An Efficient Model for a Secured LSB based Image Steganography in YCbCr Color Space

By

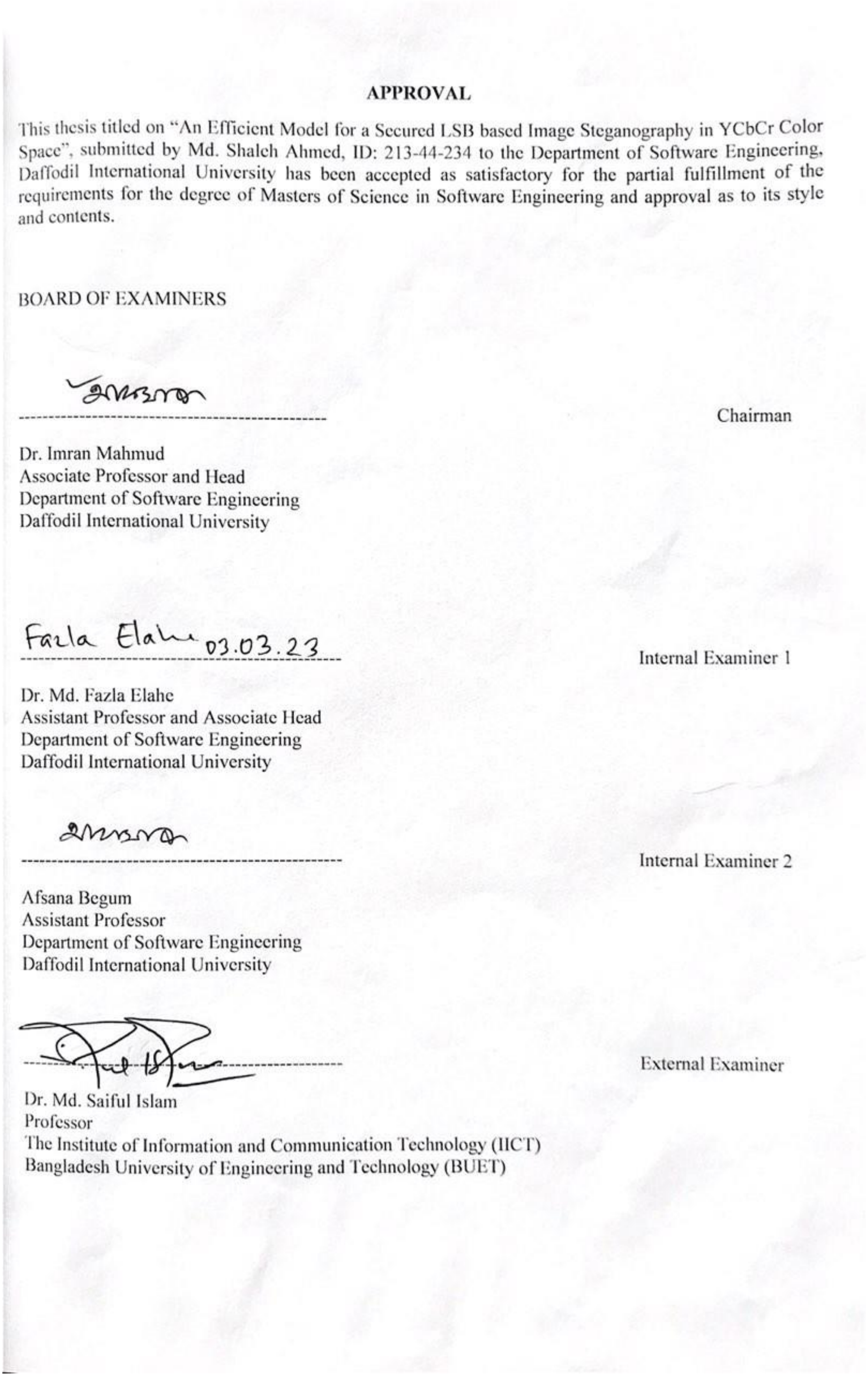
Name-Md. Shaleh Ahmed

(213-44-234)

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 titled on "An Efficient Model for a Secured LSB based Image Steganography in YCbCr Color Space", submitted by Md. Shaleh Ahmed, ID: 213-44-234 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

Fazla Elahe 03.03.23
-- Internal Examiner 1

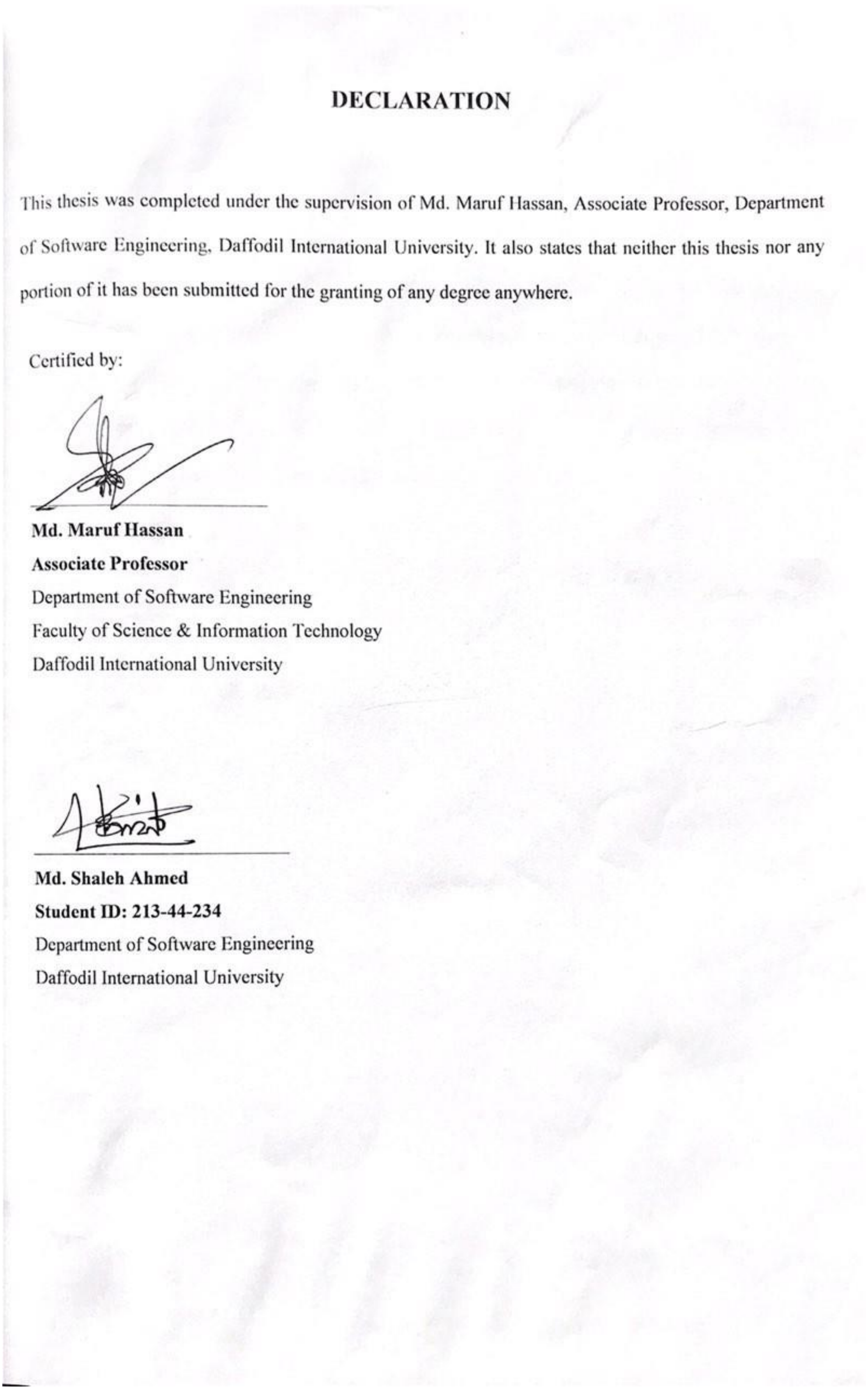
Dr. Md. Fazla Elahe
Assistant Professor and Associate Head
Department of Software Engineering
Daffodil International University

-- 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 (IICT)
Bangladesh University of Engineering and Technology (BUET)



DECLARATION

This thesis was completed under the supervision of Md. Maruf Hassan, Associate Professor, Department of Software Engineering, Daffodil International University. It also states that neither this thesis nor any portion of it has been submitted for the granting of any degree anywhere.

Certified by:

Md. Maruf Hassan
Associate Professor
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Md. Shaleh Ahmed
Student ID: 213-44-234
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

In this thesis, I've gone through certain hardships. Regardless, it would not have been possible without the generous assistance and assistance of several individuals. Because of each of them, I may desire to extend my focus. I'm exceedingly appreciative of Daffodil International University's direction and Md. Maruf Hassan's constant monitoring, as well as aimed at providing vital evidence about the journey and assistance in completing the assignment. I'd want to thank our parents, class mates, and DIU members for their kind cooperation and consolation in assisting us in completing this assignment. I would want to sincerely thank everyone for their contributions and acknowledge their efforts. My gratitude and appreciation also go to my partner in setting up the adventure and those who have steadfastly aided us with their abilities.

TABLE OF CONTENT

APPROVAL ii

DECLARATION iii

ACKNOWLEDGEMENT iv

TABLE OF CONTENT v

LIST OF TABLE vi

LIST OF FIGURE vi

ABSTRACT vii

CHAPTER 1: INTRODUCTION 1

1.1 Background 1

1.2 Motivation of the Research 6

1.3 Problem Statement 6

1.4 Research Questions 7

1.5 Research Objectives 6

1.6 Research Scope 8

1.7 Thesis Organization 8

CHAPTER 2: LITERATURE REVIEW 9

CHAPTER 3: RESEARCH METHODOLOGY 13

3.1 Encrypting the Secret Message 13

3.2 Pixel Filtering Algorithm 14

3.3 Steganographic Process 15

3.4 Algorithm for embedding and retrieving. 18

CHAPTER 4: RESULTS AND DISCUSSION 21

4.1 Result Discussion 21

4.2 Implementation on Desktop App 27

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS 28

REFERENCES 29

LIST OF TABLES

Table 1: Quality measurement metrics of the projected method 23
Table 2: Comparison among recent steganographic techniques 25
Table 3: Comparison among recent steganographic techniques 26

LIST OF FIGURES

Figure 1: General Block Diagram of Steganography 2
Figure 2: Types of Steganography 2
Figure 3: RSA encryption 4
Figure 4: Approach of Canny Edge Detection 14
Figure 5: Sampling of Cunny edge detection 15
Figure 6: Embedding Process 17
Figure 7: Retrieving Process 18
Figure 8: Cover Images 21
Figure 9: Desktop Application 27

ABSTRACT

Data is currently one of the most important means, and it must deal appropriately with the looming threat of cybersecurity. Furthermore, when data is transmitted from one place to another by the internet, there is a possibility that hackers may hack the data and modify it. That's why we need to increase our security during data transmission. As a result, Steganography with cryptography terms came. Regardless matter how secures the crypto is, information is converted to encrypted message using a case of private key in cryptography. in cryptography, information is converted to an encrypted message using private key cryptography. However, the actual message is still accessible to others. And hackers know a secret communication is running. Contrarily, steganography is the use of various methods to hide information from unwanted eyes. Steganography by definition is the hiding of one file within another. This study offered a brand-new data-hiding technique based on LSB steganographic techniques, whereby only the user-selected picture pixels are used to conceal sensitive information. In order to do this, in LSB steganography-secured word and pixel intensity metadata are utilized so that the user needs to filter the whole picture in order to find the seeker pixel. The suggested approach improves security by converting each RGB pixel to YCbCr during embedding, using the XOR method to incorporate secret information, and encrypting the secret message using the RSA system before performing obfuscation techniques. In the experiment, MSE and PSNR values are scaled to control the stego picture's attractiveness. The stego picture has a greater PSNR but a lower MSE value when related to other analyzed styles, highlighting the rigidity of the suggested method.

Keywords: RSA, Image Steganography, YCbCr, PST, LSB, Canny Edge detection

CHAPTER 1

INTRODUCTION

1.1 Background

The internet's applicability is rapidly developing in current times. One of the most important topics that people are interested in is safety in cutting-edge the sphere of online. Humans, being communal organisms, interact with one another under all circumstances. Every human being has their own communication style, and they sometimes desire to share nonpublic information with the expected individual [1]. But it couldn't be sending documents or material to the designated individual altogether the period while being safe plus secure. As a result, data must be sent invisibly in order to preserve legitimate conversation. As a result, documents encryption is required aimed at safe data transmission amongst double or several entities. Cryptography is the furthermost widely used method of information encryption. However, by way of we all distinguish, relying exclusively on encryption is not safe since the existence of nonpublic information might be connected [2]. Steganography, which comes after the next pointer, uses the covert communication channel to obfuscate it so that no one can accurately identify it. The main advantage of steganography rendering is that it hides the data behind a cover medium, keeping it secret from everyone save the beneficiary. Steganography is an important and effective technique that furthers strong protection, particularly by defeating encryption [3]. Steganography hides the text's true nature so that unauthorized individuals cannot assume that communication is happening. In this approach, information data must be protected is transferred into an unanticipated network [4].

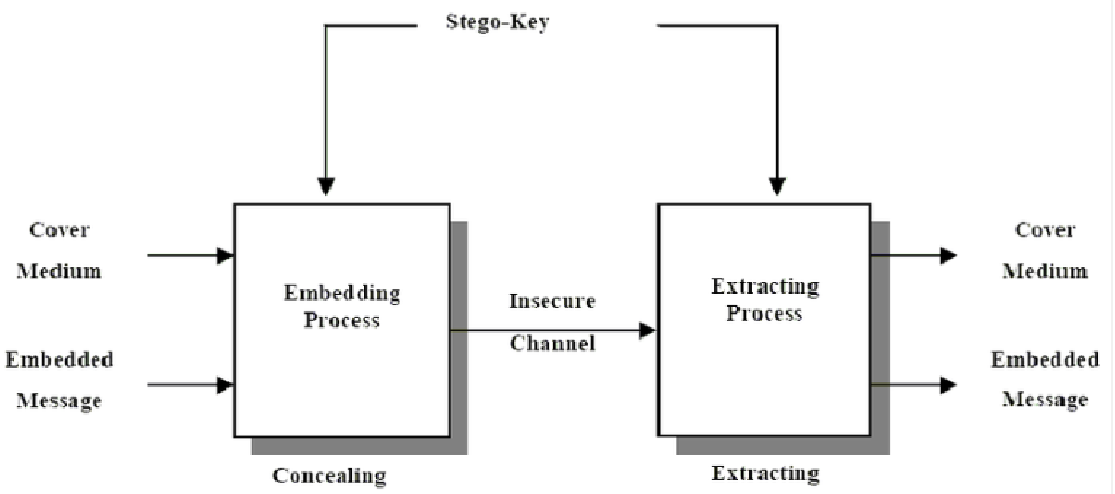


Figure 1: General Block Diagram of Steganography [5]

The outlines of the steganography method are seen in Figure 1. There are numerous sorts of cover media on which we may use steganography. Steganography techniques conceal sensitive information in carrier media such as pictures, sound, data, and film lines [6].

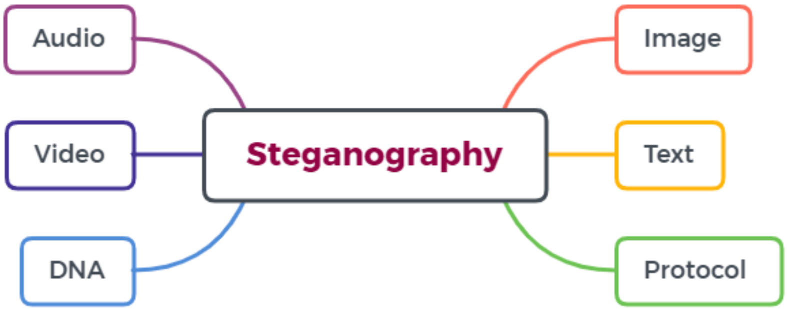


Figure 2: Types of Steganography

Figure 2 depicts various possible cover medium where we might use steganography effectively. However, the picture is the supreme extensive besides diverse standard for safeguarding instructional material. By way of we age, the mortal appreciation is more sensitive to brightness than chrominance. Thus, Steganography trades data by exploiting the human eye's weakness in perceiving picture lines. As cover material for this publication, we utilized a 24-bit color picture. The image The frequency sphere and the spatial sphere are the two components of the obfuscation techniques system [7]. The image data 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 spatially globe steganography is the least significant bit (LSB) approach, with which the secret transmission bits are used in lieu of the picture's LSB bit [10]. There are two categories of LSB photo steganography: non-filtering and processing. In the non-filtering method, every pixel in the image is used to steganographically conceal information, 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 classified info can only be secured using obfuscation techniques. As a consequence, we combined the recommended steganography with the most sophisticated RSA encryption technique. The core principles of RSA encryption are shown in Figure 3.

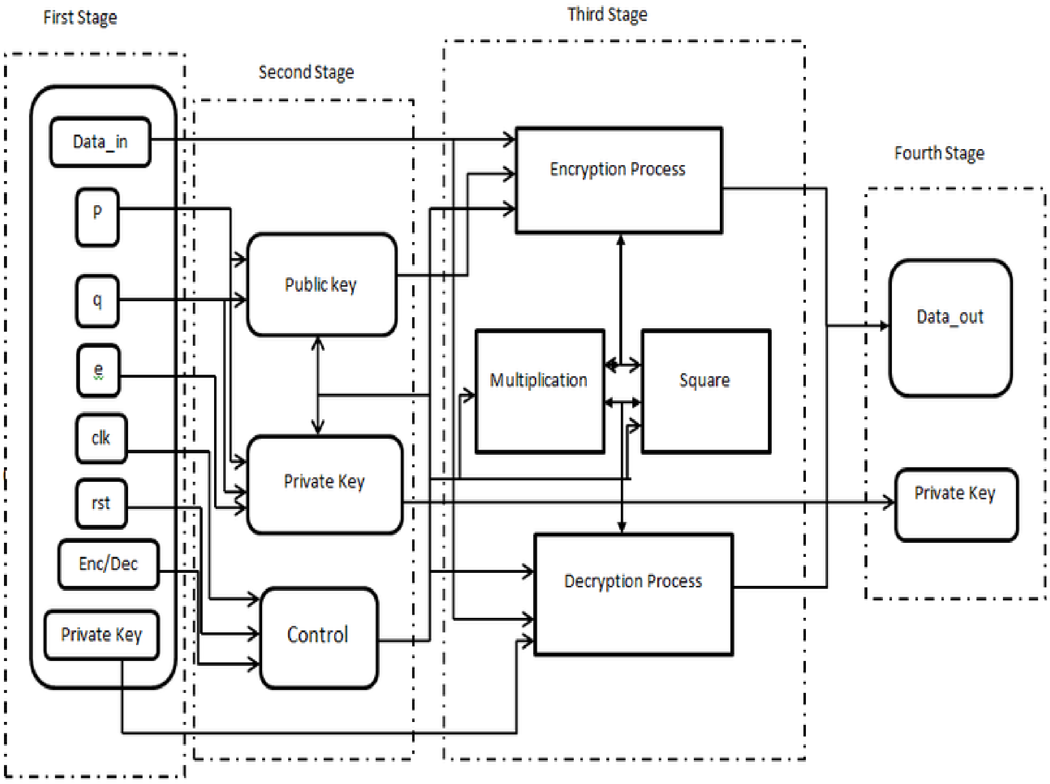


Figure 3: RSA encryption [13]

In this study, we employ a user-defined word to qualify the traditional LSB technique. Our suggested solution employed a reasonable process involving a communication bit then a word morsel, rather than just changing the Least Significate Bit bit of an image cell. First, we strainer the entire picture toward choose the expected pixels aimed at use with the steganography machinery. This paper's key contribution is as follows.

(1) The system employs a novel user-defined dynamic method of pixel filtering that differs from picture to image. As a result, nothing can tell which pixels are employed to conceal surreptitious info.

(2) We use YCbCr Color space that is converted from RGB. YCbCr can work with 7 bits. We may use our proposed method in low storage device where use of YCbCr color space will work fine.

(3) we use a pixel selection algorithm like canny edge which considered good so far due to non-maximal suppression and use of thresholding which extracts most of the edges. However Canny edge detection smooth the image with removing the noise.

(4) The recommended fix uses the XOR procedure to introduce the supplementary bit rather than replacing the LSB bits entirely.

(5) Before embedding secret message in picture, the system applied the RSA cryptography technique.

The leftovers of the document is arranged as tracks. The second section discusses a topical related composition continuously steganography. Suggested algorithm is shown briefly in the next section. The flowchart and exemplification table are then used to demonstrate three separate methods for how we implemented the filtering, embedding, and rooting approaches. The fourth portion of the paper presents various experimental data as well as performance assessment matrices utilized in the steganography technique. We also compared it to various other ways. The conclusion is shown at the end of the article.

1.2 Motivation of the Research

The online world has evolved in recent years into a vast technological infrastructure for cutting-edge manufacturing applications. Internet hosting has lately replaced organizing programs in colorful organizations. They have offered their services to users of the internet and drug users who get data via those online operations. To recognize 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 gaps in pixel selecting manner, is the main driving force behind the development of a security policy which would give multiple sub caste in verification system.

1.3 Problem Statement

- we know that steganography is a message hiding technique so that a user can send or communicate to the other user about their secret message securely.
- In the modern cloud storage era storage is bigger issue.
- We use YCbCr Color space that is converted from RGB. YCbCr can work with 7 bits. We may use our proposed method in low storage device where use of YCbCr color space will work fine.
- Some Established method works with YCbCr, but they didn’t use any encryption technique. If Secret message is not encrypted hacker can easily get the secret data.

- We use RSA algorithm for more securing the data.

- Several experiments use random pixels from cover image and convert them into binary and use LSB, XOR to embed the secret message. But use of random pixel is a threat.

- we use a pixel selection algorithm like canny edge which considered good so far due to non-maximal suppression and use of thresholding which extracts most of the edges. However Canny edge detection smooth the image with removing the noise.

1.4 Research Questions

1. Question 1: How will our proposed method hide data according to the rules of steganography?
2. Question 2: How does the proposed validation method produce better results than other established methods?

1.5 Research Objectives

- A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. Our proposed method works according to the rules of steganography.
- The aim of the new research is to overcome the limitations of currently established methods and provide better results. Our proposed method has provided a better result compared to the limitations of currently established methods

1.6 Research Scope

Many organizations provided their services to their drug addicts via the internet. Thus, authentication is critical in identifying their stoner. Interferers have developed a variety of methods for breaking down authentication systems in recent years. We must continue to improve our security in this sector. As a result, there are several exploratory compasses vogueish this region.

1.7 Thesis Organization

This paper uses IEEE representing organism in this investigation. This article is divided into five chapters, which are discussed below.

1st Chapter provides a summary of the exploration context, provocation, problematic statement, as well as objects.

Chapter 2 This chapter discusses being affiliated work and determining the exploration gap.

Chapter 3 provides the exploration technique and methods that will be used throughout the expedition.

Chapter 4 contrasts the experimental outcomes to being methods.

Chapter 5 presents the exploration expansion and limitations of this research, as well as the direction of the upcoming effort of exploration.

CHAPTER 2

LITERATURE REVIEW

While doing the research, numbers on image steganography and mathematical hash for verification were discovered. The following is an examination of those similar works.

The application of steganography concepts to encompass different media has been shown in a number of ways. A technique that combines image obfuscation techniques and encryption was presented by Islam et al. [14]. Before overlaying the image, the secret message is first encrypted using the Cryptography procedure. Additionally, they have employed the idea of filtering, in which not all of the pixels in the image are used to conceal data. A technique for hiding private information while interaction that combines encryption technology and perceptual obfuscation was put out by Mukhedkar et al. [15]. Data bits were concealed in the LSB position and the Blowfish Process was used to encrypt the picture. An LSB approach that Singh et al. [16] presented involves hiding peek data in non-adjacent pixel locations of the selected image. The adversary is not able to identify the corporality of private data bits on the margins because the pixels on the edges are brighter and more dark than their neighbours. A unique technique for fusing grayscale obfuscation techniques in the geographical realm with encryption was put out by Joshi and Yadav [17]. This method encrypts the secret message using the Vernam encryption technique. Additionally, the LSB bit positions of the pixels include the ciphered data. The left shifting 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 encoding 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 image and an RGB image that serves as the concealed image in a steganography approach developed by Raniprima et al. [24]. A hidden message is substitution cipher using the Rubik's cube method, which modifies the positions of pixels in a captured file, for even more genuine encryption. The method Phadte and Dhanaraj [25] developed combines Steganography and Cryptography. To hide critical information, this system uses the unstable approach to encrypt this producing 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 concealing secret information in a color image using the LSB replacement technique. The confidential data is first encrypted using the Caesar cipher method, and then the encrypted data is embedded into the image. A hybrid approach that integrates recognition and material hiding was described by Khalaf and Sulaiman [28]. Two RGB streams are used to mask the third channel's private information. The other channels determine the number of ones within the selected index path by using one channel as an indication route. A steganography method was developed by Emad et al. [29] to conceal a data machine code in the LSB bits. The system approximates grayscale images using the integer wavelet decomposition (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 method for identifying pixels 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 constant, which might be a weakness there in 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 methodology, which is very well-liked by invaders but results in greater PSNR and reduced MSE values. Information disguising 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 encrypt the embedded image and the LSB technology to hide data in pictures. The spatial domain method includes a number of data hiding techniques in an image. The LSB substitution method is the simplest and most popular of the other methods. 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 inclusion 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. XOR was used to display a bit on a specific pixel bit. M. Sengupta, J.K. Mandal, and [44] The smallest variance of the data integration technique is suggested based on fidelity. In this case, two bits by the sequence here between LSB and the sixth bit toward MSB are changed by the use of random replacement sites. In order to conceal text in color images with greater PSNR and smaller MSE scores for a variety of images, Deepak Kumar [45] adopted the YCbCr color scheme.

To work out the above disadvantages and faults, we used the 1-Bit LSB approach, which is a spatial domain methodology to entrench secret data. Before encoding it into cover dispatch, we used a data encryption named Rivest, Shamir, Adleman (RSA), where a 1024-bit secret key (randomly generated by automating using c# language) was used so that time could be consumed. Thus, a user-selected pixel detecting technique is employed with LSB during embedding, which delivers improved performance in arbitrary permutations. As a result, we chose PNG graphics with a fashionable perceptibility quality as cover images [33]. We also employed the quality dimension criterion Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE).

CHAPTER 3

RESEARCH METHODOLOGY

An experimental design technique was used to demonstrate the suggested paradigm. The experimental terrain has been separated into two pieces in this methodology: the suggested steganography exemplary in addition to the perpetration of the entire projected model aimed at the donation of its efficacy. An automated two-layered safe data hiding technique for picture steganography employing 1-bit LSB and a user-selected dynamic pixel selection approach has been shown in this research, with the encryption system and steganography perpetration discussed in depth in the following subsections.

3.1 Encrypting the Secret Message

This is one of the basic issues in cryptography, and RSA and other public-key encryption technologies have found solutions to it [34, 35].

Utilizing RSA encryption and a secret key, which is a freely sharable code, messages are secured. A message can only be decoded using a separate key, called the private key, when it is encrypted with the cryptographic key that use the RSA technique. Each RSA user has a key pair made up of both public and private keys. As when the name implies, the private key must remain a hidden.

As opposed to encrypted with public keys methods, encryption algorithm employs the same confidential key for encryption and decryption. Due to these distinctions, public key encryption systems like RSA are beneficial for communication in circumstances when it is impossible to reliably disseminate keys in advance [36].

Symmetric-key algorithms have their own uses, such as securing information for private use or for situations where secret keys may be exchanged across secure channels

[37]. The whole RSA 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.

3.2 Pixel Filtering Algorithm

This pixel filtering is a dynamic user-selected approach. Here we used Canny edge detection formula to detect edge from image [46]. Figure 5 depicts this technique. Here, we utilize equation 1 to examine all pixels. The operation is applied by these formulas such as gradient magnitude and gradient direction.

$$||\nabla f|| = \sqrt{\left(\frac{\partial f}{\partial x}\right)^2 + \left(\frac{\partial f}{\partial y}\right)^2} \qquad (1)$$

$$\theta = \tan^{-1}\left(\frac{\partial f}{\partial y} / \frac{\partial f}{\partial x}\right) \qquad (2)$$

Equation 2 is used to determine an even or odd pair from the first and second MSB positions using a user-specified method. Where FXB indicates the binary conversion function and FXr signifies the red value retrieval function.

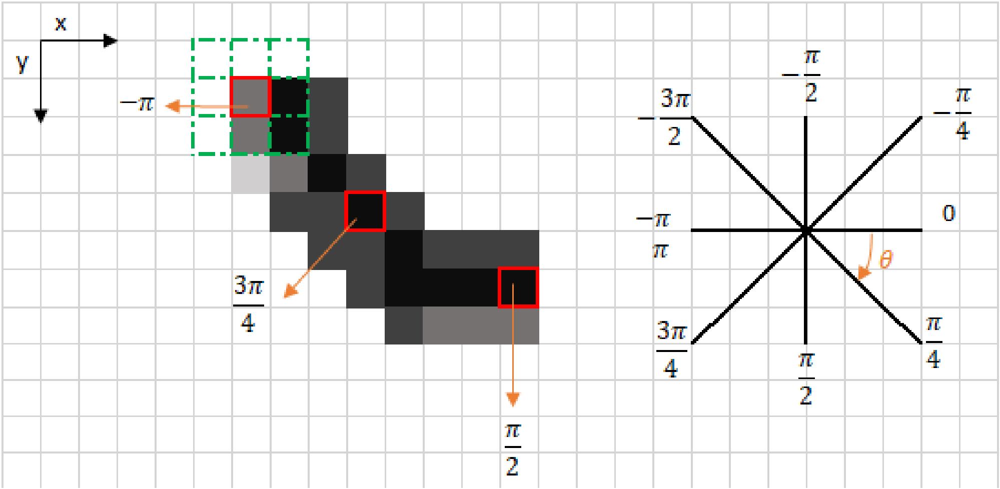


Figure 4: Approach of Canny Edge Detection

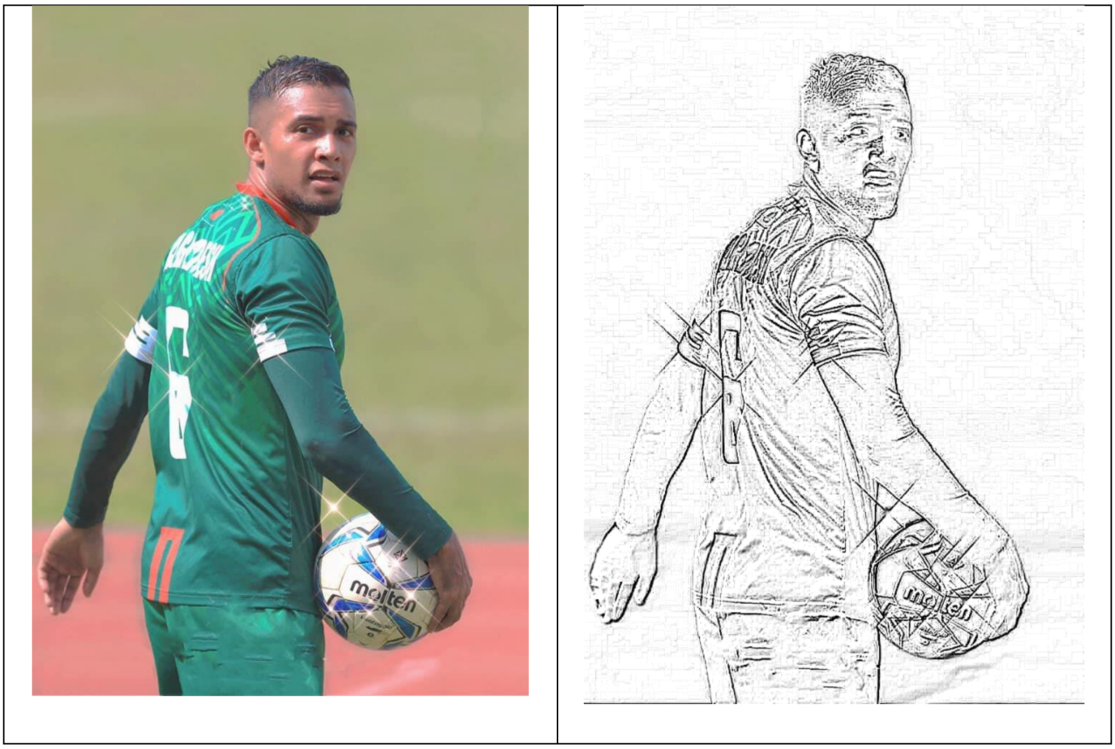


Figure 5: Sampling of Cunny edge detection.

3.3 Steganographic Process

The steganographic process is divided into two corridors: the Embedding approach and another called the Retrieve approach. Figure 6 depicts the proposed system's embedding process, which takes secret plain text from the stoner and encrypts the communication with a 1028-bit RSA algorithm. The images are uprooted from the cover carrier in the second phase, and the pixel selection system then interacts with the aforementioned systems. The encoded secret message will be converted into 8-bit binary data and embedded with 1 bit LSB position of filtered pixels via XOR operation in the third phase. In this case, XOR determination used with the secret communication bit also the sixth indexed bit, and the last indexed to RGB blocks will be replaced. Figure 7 depicts the retrieval procedure. To retrieve secret data, you must first understand the metadata, which includes the secret message embedding key, message size, and pixel filtering algorithm, which will store the fixed four pixels using Equation.

1st-pixel position (X1, Y1) = $(H/2 - 3,1)$ (3)

2nd-pixel position (X2, Y2) = $(H, W/2 - 3)$ (4)

3rd-pixel position (X3, Y3) = $(H/2 + 3, W)$ (5)

4th-pixel position (X4, Y4) = $(1, H/2 + 3)$ (6)

Those pixels are used to record information that is utilized to extract the RSA key and message size, as well as the filtering pixels' method. Knowing the filtering method will allow our system to get filtering pixels where the secret message bit is stored in the embedding approach. Then, to get the secret message bit, we will do an XOR operation with the 6th and 7th indexed bit for RGB blocks. After obtaining the bits depending on message size, we may crack the clandestine data using the RSA vital and get the required plain text that was hidden.

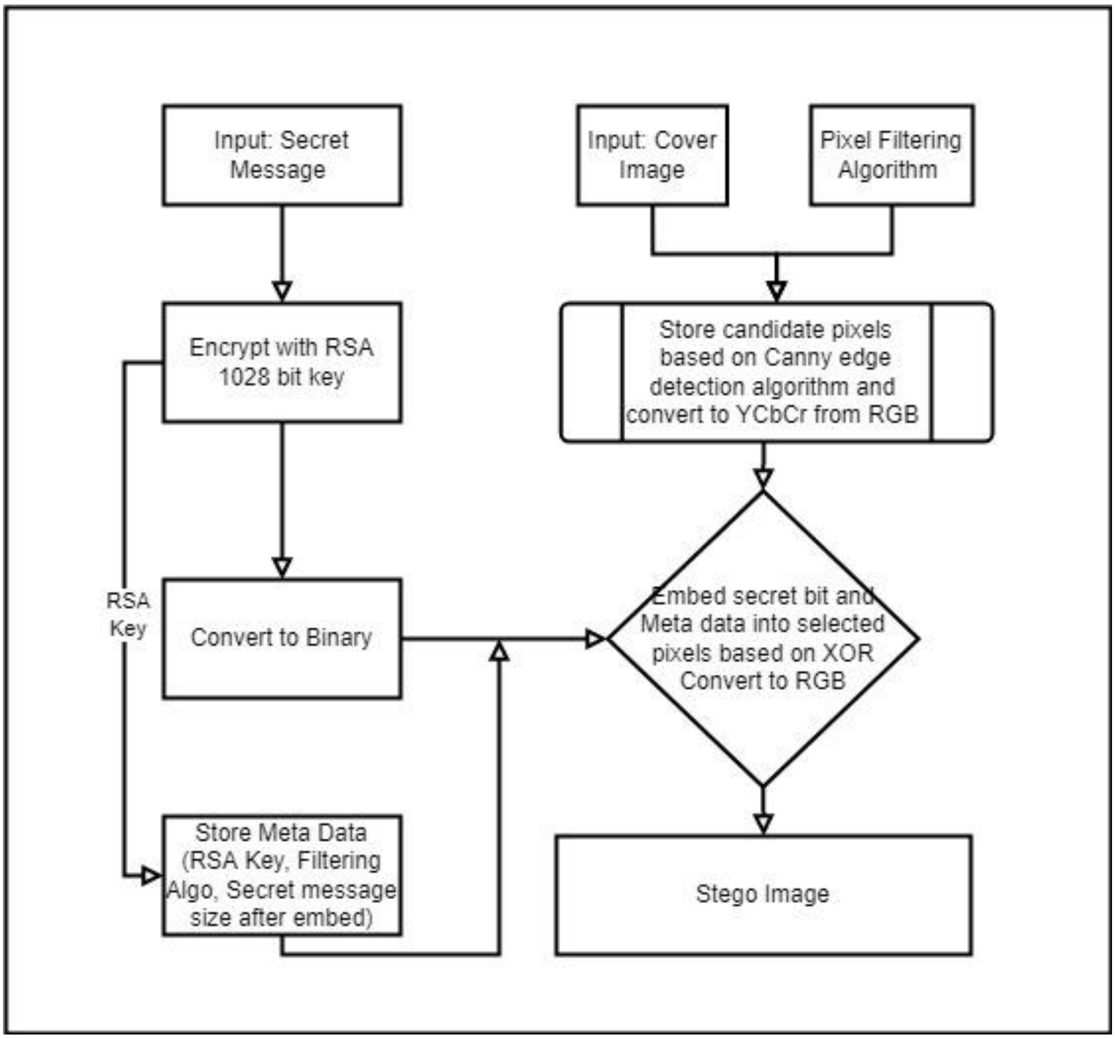

Input: Secret Message
Input: Cover Image
Pixel Filtering Algorithm
Encrypt with RSA 1028 bit key
Store candidate pixels based on Canny edge detection algorithm and convert to YCbCr from RGB
RSA Key
Convert to Binary
Embed secret bit and Meta data into selected pixels based on XOR Convert to RGB
Store Meta Data (RSA Key, Filtering Algo, Secret message size after embed)
Stego Image

Figure 6: Embedding Process

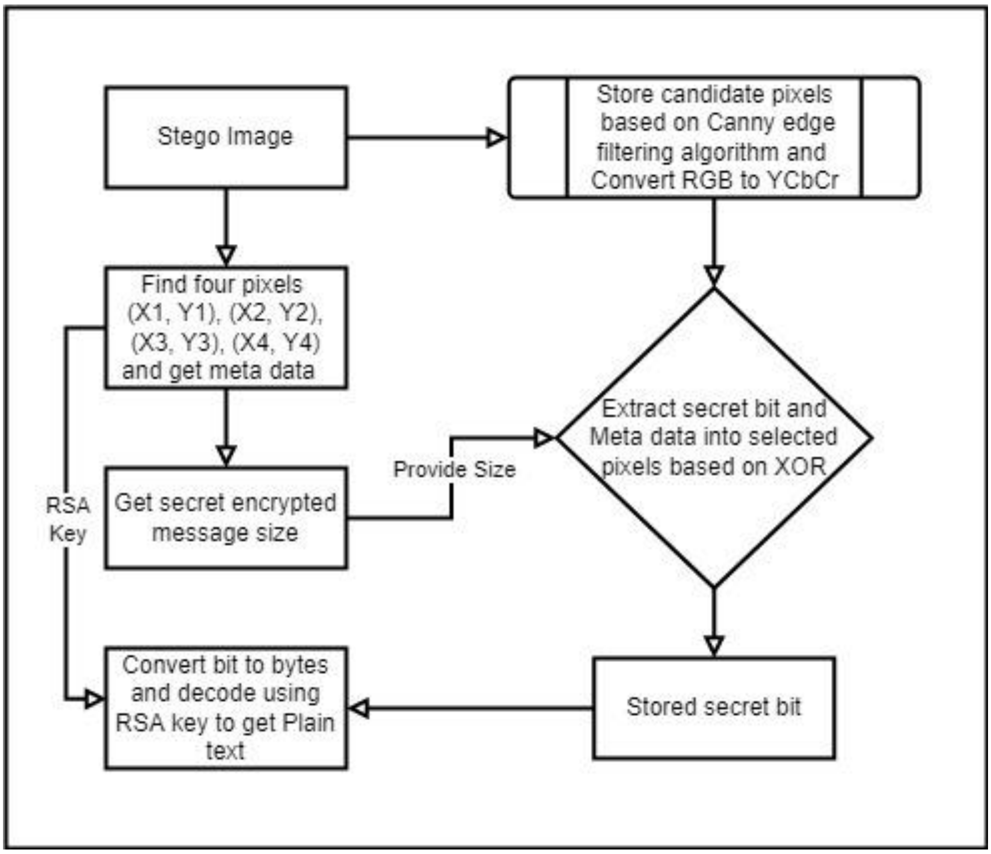

Stego Image
Store candidate pixels based on Canny edge filtering algorithm and Convert RGB to YCbCr
Find four pixels (X1, Y1), (X2, Y2), (X3, Y3), (X4, Y4) and get meta data
Extract secret bit and Meta data into selected pixels based on XOR
Provide Size
RSA Key
Get secret encrypted message size
Convert bit to bytes and decode using RSA key to get Plain text
Stored secret bit

Figure 7: Retrieving Process

3.4 Algorithm for embedding and retrieving

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 RSA 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 saving them in a pixel list for use in the embedding process. These pixels are used to hide secret bits from the encoded message that was transformed by the RSA key. The retrieving procedure, on the other hand, is the inverse of the embedding process.

Embedding Algorithm:

```
Result: Stego Image
$S_m$ ← input
$C_I$ ← input
$F_A$ ← input
$E_K$ = RSAKey();
$ES_m$ = RSAEncryption($S_m$, $E_K$);
FilteredPixels[] = $F_{XB}$(Fxr(X, Y))[0][1]($C_I$);
$M_D$ = $F_{XB}$($E_K$+$F_A$+Size($ES_m$));
4(xn, yn) ← $M_D$
$S_{MB}$ = $F_{XB}$($ES_m$);
For a ≤ FilteredPixels[]
    RGB = Read(FilteredPixel[n]);
    embedLSBXOR(RGB, $S_{MB}$)
    UpdatedRGB();
End For
```

Retrieving Algorithm

```
Result: Clandestine Message
$S_I$ ← input
$M_D$ ← 4(xn, yn)
FilteredPixels[] = Fx($M_D$,$S_I$);
$M_S$ = $M_D$[Size($ES_m$)]
For a ≤ FilteredPixels[]
    SecretBit[] = retrieveLSBXOR(RGB, $S_{MB}$)
    if(SecretBit[] >= $M_S$)
        Break;
End For
encryptedMessage = BitToBytes(SecretBit[])
Plaintext = Decode (encryptedMessage, Key)
```

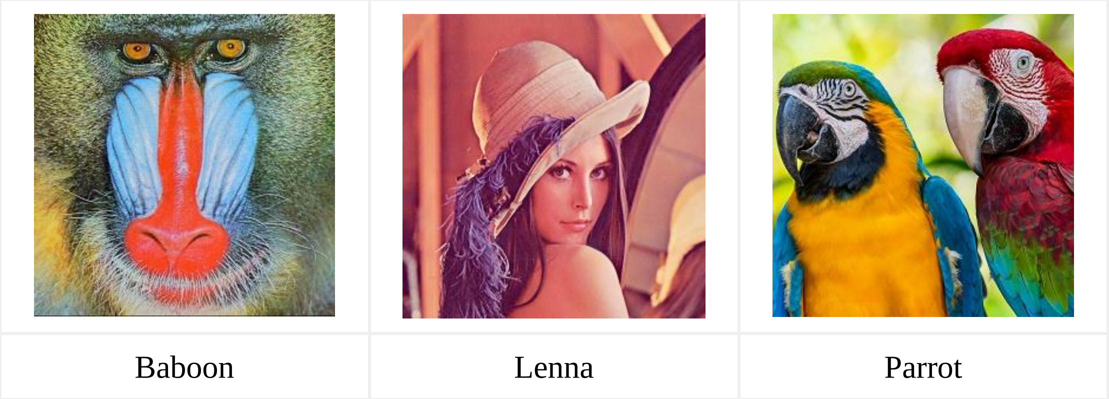
CHAPTER 4

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 such as Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), and Mean-Square Error (MSE).

Figure 8 shows three photographs chosen for the experimental test (Baboon, Lena, and Parrot). The three photos are in PNG format and have dimensions of (512 x 512). The suggested approach is implemented using the.NET Framework version 4.8, which is a C Sharp language framework.



Baboon Lenna Parrot

Figure 8: Cover Images

The scientific illustrations for the stated three quality measure matrices (i.e., PSNR, RMSE, and MSE) are shown in Eqs. 7 to 9, which are often used envoys to quantify the efficacy and safety of the steganographic activity.

The Mathematical illustration for PSNR is [38]

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\,\mathrm{dB} \tag{7}$$

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 both the cover with stego frame is more around 40 dB.

The MSE and RMSE scientific expression [39, 40]

To find the MSE, take the observed value, abate the prognosticated value, and forecourt that difference. Reprise that for all compliances. Also, sum all of those squared values and peak by the number of compliances.

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

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

The suggested system's output is limited to a 15 Kilobyte payload on the specified four videotape frames. The findings of PSNR commitment to improving matrix 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 also to bed all secret data, the current proposal was capable of hiding 27000 bytes to 65000 bytes for different pictures gradationally, but it was observed that the frames of Parrot achieved slightly higher PSNR values than other named images. Pixel selection approach is applied in the table 0.

TABLE 0. Provided Detecting Pixels from Cover Image

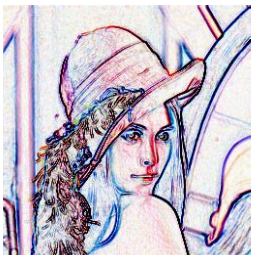
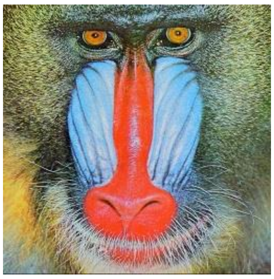
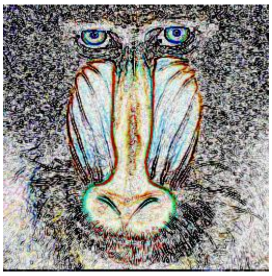
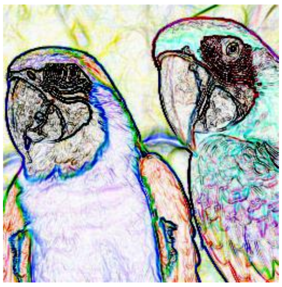
		29%
		56%
		29%

TABLE I. Quality measurement metrics of the projected method

Image	Dimension	Pixels Selections	Payload	PSNR	MSE	RMSE
Lenna	512X512	43%	512 Bytes	69.8456	0.0027	0.0519
	512X512		256 Bytes	72.0204	0.0013	0.0363
	512X512		128 Bytes	75.6643	0.0007	0.0260
Babbon	512X512	38%	512 Bytes	69.8655	0.0026	0.0512
	512X512		256 Bytes	72.8456	0.0013	0.0356

	512X512		128 Bytes	76.6664	0.0006	0.0252
Parrot	512X512	54%	512 Bytes	70.9645	0.0017	0.0417
	512X512		256 Bytes	73.6456	0.0010	0.0299
	512X512		128 Bytes	76.0695	0.0005	0.0223

In this board, 512 X 512 dimensioned images were utilized for Baboon, Lena, and Parrot, whereas load sizes of .512 Kilobytes, .256 Kilobytes, and .128 Kilobytes 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 (69.8456, 72.0204, 75.6643), (69.7655, 72.8456, 76.6664), and (69.8655, 72.8456, 76.6664), respectively (70.6645, 73.6456, 76.0695). We saw that Parrot had a higher quality than others.

TABLE 2 The comparison of three steganographic algorithms with 512 Bytes payload and 512 X 512 sized frame [31, 32, 41] In this table, the XOR substitution [32] model represents Model1, the 8-directional based model [31] denotes Model2, Combination of YCbCr and DWT [26] denotes Model3, Hiding Text In Color Image Using YCbCr Color Model [45] denotes Model 4, and our suggested model denotes P-Model, where the recital of the P-model denotes as Proposed Model is better than the current models.

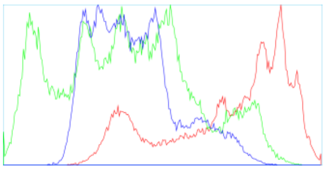
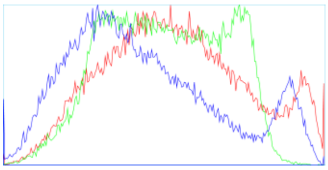
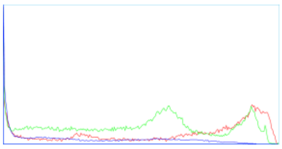
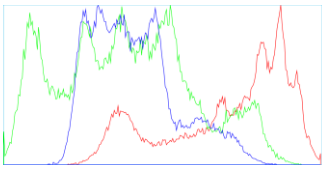
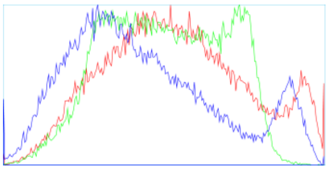
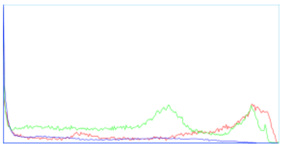
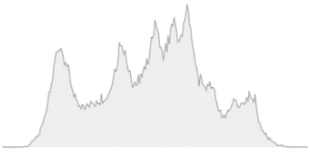
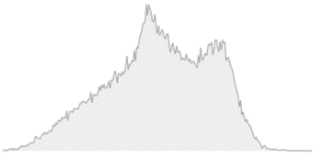
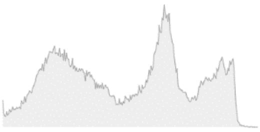
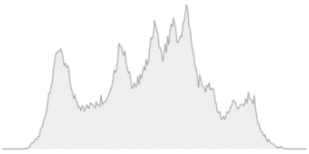
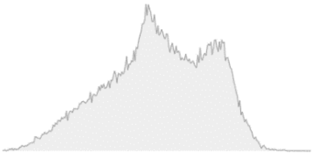
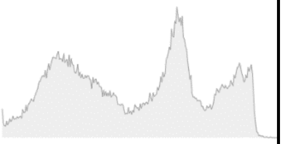
TABLE II. Comparison among recent steganographic techniques

Image	Model	Dimension	Payload	PSNR	MSE	Time (MiliSec)
Lenna	Model 1 (XOR substitution [32])	512X512	512 Bytes	66.5456	0.0029	171
	Model 2 (8-directional [31])	512X512	512 Bytes	68.5615	0.0028	169
	Model 3 (Combination of YCbCr and DWT [26])	512X512	512 Bytes	52.02	-	-
	Model 4 (YCbCr Color Model [45])	512X512	512 Bytes	44.52	-	-
	P-Model	512X512	512 Bytes	69.7456	0.0027	155
Babbon	Model 1 (XOR substitution [32])	512X512	512 Bytes	66.9655	0.0028	178
	Model 2 (8-directional [31])	512X512	512 Bytes	68.5315	0.0027	197
	Model 3 (Combination of YCbCr and DWT [26])	512X512	512 Bytes	48.87	0.84	-
	Model 4 (YCbCr Color Model [45])	512X512	512 Bytes	65.25	-	-
	P-Model	512X512	512 Bytes	69.7655	0.0026	184
Parrot	Model 1 (XOR substitution [32])	512X512	512 Bytes	65.5154	0.0029	245
	Model 2 (8-directional [31])	512X512	512 Bytes	68.3265	0.0027	178

	Model 3 (Combination of YCbCr and DWT [26])	512X512	512 Bytes	50.68	0.55	-
	Model 4 (YCbCr Color Model [45])	512X512	512 Bytes	55.52	-	-
	P-Model	512X512	512 Bytes	69.8645	0.0026	154

For the 3 photos above, the distribution is shown in Table 3 for the both the 512 X 512 cover picture and the stego picture.

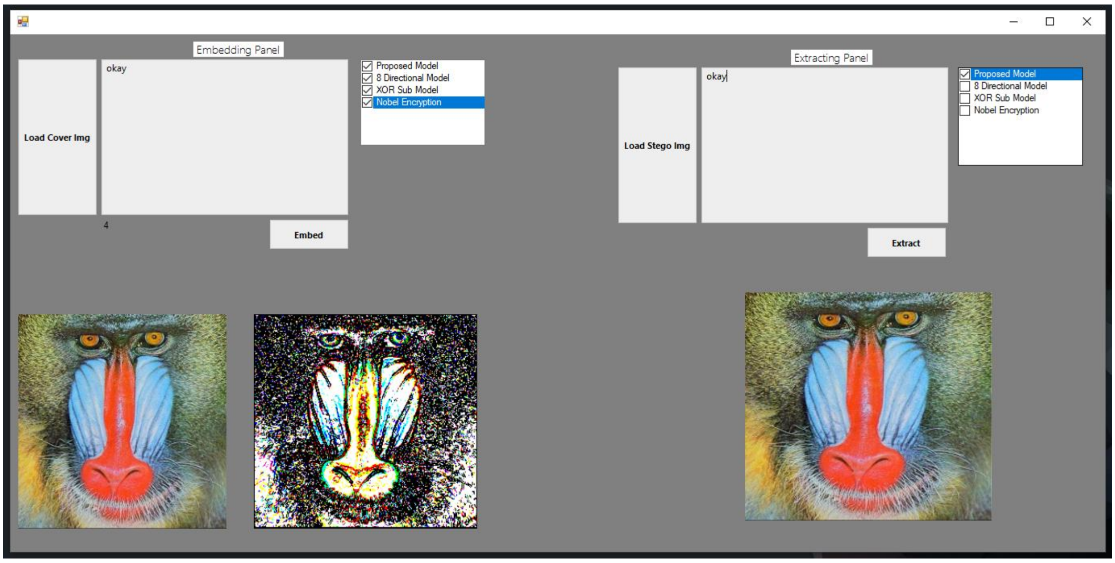
TABLE III. Comparison among recent steganographic techniques

Frames Type	Lenna	Babbon	Parrot
Cover			
Stego			
Cover (Gray)			
Stego (Gray)			

Consistent with an outcome of the bar diagram, the change amongst two frames is inconsequential, i.e.- these alterations cannot be predicted with bare eyes.

4.2 Implementation on Desktop App

We have implemented using c-sharp language



okay

☑ Proposed Model
☑ 8 Directional Model
☑ XOR Sub Model
☑ Nobel Encryption

4

okay

☑ Proposed Model
□ 8 Directional Model
□ XOR Sub Model
□ Nobel Encryption

Figure 9: Desktop Application

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

To hide confidential data using 1028-bit RSA encryption in the cover picture, this study proposes an automatic two-layer method for pictorial steganography to obfuscate Confidential data that combines LSB and XOR with a dynamic pixel allocation scheme. Unlike the current data-hiding techniques, the proposed steganography data-hiding method provides higher security and less complex encryption shown by supplementary discussion and proper performance tests.

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] Khudair, Enas Tariq, Ekhlas Falih Naser, and Alaa Noori Mazher. "Comparison between RSA and CAST-128 with Adaptive Key for Video Frames Encryption with Highest Average Entropy." Baghdad Science Journal 19.6 (2022): 1378-1378.

[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). Waknaghat, 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 YC b C r 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] Yudheksha, G. K., Prince Kumar, and Sharon Keerthana. "A study of AES and RSA algorithms based on GPUs." 2022 International Conference on Electronics and Renewable Systems (ICEARS). IEEE, 2022.

[37]. Harjito, Bambang, et al. "Comparative Analysis of RSA and NTRU Algorithms and Implementation in the Cloud." International Journal of Advanced Computer Science and Applications 13.3 (2022).

[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 (STMDF).”, 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] 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.

[47] Jain, Mamta, Saroj Kumar Lenka, and Sunil Kumar Vasistha. "Adaptive circular queue image steganography with RSA cryptosystem." Perspectives in Science 8 (2016): 417-420.

[48] Kusuma, Edi Jaya, et al. "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography." Journal Of ICT Research & Applications 12.2 (2018).

[49] Bhargava, Swati, and Manish Mukhija. "HIDE IMAGE AND TEXT USING LSB, DWT AND RSA BASED ON IMAGE STEGANOGRAPHY." ICTACT Journal on Image & Video Processing 9.3 (2019).