated using AES, a widely used and safe symmetric encryption technology that may render data blocks utilizing symmetric keys of 128, 192, or 256 bits gradationally, and which uses the same cryptographic keys to crack and decrypt secret data. Still, in this study, a 128-bit essential length was employed to encrypt the secret data, which produces better results at a faster rate and consumes less RAM [27]. Although a critical length of 128 bits is unbreakable, [28] it is handed from the computerizing function automatically. Thus, 128-bit AES was established with the purpose of ensuring data security for everybody, regardless of whether it was plucked from video frames or not. For critical lengths of 128 bits, the duplication cycle number is 10 rounds. Each round has the four following stages: SubBytes, ShiftRows, MixColumns, and AddRoundKey. SubBytes is a byte negotiation technique that passes each byte through a separate system before returning

a new value. It also employs its hexadecimal logic to patch the byte into another value using the S-box table. In the ShiftRows stage of AES, each row of the cipher's 128-bit internal state is shifted. As long as rotation offers prolixity, for the AES, the MixColumns method is important. The branch number guarantees that any of the AES's constant four rounds have at least 25 active S-Boxes, protecting the AES from the difference and direct cryptanalysis. The colored rounds employ a separate 128-bit round key computed from the core AES key. The entire AES technique is carried out via a function written in the C Sharp computer language. After encrypting the secret message, the ciphertext is ready to be embedded into the cover carrier, which is converted to PNG image-structured pictures created in C Sharp.

$$\text{1st-pixel position } (X1, Y1) = (W/2-3, 1) \quad (1)$$

$$\text{2nd-pixel position } (X2, Y2) = (W, H/2 - 3) \quad (2)$$

$$\text{3rd-pixel position } (X3, Y3) = (W/2+3, H) \quad (3)$$

$$\text{4th-pixel position } (X4, Y4) = (1, H/2+3) \quad (4)$$

### **3.2 Algorithm for embedding and retrieving**

Those pixels are used to contain metadata that is needed in the retrieval process to determine the AES key and message size, as well as the filtering pixels algorithm. Knowing the filtering method will allow our system to obtain filtering pixels where the secret message bit is stored in the embedding approach. Then, to obtain the secret message bit, we will do a Subtractions operation with the 6th and 7th indexed bit for RGB blocks. After obtaining the bits based on message size, we may decode the secret



message using the AES key and obtain the desired plain text that was hidden.

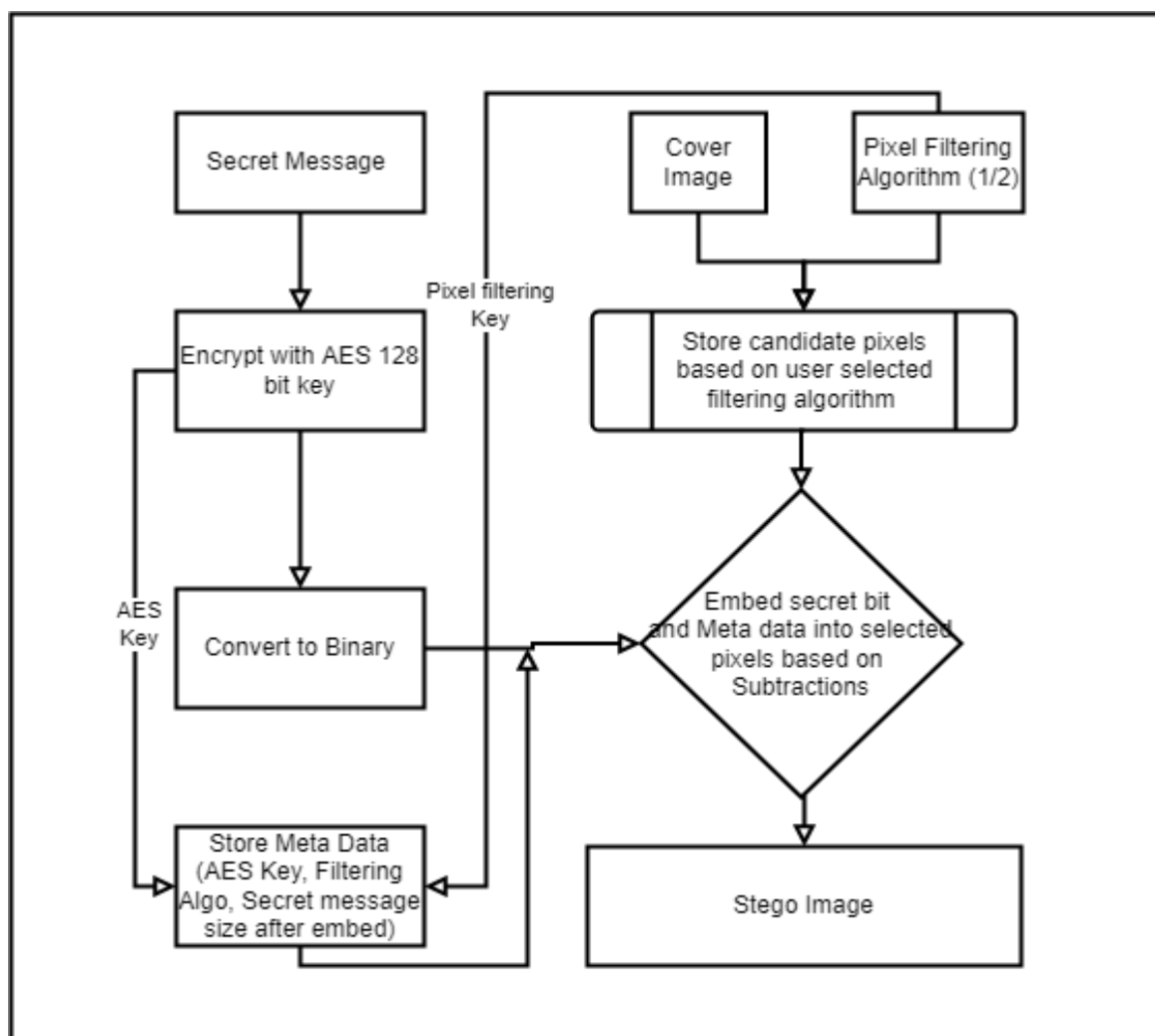


Figure 4: Embedding Process

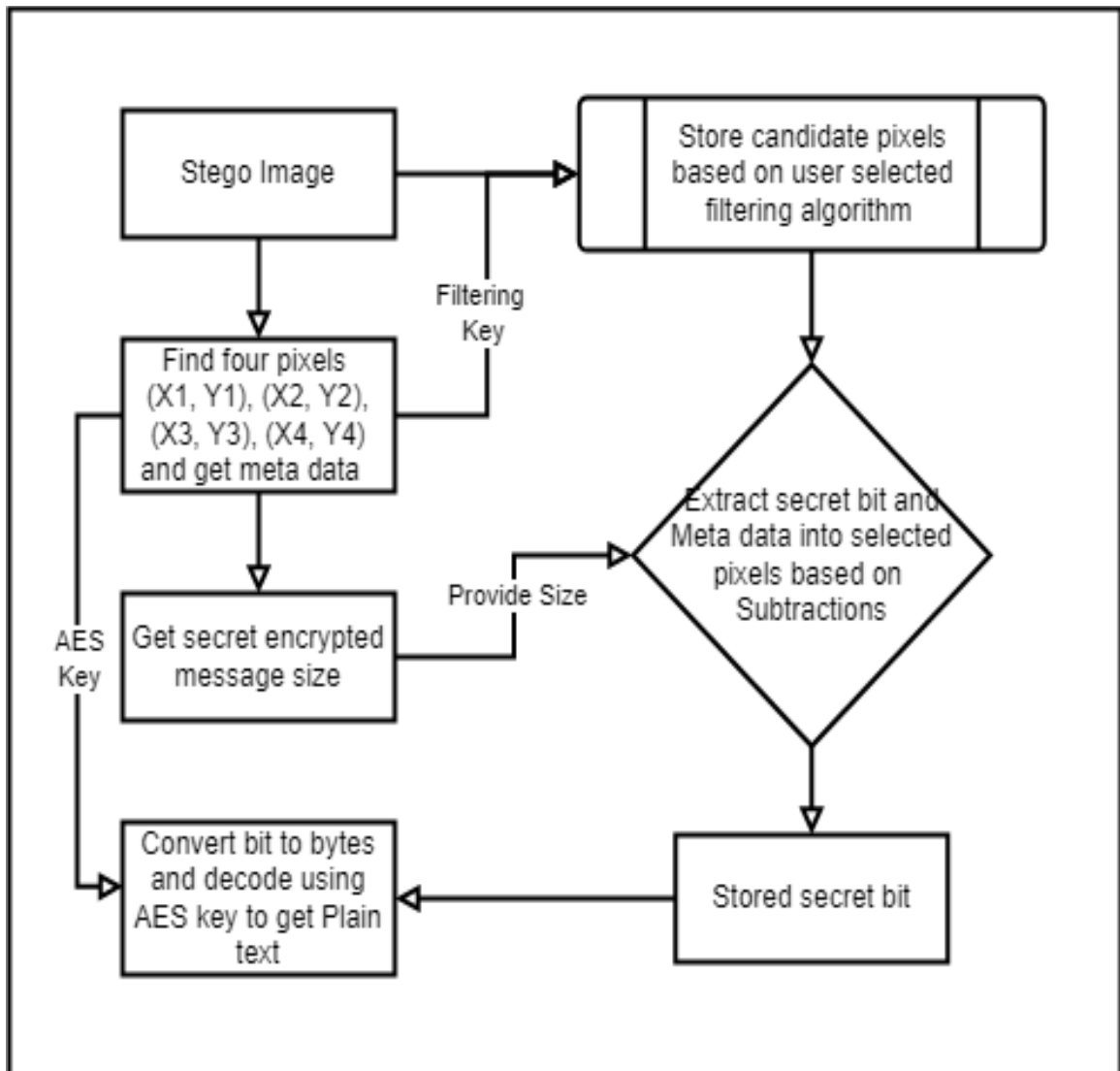


Figure 5: Retrieving Process

The user must submit a secret message, cover picture, and pixel filtering method throughout the embedding procedure. The machine will then initially load the specified information into memory. Second, the AES key is produced at random using 128 bits. The system, on the other hand, will begin filtering pixels based on the pixel filtering algorithm and store them in a pixel list for use in the embedding process. These pixels are secondhand to pigskin clandestine bits from the encoded message that was transformed by the AES key. The retrieving procedure, on the other hand, is the inverse of the embedding process

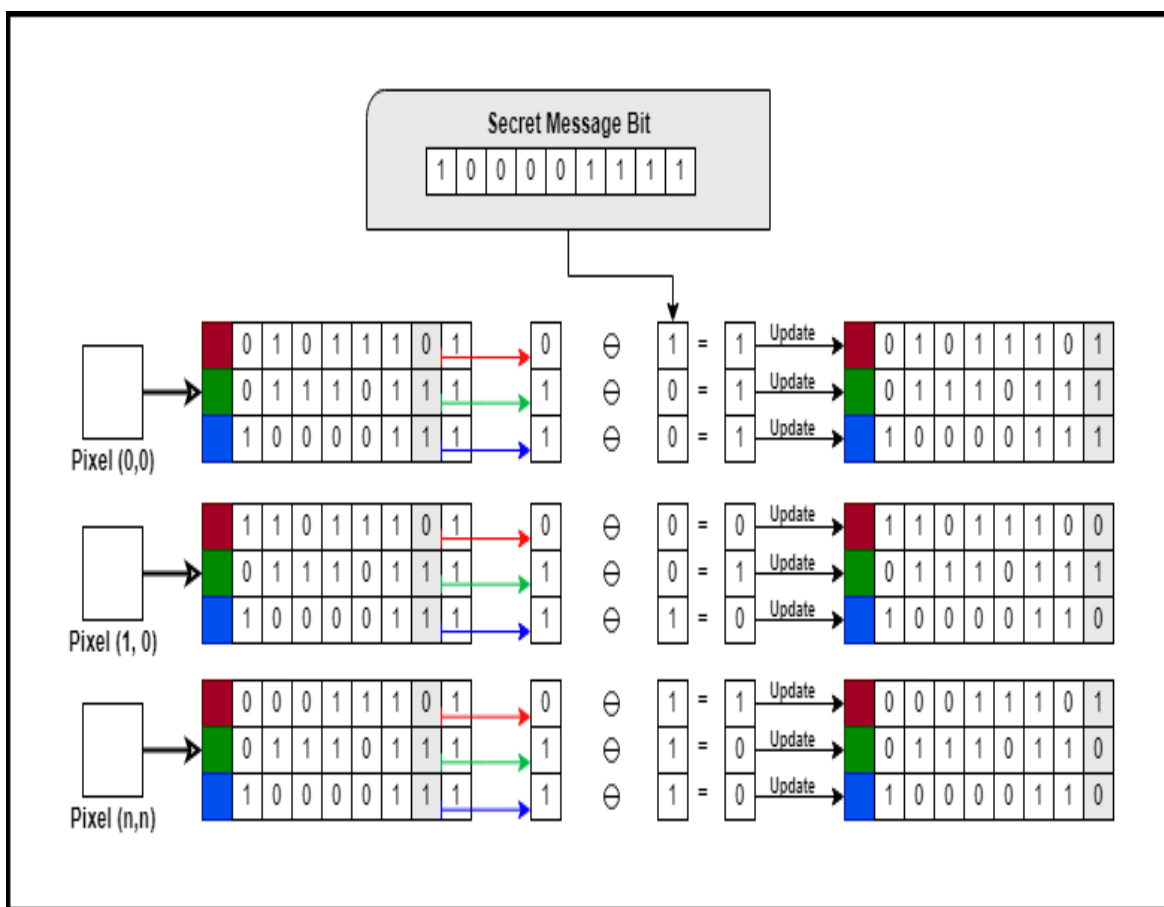


Figure 5: Embedding Process

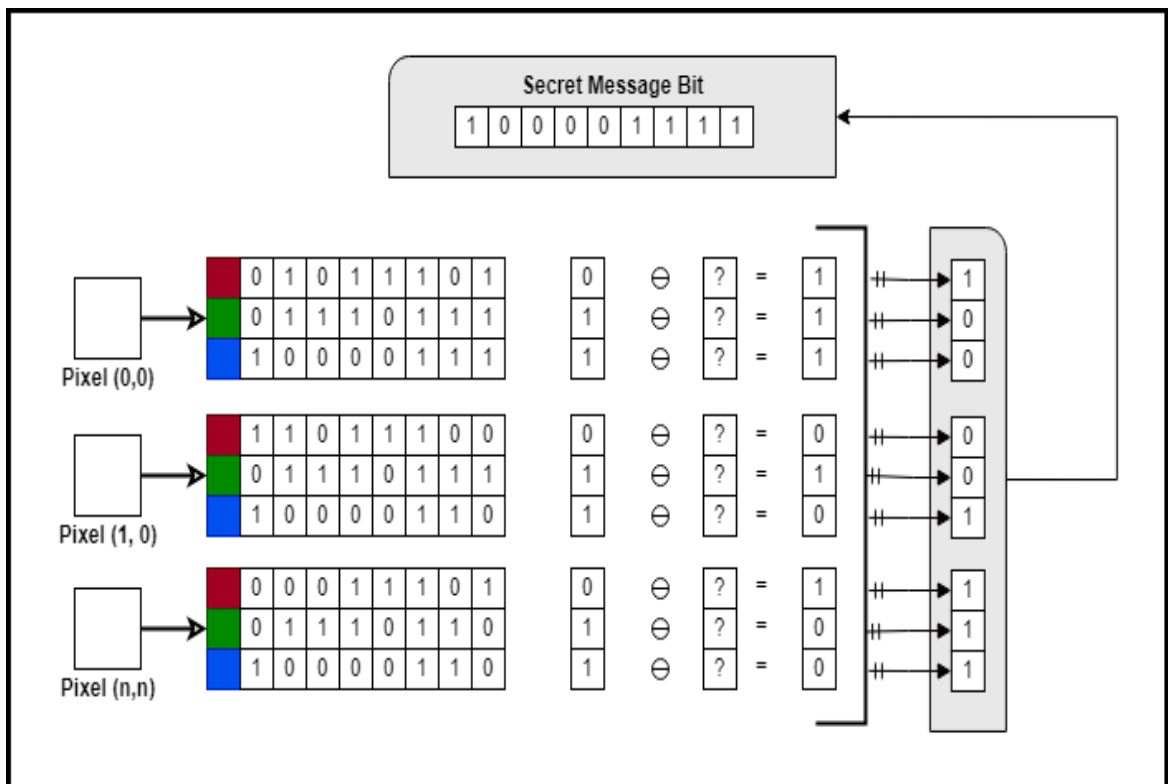


Figure 6: Retrieving Process

Figure 5 and 6 illustrate the subtraction-based LSB technique for embedding and retrieving technique.

### Embedding Algorithm:

**Result:** Stego Image

1.  $M \square input$
2.  $I \square input$
3.  $W = \text{Width of Image};$
4.  $H = \text{Height of Image};$
5.  $B_M \square \text{binaryAES}(M);$
6. **For**  $(0 \rightarrow W)\{$
7.     **For**  $(0 \rightarrow H)\{$
8.         **If**  $(M.length == 0)$

```

9.          break;
10.        embed ((X, Y), BM[n]);
11.        n++;
12.        updateRGB(X,Y);
13.    }
14.}
15.BL = Length of M;
16.BL □ reverse (binary (BL));
17.(x1, y1), (x2, y2), (x3, y3), (x4, y4) □ BL;

```

## Retrieving Algorithm

**Result:** Secret Message

```

1.SI □ input
2.W = Width of Image;
3.H = Height of Image;
4.BL □ (x1, y1), (x2, y2), (x3, y3), (x4, y4);
5.BL = Length of M;
6.SB = Secret Binary
7.For (0 → W){
8.    For(0 → H){
9.        If (BL.length == 0)
10.            break;
11.        SB[n] = extract ((X, Y));
12.        n++;
13.    }
14.}
15.secret_message ← ConvertByteFromBit(SB[n])

```

## CHAPTER 4

### RESULTS AND DISCUSSION

#### 4.1 Result Discussion

The effects are demonstrated in this part by visual explanation and assessment of the cover and stego picture. In addition, the proposed system's findings are linked to other well-known steganographic systems to demonstrate its efficacy. The statistical disquisition of the research is well-appointed with six quality dimension criteria as Root Mean Square Error (RMSE), Mean-Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR).

Figure 8 shows three photographs chosen for the experimental test (Baboon, Lena, Parrot, tiger, lili, and jackfruit). The six photos are in PNG format and have dimensions of (512 x 512). The suggested approach is implemented using the.NET Framework version 4.7.2, which is a C Sharp language framework.

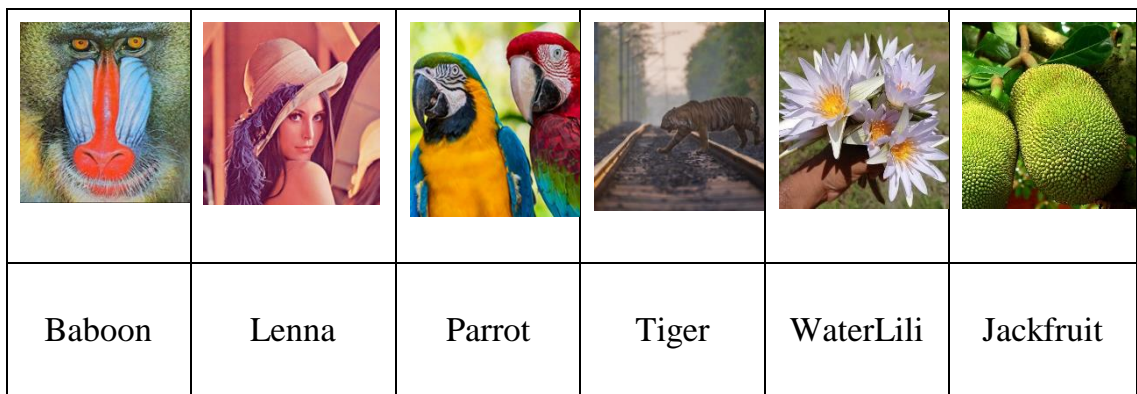


Figure 7: Cover Images

The PSNR, RMSE, and MSE quality measure matrices, which are often employed envoys to estimate the effectiveness and safety of the steganographic activity, are scientifically shown in Eqs. 7 to 9. [38] is a mathematical depiction of PSNR.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{ dB} \quad (7)$$

Previously, PSNR was measured in dB, which relies on MSE. Numerous forms of research demonstrate that it is also deemed acceptable if the PSNR between the cover and stego frame is more than 40 dB.

The MSE and RMSE definitions in mathematics [39, 40]

Take the observed value, subtract the prognosticated value, then use that difference to obtain the MSE. Say it again for each compliance. Additionally, add together all of those squared numbers and divide by the compliance rate..

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2 \quad (8)$$

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (\hat{y}_i - y_i)^2}{n}} \quad (9)$$

The suggested system's output is limited to a 15 Kilobyte payload on the specified four videotape frames. The findings of PSNR quality dimension matrices for specified frames are shown in Table I. Then, for Baboon, Lenna, and Parrot, 512 X 512 sized frames were used with a payload of 15 Kilobytes or 15000 bytes, and to bed all secret data, the proposed system was able to conceal 27000 bytes to 65000 bytes for various images gradationally, but it was observed that the frames of Parrot achieved slightly higher PSNR values than other named images.

TABLE I. Quality measurement metrics of the projected method

Image	Dimension	Payload	PSNR	MSE	RMSE
Lenna	512X512	512 Bytes	69.7456	0.0027	0.0519
	512X512	256 Bytes	72.9204	0.0013	0.0363
	512X512	128 Bytes	75.5643	0.0007	0.0260
Babbon	512X512	512 Bytes	69.7655	0.0026	0.0512
	512X512	256 Bytes	72.7456	0.0013	0.0356
	512X512	128 Bytes	76.5664	0.0006	0.0252
Parrot	512X512	512 Bytes	70.8645	0.0017	0.0417
	512X512	256 Bytes	73.5456	0.0010	0.0299
	512X512	128 Bytes	76.9695	0.0005	0.0223



Tiger	512X512	512 Bytes	69.1754	0.0017	0.0417
	512X512	256 Bytes	72.32321	0.0010	0.0299
	512X512	128 Bytes	75.93212	0.0005	0.0223
WaterLili	512X512	512 Bytes	69.3233	0.0017	0.0417
	512X512	256 Bytes	72.9562	0.0010	0.0299
	512X512	128 Bytes	75.32154	0.0005	0.0223
jackfruit	512X512	512 Bytes	73.5195	0.0017	0.0417
	512X512	256 Bytes	76.6545	0.0010	0.0299
	512X512	128 Bytes	80.6351	0.0005	0.0223

In this table, 512 X 512 sized images were utilized for Lena, Baboon, and Parrot, whereas payload sizes of 512 bytes, 256 bytes, and 128 bytes were progressively considered. The suggested technique yielded MSE values of 0.0027, 0.0013, and 0.0007 for Lena, 0.0026, 0.0013, and 0.0006 for Baboon, and 0.0017, 0.0010, and 0.0005 for Parrot. PSNR values for Lenna, Baboon, and Parrot were (69.7456, 72.9204, 75.5643), (69.7655, 72.7456, 76.5664), and (69.7655, 72.7456, 76.5664), respectively (70.5645, 73.5456, 76.9695). We saw that Parrot had a higher quality than others.

Table III compares the results of two steganographic algorithms with 512 Bytes payload and 512 X 512 sized frame [34, 32]. In this table, the XOR substitution [24] model represents Model1, the 8-directional-based model [32] denotes Model2, and our suggested model denotes the P-Model, where the performance of the P-model (Proposed Model) is better than the current models.

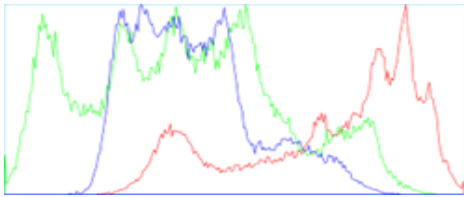
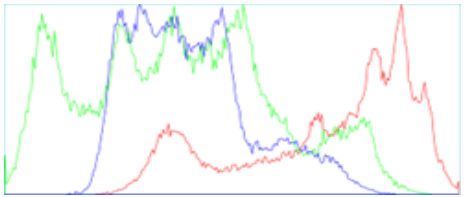
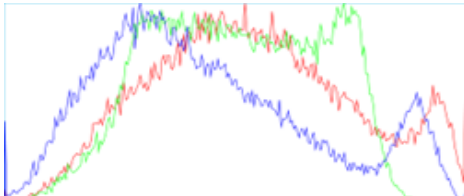
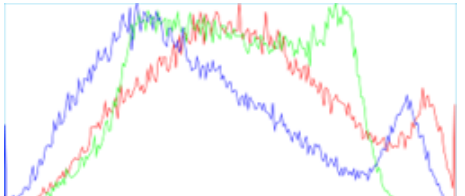
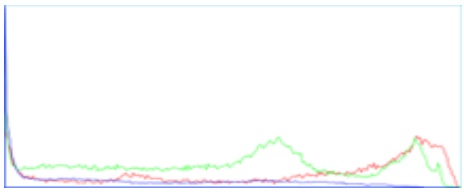
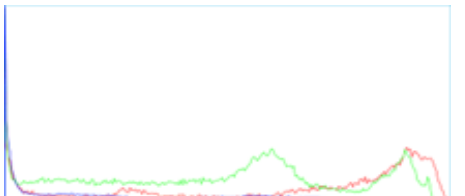
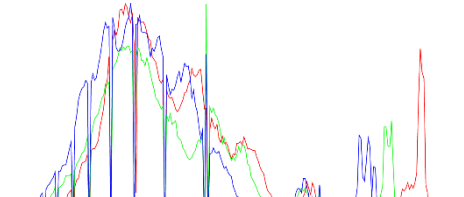
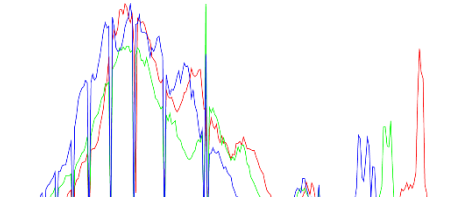
TABLE II. Comparison among recent steganographic techniques

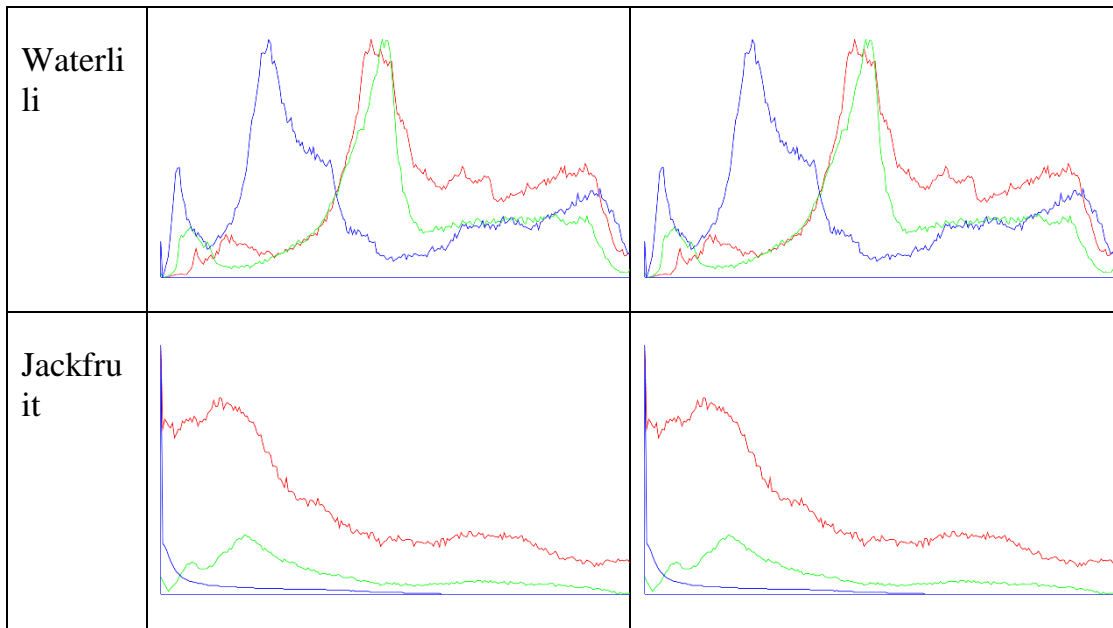
Image	Model	Dimension	Payload	PSNR	MSE	Time (MiliSec)
Lenna	Model 1	512X512	512 Bytes	66.5456	0.0029	181
	Model 2	512X512	512 Bytes	68.5615	0.0028	141
	P-Model	512X512	512 Bytes	69.7456	0.0027	115
	Model 1	512X512	512 Bytes	66.9655	0.0028	188

Babbon	Model 2	512X512	512 Bytes	68.5315	0.0027	157
	P-Model	512X512	512 Bytes	69.7655	0.0026	124
Parrot	Model 1	512X512	512 Bytes	65.5154	0.0029	205
	Model 2	512X512	512 Bytes	68.3265	0.0027	168
	P-Model	512X512	512 Bytes	70.8645	0.0026	144
Tiger	Model 1	512X512	512 Bytes	67.54541	0.0029	232
	Model 2	512X512	512 Bytes	68.9317	0.0027	159
	P-Model	512X512	512 Bytes	69.1754	0.0026	122
WaterL ili	Model 1	512X512	512 Bytes	68.8939	0.0029	209
	Model 2	512X512	512 Bytes	68.8254	0.0027	158
	P-Model	512X512	512 Bytes	69.3233	0.0026	128
	Model 1	512X512	512 Bytes	73.2356	0.0029	255
	Model 2	512X512	512 Bytes	96.74695	0.0027	174

Jackfruit	P-Model	512X512	512 Bytes	73.5195	0.0026	125
-----------	---------	---------	-----------	---------	--------	-----

The Table 3. shows the histogram for both 512 X 512 sized cover and stego images for the above three images.

Frame	Cover	Stego
Lenna		
Baboon		
Parrot		
Tiger		



Consistent with the histogram finding, the difference between the two frames is insignificant, indicating that these changes cannot be anticipated with the naked eye.

## **CHAPTER 5**

### **CONCLUSIONS AND RECOMMENDATIONS**

This study presents an automated two-layered safe data concealing technique for picture steganography that uses LSB and Subtractions with a user-selected dynamic zig-zag pixel selection strategy to hide the secret data with 128-bit AES encryption in the cover image. The overhead explanation and appropriate result analysis demonstrate that the suggested steganography data concealing methodology delivers redundant security and decreased imperceptibility as compared to other data hiding techniques currently in use.

## REFERENCES

- [1] Delenda, S., & Noui, L. (2018, May 4). A new steganography algorithm using polar decomposition. *Information Security Journal: A Global Perspective*, 27(3), 133–144.
- [2] Shehzad, D., & Dag, T. (4–5 August. 2017). A novel image steganography technique based on the similarity of bits pairs. 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia
- [3] Tiwari, R. K., & Sahoo, G. (2011, February 11). A novel methodology for data hiding in PDF files. *Information Security Journal: A Global Perspective*, 20(1), 45–57.
- [4] Shirafkan, M. H., Akhtarkavan, E., & Vahidi, J. (5–6 November. 2015). An image steganography scheme based on discrete wavelet transforms using lattice vector quantization and reed-Solomon encoding. 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran
- [5] Chandramouli, R., & Memon, N. (October 2001). Analysis of LSB-based image steganography techniques. In *Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205)*, 3, 1019–1022. IEEE
- [6] Islam, M. R., Siddiqa, A., Palash, U., Md., Mandal, A. K., & Hossain, M. D. (23–24 May 2014). An efficient filtering-based approach improving LSB image steganography using status bit along with AES cryptography. 2014 International Conference on Informatics, Electronics & Vision (ICIEV). Dhaka, Bangladesh.
- [7] Kaur, N., & Behal, S. (2014). A survey on various types of steganography and analysis of hiding techniques. *International Journal of Engineering Trends and Technology*, 11(8), 388–392.
- [8] Chen, P. Y., & Lin, H. J. (2006). A DWT-based approach for image steganography. *International Journal of Applied Science and Engineering*, 4(3), 275–290

- [9] Lai, C. C., & Tsai, C. C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, 59(11), 3060–3063
- [10] Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, 12(6), 441–444.
- [11] Sultana, S., Khanam, A., Islam, M. R., Nitu, A. M., Uddin, M. P., Afjal, M. I., & Rabbi, M. F. (2018). A modified filtering approach of LSB image steganography using stream builder. *INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE* 11 along with AES encryption. *HBRP Recent Trends in Information Technology and Its Applications*, 1(2), 1–10.
- [12] Begum, F., & Suthoju, G. R. (2021). Types of Steganography for Secure Data Maintenance. *Annals of the Romanian Society for Cell Biology*, 25(6), 2144-2159.
- [13] Mathur, N., & Bansode, R. (2016). AES-based text encryption using 12 rounds with dynamic key selection. *Procedia Computer Science*, 79, 1036-1043.
- [14] Islam, M. R., Siddiqa, A., Palash, U., Md., Mandal, A. K., & Hossain, M. D. (23–24 May 2014). An efficient filtering-based approach improving LSB image steganography using status bit along with AES cryptography. 2014 International Conference on Informatics, Electronics & Vision (ICIEV). Dhaka, Bangladesh.
- [15] Mukhedkar, M., Powar, P., & Gaikwad, P. (17–20 December. 2015). Secure non-real-time image encryption algorithm development using cryptography & steganography. 2015 Annual IEEE India Conference (INDICON), New Delhi, India.
- [16] Singh, K. M., Singh, L. S., Singh, A. B., & Devi, K. S. (7–9 March 2007). Hiding Secret Message in Edges of the Image. 2007 International Conference on Information and Communication Technology, Dhaka, Bangladesh.



- [17] Joshi, K., & Yadav, R. (21–24 December, 2015). A new LSB-S image steganography method blended with Cryptography for secret communication. 2015 Third International Conference on Image Information Processing (ICIIP). Wagnaghat, India.
- [18] Li, X., Zeng, T., & Yang, B. (2008). Detecting LSB matching by applying calibration technique for difference image. Proceedings of the 10th ACM workshop on Multimedia and security, Oxford, United Kingdom.
- [19] Loukhaoukha, K., Chouinard, J.-Y., & Berdai, A. (2012, March 7). A secure image encryption algorithm based on Rubik's cube principle. Journal of Electrical and Computer Engineering, 2012, 173931.
- [20] Majeed, A., Mat Kiah, M. L., Madhloom, H. T., Zaidan, B., & Zaidan, A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and Technology, 1(2), 63–69.
- [21] Ghosal, S. K. (2011). A new pair wise bit based data hiding approach on 24 bit color image using the steganographic technique. Greater Kolkata College of Engineering & bit-based management.
- [22] Kaur, D., Verma, H. K., & Singh, R. K. (2016). A hybrid approach of image steganography. 2016 International Conference on Computing, Communication, and Automation (ICCCA). Noida, India.
- [23] Ren-Er, Y., Zhiwei, Z., Shun, T., & Shilei, D. (2014). Image steganography combined with DES encryption pre-processing. 2014 Sixth International Conference on Measuring Technology
- [24] Raniprima, S., Hidayat, B., & Andini, N. (2016). Digital image steganography with encryption based on Rubik's cube principle. 2016 International Conference on Control,

Electronics, Renewable Energy and Communications (ICCEREC), Bandung, Indonesia.

[25] Phadte, R. S., & Dhanaraj, R. (2017). An enhanced blend of image steganography and cryptography. 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India.

[26] Broda, M., Hajduk, V., & Levický, D. (2015). Image steganography based on a combination of YCbCr color model and DWT. 2015 57th international symposium ELMAR (ELMAR). Zadar, Croatia.

[27] Charan, G. S., SSV, N. K., Karthikeyan, B., & Vaithiyanathan, V. (2015). A novel LSB-based image steganography with multi-level encryption. 2015 international conference on innovations in information, embedded and communication systems (ICIIECS). Coimbatore, India.

[28] Khalaf, E. T., & Sulaiman, N. (2011). Segmenting and hiding data randomly based on index channel. International Journal of Computer Science Issues (IJCSI), 8(3), 522.

[29] Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E., & Mohamed, E. (2018). A secure image steganography algorithm based on a least significant bit and integer wavelet transform. Journal of Systems Engineering and Electronics, 29(3), 639–649.

[30] Deeba, F., Kun, S., Dharejo, F. A., & Memon, H. (2020). Digital image watermarking based on ANN and least significant bit. Information Security Journal: A Global Perspective, 29(1), 30–39.

[31] Alam, S.T., Jahan, N. and Hassan, M., 2020, February. A New 8-Directional Pixel Selection Technique of LSB Based Image Steganography. In International Conference on Cyber Security and Computer Science (pp. 101-115). Springer, Cham.

- [32] Bhuiyan, T., Sarower, A.H., Karim, R. and Hassan, M., 2019, July. An image steganography algorithm using LSB replacement through XOR substitution. In 2019 International Conference on Information and Communications Technology (ICOIACT) (pp. 44-49). IEEE.
- [33] Ansari, A.S., Mohammadi, M.S. and Parvez, M.T., 2019. A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security*, 11(1), pp.11-25.
- [34] K. Patel, "Performance analysis of aes, des and blowfish cryptographic algorithms on small and large data files," *International Journal of Information Technology* 11(4), 813–819 (2019).
- [35] E. S. I. Harba, "Secure data encryption through a combination of aes, rsa and hmac," *Engineering, Technology Applied Science Research* 7, 1781–1785 (Aug 2017)
- [36] S. E. W. Ria Andriani and F. W. Wibowo, "Comparision of aes 128, 192 and 256 bit algorithm for encryption and description file," 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE) , 120–124 (Nov 2018).
- [37]. H. K. Hoomod and A. M. Radi, "New secure e-mail system based on bio-chaos key generation and modified aes algorithm," *Journal of Physics: Conference Series* 1003, 012025 (May 2018)
- [38] Singh, N. (2019). High PSNR based image steganography. *International Journal of Advanced Engineering Research and Science*, 6(1).
- [39] Farrag, S., & Alexan, W. (2019, April). Secure 2d image steganography using recamán's sequence. In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-6). IEEE.

- [40] Sabilla, I. A., Meirisdiana, M., Sunaryono, D., & Husni, M. (2021, September). Best Ratio Size of Image in Steganography using Portable Document Format with Evaluation RMSE, PSNR, and SSIM. In 2021 4th International Conference of Computer and Informatics Engineering (IC2IE) (pp. 289-294). IEEE.
- [41] Chaudhary, Paras. "A Novel Image Encryption Method Based on LSB Technique and AES Algorithm." *Computational Methods and Data Engineering*. Springer, Singapore, 2021. 539-546.
- [42] J M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in 2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017. IEEE, mar 2017, pp. 86–90.
- [43] J. Baek, C. Kim, P. S. Fisher, and H. Chao, "(N, 1) secret sharing approach based on steganography with gray digital images," in Proceedings - 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, WCNIS 2010. IEEE, Jun 2010, pp. 325–329
- [44] Mandal, J.K., Sengupta, M., (2011), "Steganographic Technique Based on Minimum Deviation of Fidelity (ST MDF).", Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 – 301.
- [45] Deepak kumar," Hiding Text In Color Image Using YCbCr Color Model: An Image Steganography approach," in 2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019.

- [46] Chikouche, S.L. and N. Chikouche. An improved approach for LSB-based image steganography using the AES algorithm. In 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B). 2017. IEEE.
- [47] Santoso, H.A., E.H. Rachmawanto, and C.A. Sari. An improved message capacity and security using divide and modulus function in spatial domain steganography. in the 2018 International Conference on Information and Communications Technology (ICOIACT). 2018. IEEE.
- [48] Roy, A., J. Bhattacharya, S. Kundu, S. Sahana and D. Singh. Block Steganography-Based Secure Key Encryption to Improve Data Security. in International Conference on Innovation in Modern Science and Technology. 2019. Springer.
- [49] Astuti, Y.P., E.H. Rachmawanto, and C.A. Sari. Simple and secure image steganography using LSB and triple XOR operation on MSB. in 2018 International Conference on Information and Communications Technology (ICOIACT). 2018. IEEE.
- [50] J M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in 2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017. IEEE, mar 2017, pp. 86–90.
- [51] J. Baek, C. Kim, P. S. Fisher, and H. Chao, "(N, 1) secret sharing approach based on steganography with gray digital images," in Proceedings - 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, WCNIS 2010. IEEE, Jun 2010, pp. 325–329
- [52] Mandal, J.K., Sengupta, M., (2011), "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).", Proceedings of Second International

Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 – 301.

[53] Deepak kumar,” Hiding Text In Color Image Using YCbCr Color Model: An Image Steganography approach,” in 2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019.

[54] Touhid Bhuiyan, Afjal H. Sarower, Md. Rashed Karim, Md. Maruf Hassan,” An Image Steganography Algorithm using LSB Replacement through XOR Substitution,” in International Conference on Information and Communications Technology (ICOIACT),2019.

[55] Wu, Fangsheng, et al. "Research on image text recognition based on canny edge detection algorithm and k-means algorithm." International Journal of System Assurance Engineering and Management 13.1 (2022): 72-80.

