

Master of Science in Software Engineering

**A Secured Stenographic Technique in Spatial Domain for
Uncompressed Video.**

Md. Mushfiqur Rahman

ID: 213-44-229

March 2023

**Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY
Dhaka-1229, Bangladesh.**

**A Secured Stenographic Technique in Spatial Domain for
Uncompressed Video**



This thesis is submitted in partial fulfillment of the requirement for the degree of Master of
Science in Software Engineering.

Submitted by

Md. Mushfiqur Rahman

ID: 213-44-229

Supervised by

Md. Maruf Hassan

Associate Professor

**Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY**

Fall – 2022

Dhaka-1216, Bangladesh.

April, 2023

APPROVAL

This thesis/project/internship titled on "A Secured Stenographic Technique in Spatial Domain for Uncompressed Video", submitted by Md. Mushfiqur Rahman, ID: 213-44-229 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

Afsana Begum

Internal Examiner 2

Afsana Begum
Assistant Professor
Department of Software Engineering
Daffodil International University

Dr. Md. Saiful Islam

External Examiner

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

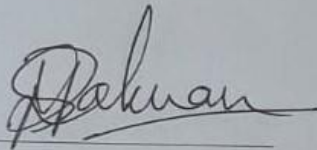
DECLARATION

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. Mushfiqur Rahman
Student ID: 213-44-229
Department of Software Engineering
Daffodil International University

Acknowledgment

I am very grateful to Daffodil International University for their guidance then consistent direction by Md. Maruf Hassan, Associate Professor of Software Engineering Department as well as for providing vital material about the journey and assistance in completing the assignment. I'd want to thank our parents, classmates, and DIU members for their kind cooperation and consolation, which enabled us to complete this assignment. I'd want to express my heartfelt gratitude and give credit to those who have given me comparable thought and time. My gratitude and appreciation also go to my partner in setting up the adventure and those who have steadfastly aided us with their abilities.

Abstract

In commercial, procedural, and legal procedures for the sensitive information, the best secrecy necessity must be emphasized. One remedy for this problem is cryptography, however if it is broken, there is no longer any data confidentiality. It could be reached out to computerized material as well as covering data in a picture. To build unintelligibility, strength, and payload limit, this examination demonstrates a progressive mechanized philosophy for accomplishing deuce stages of safety that joins encryption and steganography strategies. In the primary stage, the High-level AES calculation is utilized to scramble privileged information utilizing the .NET Structure of C-Sharp language, which is furnished by the client as contribution with a modernized, haphazardly produced 128-cycle secret key, which delivers the information disjointed. In the subsequent level, bitmap (BMP) pictures are utilized as an edge of video to spiritualists the encoded privileged information that delivers the information subtle, which is a steganography strategy. In order to preserve significantly high frame imperceptibility, the steganography algorithm uses the LSB methodology, XOR in conjunction with the 8 directional photo element election approach, a more secure image choosing methodology. The importance of quality measurement matrices has resulted in considerable advancements in the statistical analysis used to evaluate quality.

Keywords: Data hiding · Video steganography · Canny Pixel selection detection · LSB · AES
FFMPEG.

Table of Contents

Chapter 1	9
Introduction	9
1.1 Background and Present State of the Problem.....	9
1.2 Motivation of the Research.....	12
1.3 Objectives	12
1.4 Research Questions.....	12
1.5 Research Scope	13
1.6 Organization of the Report.....	13
Chapter 2	14
Literature Review	14
Chapter 3	17
Methodology.....	17
3.1 Encrypting the Secret Message.....	17
3.2 Steganographic Process	20
3.3 Algorithm for embedding and retrieving.....	23
3.4 Example	27
Chapter 4	30
RESULTS AND DISCUSSION.....	30
4.1 Result Discussion.....	30
Chapter 5	42
CONCLUSIONS AND RECOMMENDATIONS.....	42
References	43

List of Figures

Figure 3.1.1 : AES Encryption and Decryption process	17
Figure 3.1.1 : Frame Selection Based on Fisher Yeats through video splitter head parts in the c# language once the mystery message has been scrambled.	19
Figure 3.2.1 : Direction pixel selection positions.	21
Figure 3.2.2 : Embedding Process.	22
Figure 3.2.2 : Retrieving Process.....	23
Figure 3.4.1 : Embedding technique for 8 direction pixel position.	28
Figure 3.4.1 : Retrieve technique for 8 direction pixel position.	29
Figure 4.1 : Screenshot of proposed system	41

List of Tables

Table 4.1: PSNR for selected videos	33
Table 4.2: Quality measurement metrics of the projected method using different standard sized payload.....	35
Table 4.3: Comparison among 2 recent steganographic techniques.....	38
Table 4.4: Comparative histogram for cover and stego frames	39
Table 4.5: Bar Chart for PSNR values of selected frames.....	40

Chapter 1

Introduction

1.1 Background and Present State of the Problem

Due to fast progression of innovation, a ton of secret material is being kept on cloud servers, however security is likewise a significant issue in this day and age on the grounds that the cloud data set is kept up with by a solid outsider [1]. Albeit a few online protection methods, for example, information encoding and information hiding, have been embraced to address information security. Information encoding is a perceived type of encryption that changes a mystery message into an unlimited one. Nonetheless, the mystery figure message's substance likely could be gotten to by the aggressor since cryptography is available. Subsequently, cryptography doesn't give greater security like present information security interest. For the issue, two-level information security, for example, cryptography with steganography can be a solution. Words of steganography which is divided into “stegos (στεγανος)” and “grafia (γραφη’)” where “stegos” denote as “cover” , “grafia” denote as “writing” which become “covered writing”. There are two vital parts in steganography, the embedding system is one of them and extracting the data is another part. Obfuscation techniques is a kind of concealed handwriting which has been practiced for thousands of years. In 1499, a German security analyst identified as "Johannes Trithemius" camouflaged herself as a magic and printed a book on the study of steganography and cryptography, which resulted in the earliest documented use of the term [2]. Computer vision is a type of hiding data, which is a method of condensing communications onto daily cover used in a range of applications including healthcare systems, police departments, securing intellectual property, and security systems. [3]. Because the human eye is not very sensitive to minor changes in electronic material, leverage brief clips, video steganography can be was using to disguise the data in the film as well as the authenticity of the message. And feature extraction has become increasingly popular over time for two primary reasons: Furthermore, as software packages become more complex, metadata security issues become more relevant. Film is a silicon chips channel that may be more suitable than some other perceptive technologies due to the abundance of strong transmission improvements for computerized video contents and its compactness. The secret data, the cover paper, and the encoded

document are the four essential parts of a steganographic tactic. An effective steganographic system focuses primarily on preserving and improving three crucial characteristics, such as robustness, imperceptibility, and payload capacity. Both the spatial and frequency domains are possible applications for steganography [4]. The obfuscation techniques technology employs the image element of the cover object to conceal the private documents contained inside them in the wavelet coefficients. The secret data is hidden using steganographic techniques that work with the cover file's frequencies in the frequency domain. However, because it depends on anonymity, adopting simply steganographic methods is not a perfectly secure solution. If a service provider has a stego file and is knowledgeable about the procedure, they may be able to extract sensitive information. Our objective is to build an automated system that uses reliable encryption and steganographic technologies to completely eliminate this vulnerability. In this study, we offer our video steganalytic design, a type of fully automated device with two levels of concealment on the classified information entered by the client through a computerized methodology. Encryption of the restricted information in light of Cutting edge Encryption Standard (AES) calculation which gives better execution fast and requires low Smash [5] with 128 pieces randomize secret key utilizing Speck NET (. NET) System of C# language is the principal level of safety.

The second degree of safety contains concealing the encoded restricted information in Applying the obfuscation techniques theory described in this work, the film highlights (BMP image style, with the greatest discernible clarity). The Fisher- Yates method, which outperforms in unlimited combinations, randomly assigns the video sequence [6-7]. The objective of this research is to integrate image steganography and cryptographic methods to enhance the security of confidential material without compromising the video's accuracy or payload capacity. PVD, DCT, RPE, LSB, EBE, and MVD are really just a few of the video image steganographic we developed and decided to be utilized with 24-bit images. [8-10]. Nevertheless, the further utmost widespread and extensively used technique for a steganographic method is LSB [11] Depending on its basic encoding, it conceals secret bits within the LSB that correspond to certain picture elements of the colored picture frame. The advantage of LSB is that there's a decreased chance of the inventive cover file failing and that a covering document may carry more details. [11]. It is also possible to insert transmitted information directly and simply into the LSB location of the cover object, even if steganographic document brilliance is superior in LSB approach. Moreover, pixel selection method is increasingly significant since attackers are now acclimated to encryption algorithms, so typical pixel hiring decisions such as juke, chamfers, edge, and so forth are too familiar to attackers. Therefore, in our proposed model we used 8 directional-based pixel selection techniques which are more secure than the traditional technique [13]. Thusly, our objective is too

disguising secret messages is to be achieved in a speedy time and with a low pace of mistakes, what's more, to further develop heartiness, impalpability, and shipment limit moreover better flim excellence by coordinating solid steganographic innovation hooked on a computerization framework.

Those are few contributions:

- Encode the private information that use the 128 Bits method to generate a more complex steganographic system.
- Integrating the Aes with the Fisher-Yates notion randomized approach to increase data protection, wherein N (the amount of frame dependent on signal bit duration) is decided by combinations.
- Conveniently concealing or encoding private documents, in addition to sensitive data retrieval and decoding.
- Movies may reach an excess throughput to PSNR relation and some other quality evaluation metrics by combining the XOR or 1bit LSB methods with the eight directional pixels studies have examined the association.

The remainder of the document is arranged as tracks: The associated with current composition of steganography are described in Section 2. The proposed algorithm is succinctly illustrated in the following section. Then, using a flowchart and exemplification table, three different algorithms are illustrated in particular as to how we implemented the filtering approach, the embedding approach, and the rooting methodology. The performance assessment matrices utilized in the steganography method are displayed in the posterior section 4, along with some experimental findings. We've also contrasted it with a few other strategies. The paper's conclusion is illustrated at the end.

Whilst also evaluating someone being investigation work, it must have been discovered that many scientists involved recommended consolidating both steganography and cryptography for verification; however, in steganalysis, they was using traditional pixel classification process that are readily apparent and might allow attackers to soiree the involvement data utilizing visualize the data, and in cryptosystems, they used hash functions methodologies such as MD5, SHA-0, BASE64, and SHA-1 with certain flaws which could be misused by rainbow table attack.

1.2 Motivation of the Research

Recently, cyberspace full grownup into a significant technical framework for trimming industrial processes. Nowadays, vibrant organizations use internet hosting instead of organizing technology. They consume offered their amenities to website visitors concluded the cyberspace, allowing drug users to submit info through those online operations. To identify drug users belonging to a certain association, they have used the word-based authentication approach, which is now handicapped. A number of techniques have been created by interlopers to circumvent authentication systems, which can contribute to the theft, abuse, or loss of confidential data. Picture steganography, which is challenging to crack and can bridge the gap, is the primary motivation for the development of a security solution that would offer redundant subcomponents in authenticating systems.

1.3 Objectives

Those are few objectives given below:

- Encode the private information that use the 128 Bits method to generate a more complex steganographic system.
- Integrating the Aes with the Fisher-Yates notion randomized approach to increase data protection, wherein N (the amount of frame dependent on signal bit duration) is decided by combinations.
- Conveniently concealing or encoding private documents, in addition to sensitive data retrieval and decoding.
- Movies may reach an excess throughput to PSNR relation and some other quality evaluation metrics by combining the XOR or 1bit LSB methods with the eight directional pixels studies have examined the association..

1.4 Research Questions

- Is the suggested improved data concealment model effective?
- Is the established authentication approach producing better results than the other authentication techniques? To investigate the feasibility of real-time packet classification for launching selective jamming attacks considering an internal threat model.
- To analyze the geometric explanation.
- To detect selective jamming attack.

- To analyze the security of our schemes and show strong security with minimal impact on network performance.

1.5 Research Scope

Many organizations provided their members access to their services online. Thus, identification of their stoner depends heavily on authentication. In recent years, fraudsters have developed a number of techniques for disabling authentication systems. Nevertheless, we need to steadily increase this area's security. There are therefore several exploratory compasses in that sector.

1.6 Organization of the Report

The document uses the representation scheme in its investigation. The document is divided into 5 sections, which are listed underneath.

Chapter 1 This part covers the backdrop of the exploration, the provocation, the problem statement, and the items.

Chapter 2 This chapter discusses the job of getting associated and determining the exploration gap.

Chapter 3 Describes the exploratory methods and tactics that will be used during the investigation.

Chapter 4 Contrasts the outcomes of the experiments with existing methodologies.

Chapter 5 Discusses the exploration's outcomes and limitations, as well as the direction of the exploration's future work.

Chapter 2

Literature Review

The papers on steganography that are relevant to this research are contained in this section. These papers cover video steganography as well as other issues such as cryptography, random picture frame choosing, image element selection technique, and XOR with LSB method. The unique features or dependence on the LSB method, a commonly used steganalysis approach, were investigated in the bulk of these studies [11]. In such articles, LSB methods are used in the feature space. Karthikeyan B, et al. (2020) presented a way in [14] that could only hide confidential information, such as a OTP, into the carrier video file using simple LSB and arbitrary frame assortment, where the initial photo contains meta data, such as the frame number and extent of the hidden information, and another frame contains the hidden information. Despite the absence of the pixel selection strategy, this method managed to attain an excellent peak signal to noise ratio (PSNR). As a consequence, only LSB with basic color choice and a simple random framework is important approach can ensure appropriate information security. MB Tuieb and colleagues (2020) Although the results of their current proposal show that supreme function of the transport and digital image file is enhanced, only one level de risk is used in this investigation [15], therefore the security function is much less outstanding than that of the other design we've investigated. It typically focused on improving data security using video steganography utilizing basic random frame selection and simple LSB. In [16], Patil A, et al. (2018) employ AES encryption to encrypt plain text before implanting employing the LSB method as well as the 1-1-1 technique, the encrypted cypher text in each segmented frame of the cover video. Even so, the picture type used is not disclosed, as well as the panel method is not fully described. Despite the fact that quality measures are high, encryption may be enhanced by using the proper frame and pixel selection algorithms. In [17], Manohar N, Kumar PV (2020) projected a system that leverages video steganography to assure data security [28] The model achieved a high peak signal to noise ratio using a secure base LSB methodology, neural networks, and fuzzy logic, but it has significant flaws that prevent it from achieving additional security, such as insufficient knowledge about frame selection, pixel selection, video format, and frame rate. Singh N (2019) uses two distinct types of techniques, such as "XOR of message with LSBs" and "XOR of

message with symmetric key," to give for obfuscating [18]. In terms of measurement metrics, the first way, known as "XOR with LSB," is the most operationally similar to the revolutionary cover carrier, although "XOR of message with symmetric key" provides higher data concealing security. Unfortunately, the proposed methods heavily relied on different frames to conceal data, which is its main disadvantage in the meanwhile. Ajmera A, et al. (2019) proposed in [19] a slant which manages Stego in Changing dimension, thus weakening all faults of geographical region methods that really are subject to multiple assaults. They were using DCT and DST strategic plan just on video file while using data encryption for Rushing and achieved an acceptable outcome; even so, DCT as well as DST operation start giving fewer Signal to noise ratio self worth than the Lsb evidenced by Uphold Nevada as well as Lakshmi Versus((2018) [20] and is the biggest hindrance of a prototype; furthermore, those who didn't understand the technique of rim and bitmap selection which is absolutely critical in steganalysis. AES-256 encodes restricted data more effectively than AES-128 [22], so this could be a disadvantage of its implementation. Karthikeyan et al. (2017) [23] proposed a strategy to disguise restricted data into picture covering transporters that used a mix of two input LSB that DES calculation and provide a good result, albeit pixel choice on cover transporter is significantly less safe and faster than Des [24]. As a consequence, this paradigm may have a benefit. Alyousuf et al. developed a very well steganographic technique that incorporates an audio file into the carrying short clip (2017). Researchers ensured proper protection while improving PSNR by taking random frame in which the hidden bits got scrambled but then Decrypts the with unmodified LSBs of something like the transmission video codec frames. Yet, utilizing a proper pixel selection process instead of a popular and typical component may well have improves the security. T. Bhuiyan et al. (2019) suggested an image cryptographic framework for data hiding [12], wherein those who available a strategy that takes the encrypted connections, transform it to binary numbers, continues to perform a Reverse process among each Chroma voter's 6th index bit, but then integrate the generated outcome in each device's seventh indicator tad of Colorspace up to the final tad of the hidden code. However, employ a well loop pixel technique [13], in which pixels are purposefully picked from the beginnings of the picture matrix, which makes it simpler for hackers to detect the existence of undeclared data. Although the model produced good image quality, one of its major downsides is that it could possibly be exploited to boost confidentiality by using a broad and unusual pixel selection technique. In 2020, Mohamed A et al. proposed a model [26] with two levels of encoding and hiding processes. First, the message is scrambled using a private key and two XOR actions with binary representation. Afterwards when, an encrypted bit signal is injection into the payload of a cover image and used the LSB technique, producing a high PSNR value. In 2020, Ahmed A et al.

proposed a model [26] with two levels of encoding and hiding processes. First, the information is garbled using a secret key and doubly XOR operations with matched demarcation. Next, using the LSB approach, an encrypted piece information is inserted into the transporter of the cover picture, delivering a strong Signal to noise ratio. Alam ST et al. predicted a concept (2020) [13] that really can encompass confidential info into a photo cover shuttle and acquired an ultrahigh Signal to noise ratio by leveraging a remarkable bitmap structure based as the "8 directional pixel creation procedure," which is less recognizable to intruders than the standard pixel selection technique such as the Arrangement with comparator LSB outlook. The fact because they couldn't fit more than 765 characters into the a 512 x 512 cover object payload is a limitation, as well as the notion fact you inserted plain language right into the picture carrier causes concerns. This technique might be considerably more safe by applying an encryption software, such as AES, before inserting private data. We used the obvioulsy LSB technique, a spatial domain strategy to include secret information, to address the previous faults and inadequacies. Before placing the private data inside the cover bearer, we was using the AES strong encryption, which utilizes a 128-bit secret key generated randomly using automated c sharp language. The Bitwise approach applies to LSB while implantation to operational efficiencies in unpredictable variants. Moreover, in frame allocation, we employed a random technique based on "fishing yeats" concepts [7]. As both a consequence, we employed the common AVI video content [28] as well as a BMP image with the maximum lead to new insights grade [6,] as a video frame. In contrast to such measures, we employed Mean MAE, PSNR,SNR, MSE, RMSE, and embedding time quality assessment measurements, which could have offered a more efficient system than just another manner.

Chapter 3

Methodology

An automatic authority for support data hiding method for steganographic has indeed been designed to demonstrate the use of 1-bit Baseband one and XOR with an 8-directional pixel selection approach. In the next subsections, we will go through the cryptosystem, randomize picture choice according on the "fisher yeats" idea, and obfuscation techniques implementations in further depth.

3.1 Encrypting the Secret Message

Through our proposed apparatus, the client should enter the restricted information, which is naturally encoded whenever it is gotten. It is encoded utilizing AES, a symmetric encryption strategy that is very popular and safe [29]. AES might encode information blocks utilizing symmetric keys continuously of 128, 192, or 256 pieces, and it works a similar encryption key for both scrambling and decoding close information. Nonetheless, in this review, a 128-digit key length was utilized to encode the restricted information, which produces more prominent outcomes with quick velocity and needs little Smash [5]. Despite the fact that a 128-digit key size is tough at this point [22], it is given consequently by electronic capability. To guarantee information mystery whether or not it was recovered or not, 128-digit AES was utilized. Consequently, 128-digit AES was chosen with the aim of the assurance of information privacy generally a similar whether it was separated from the video outlines.

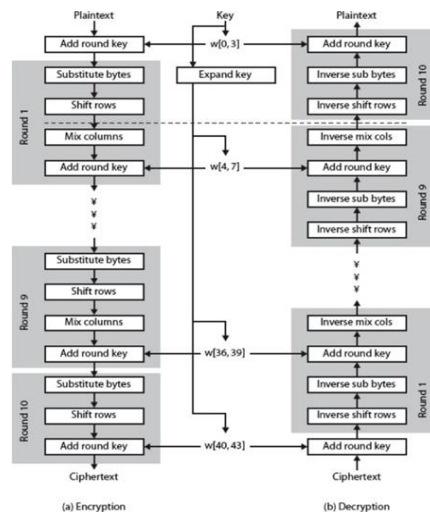


Figure 3.1.1 : AES Encryption and Decryption process

As shown in "Figure 1," the key length is 128 bits, and there are 10 rounds in each repetition cycle. The following four steps are included in each round: SubBytes, ShiftRows, MixColumns, and AddRoundKey [30]. A byte replacement mechanism called SubBytes initially applies a separate algorithm to each byte to produce a new value. The byte is then converted into another value using the S-box table by using its hexadecimal code. In the ShiftRows phase of AES, each line of the code's 128-bit inward state is moved. However long the AES is available for use, the Mix Columns activity is a significant module. The AES is gotten from divergence and direct decoding predominantly to the branch number of it, which guarantees that every consistent four rounds of the AES have no less than 25 dynamic S-Boxes. In each cycle, a special 128-bit round key that is created from the essential AES key is used. A capability characterized in the C# programming language executes the entire AES activity. The cover video transporter is extricated to BMP picture designed outlines.

Randomization Frame Selection Method

Throughout this approach, all collected images are chosen to use a randomness methodology based on Fischer Yeats principles, and the quantity stochastic images (Nf) utilized to enclose the hidden encryption algorithm (Sm L) and the duration (Dv) of cover file are determined using equations 1 and 2.

$$\text{MEMB} = \text{MaxDv of Dv} * 4 \text{ CD} * 3 \text{ bits} \dots\dots\dots (1)$$

$$\text{Nf} = \text{CB} / \text{MEMB} [\text{Where, } (\text{Nf} + 1) > 1] \dots\dots\dots (2)$$

Here, Message Embed Maximum (MEMB) stands for "bit per frame," CB for "total length of Cipher text in bits," and MaxDv for "maximum dimension of the inputted video," which may be either "width" or "height." Complete Direction (CD), which is equivalent to 8 directions, is signified. MaxDv and 4 CD were combined to give us the total number of pixels that can be embedded in a single frame, and 3 bit represents the 3-bit embedding capability for a single pixel.

Figure 2 depicts the frame method of selecting, which produces a variation according to the input value and the number of images. The images we chose are the initial $(\text{Nf} + 1) > 1$ frames from the permutation. Also, the frame sequence allows backward mix using the identical key, that will aid in recovery services

from pixels. The very first frame usually is then used gradually store elements like the scramble key, duration of the hidden information, and asymmetric cryptography.

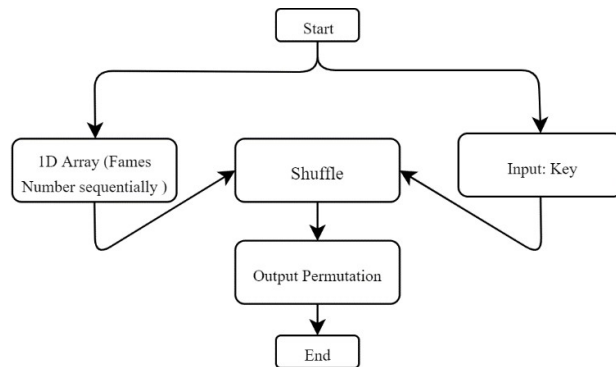


Figure 3.1.1 : Frame Selection Based on Fisher Yeats through video splitter head parts in the c# language once the mystery message has been scrambled.

3.2 Steganographic Process

The two aspects of the steganographic procedure are the embedding method and the retrieve technique. Figure 3 shows the embedding process of the suggested method, which involves taking user-supplied secret plain text and encrypting it using the 128-bit AES algorithm. Next, video frames are mined from the cover video, and the frame selection process is used to create a permutation of the video frames. Before beginning to embed data into the pixels of the chosen frames, a powerful pixel selection method known as the "8 directional pixel selection technique" is working in the function. There are a few processes in the data hiding function that must be completed gradually. The method discovers the height (H), width (W), and center position (Cx, Cy) of the frame sequentially before applying the 8-directional pixel selection approach to the identified frames. To determine the pixel value, use (Cx, Cy) and the third equation. On the other hand, a technique to determine the maximum amount of secret message bits that may be embedded into a frame using permutation and the equation (1). When message bit length will be less than the MEMB then it will follow the subsequent equations increasingly,

$$(Cx,Cy)=(2) \quad (3)$$

$$Tnp=(3) \quad (4)$$

Here Fd stands for frame dimensions which uses to find the center X and center Y. Therefore, Tnp stands for total number of pixels, BL stands for remain secret message bit length. By using the value of Tnp, it will get the value of Ppn which stands for Pixels Number for Each Direction using Eq. (5)

$$Ppn = \frac{(Tnp-1)}{8} \text{-----} (5)$$

Subsequently got the Ppn our model will use the equation (6) to find the 8 direction of pixels position (Ds) e.g., the Downhill equation will be (Cx, Cy+a) whereas Downhill -right direction will be denoted as (Cx+a,Cy+a) gradually [13] which are shown in figure 3.

$$Ds = (Cx\pm a, Cy\pm a) [where, a = 0 \text{ to } Ppn] \quad (6)$$

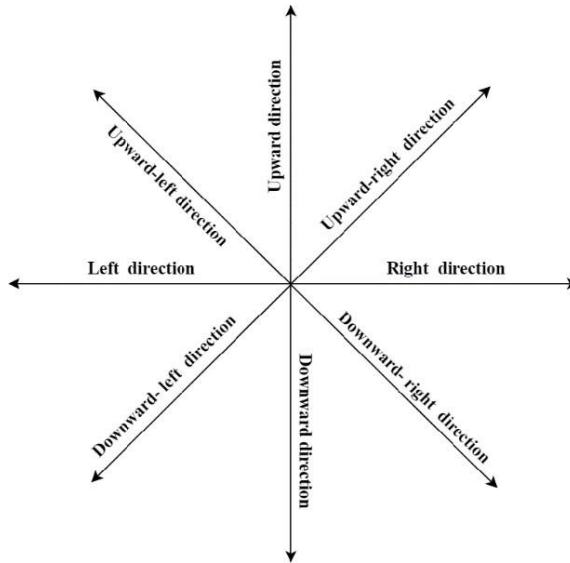


Figure 3.2.1 : Direction pixel selection positions.

Equation number (7, 8, 9, 10) is used to find out the four pixels' position where this method will embed the secret message bit size number which will use for retrieve message from stego frame when needed.

$$1^{\text{st}} \text{ pixel position, } (x_1, y_1) = \left(\frac{W}{2} - 3, 1 \right) \quad \text{----- (7)}$$

$$2^{\text{nd}} \text{ pixel position, } (x_2, y_2) = \left(\frac{W}{2} - 3, H \right) \quad \text{----- (8)}$$

$$3^{\text{rd}} \text{ pixel position, } (x_3, y_3) = \left(\frac{W}{2} + 3, H \right) \quad \text{----- (9)}$$

$$4^{\text{th}} \text{ pixel position, } (x_4, y_4) = \left(\frac{W}{2} + 3, 1 \right) \quad \text{----- (10)}$$

Notwithstanding, the fundamental edge is continuously employed to include relevant data, for example, the cipher key and fighting key, inside the eight heading pixel place, and their unit height quantity will be saved in a particular that contribute position, assisting with the repossession of the credentials from of the get these. The extra preferred outlines are then utilized to separately install private information as well as the expected to create opportunities length of the specific casing. Additionally, the recuperation cycle shown in Figures 4 and 5 is the inverse of the imbedding mechanism.

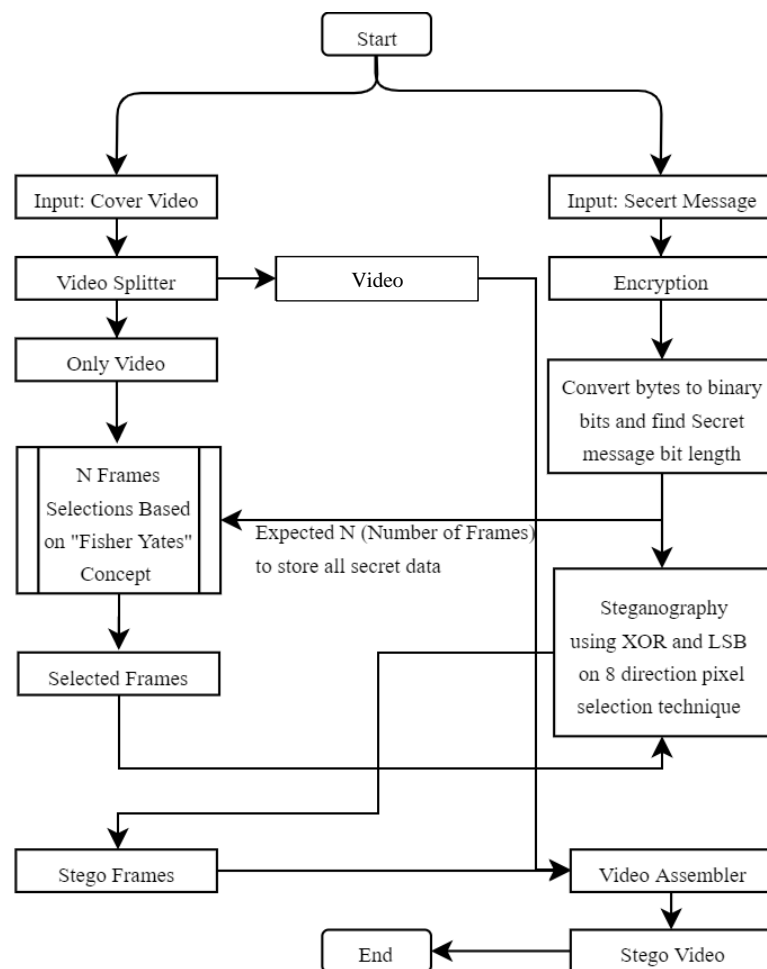


Figure 3.2.2 : Embedding Process.

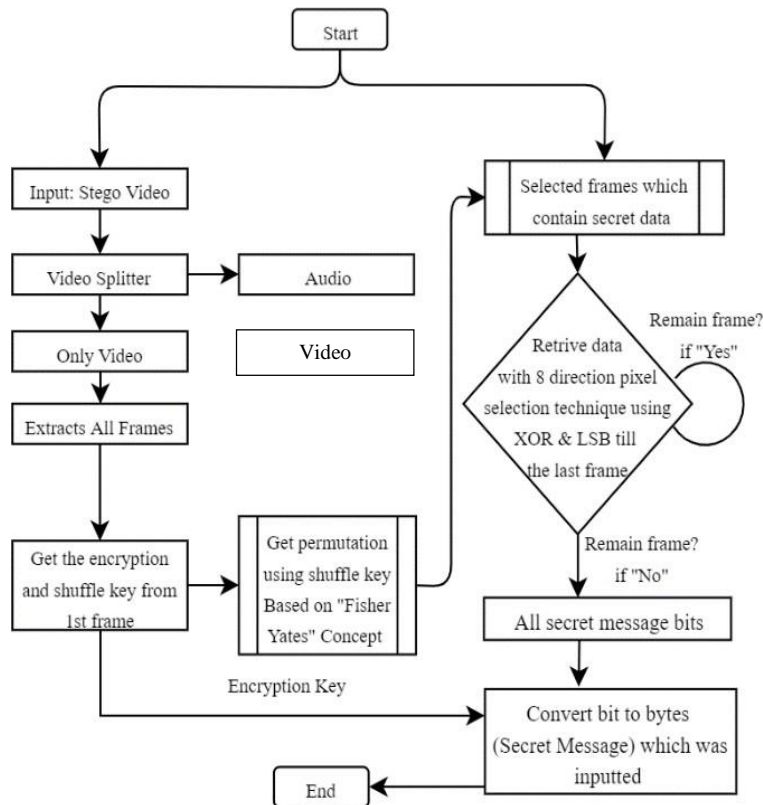


Figure 3.2.2 : Retrieving Process.

3.3 Algorithm for embedding and retrieving

The embedding and retrieval algorithm is used for the operations listed below, including data concealment, frame selection, encryption, and far more. Users provide the S_m (Secret message) and C_v (Cover video) components of the embedding process, whereas The hidden text as well as a 128-bit key are required by the AES function, which is employed to encode the confidential message. At the identical time, frames will be extracted into BMP formats in a separate thread. Following collecting the images (FE []), a numerical sequences and a randomised key would be entered into the FisherYeatsShuffle algorithm, that provides a permutation (FLp []). Based upon Fisher Yeats principles, the initial frame will embed just the insertion of location information (MD) using XOR technique into the Eight axis ($D_s = (C_xa, C_ya)$) as well as the remainder of the hidden data incorporate into to the remainder of pictures by Bitwise method

A stego video is procured by the user for the retrieving algorithm, which extracts it into BMP formats. The method then obtains meta data, including shuffle keys, encryption keys, and the total secret message bit number, from the 8-direction position. Using that shuffle key random permutation, the model then finds the required frames using the the whole message bit length.

Embedding Algorithm:

Result: Stego Video

$S_m \square \text{input}$ $C_v \square \text{input}$

$C_t = 128\text{-bit AES}(S_m, \text{key}); FE [] = \text{Extract_Frames}(C_v);$

$FLp [] = \text{FisherYeatsShuffle}(FE [], \text{key}); SF = CB / MEMB;$

$MD = \text{binary}(\text{shuffle key} + \text{salt} + \text{encryption key} + \text{salt} + \text{length of } S_m) \text{ embedMetaData}(SF [0], MD);$

$(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$ length of MD; $SMB = \text{binary}(S_m);$

$v = 0;$

For $\square SF [1 \text{ to } N-1]$ & $SMB [0 \text{ to } N-1]$

If $MEMB < SMB$

$\text{embedSecretDataXOR}(SF [v], SMB [v \text{ to } n])$

else

$W = \text{Frame Width};$

$H = \text{Frame Height};$

$(C_x, C_y) = (H/2, W/2);$

embed ((Cx, Cy)); BL= Length of M; Tnp= BL/3;

Ppn= (Tnp-1)/8; SMBL

length (SMB)

(x1, y1), (x2, y2), (x3, y3), (x4, y4) SML a = 0; □

while a ≤ Ppn do

Ds = (Cx±a, Cy±a) embedXOR (Ds); a++;

function embed (position): RGB← position UpdateRGB← message stegoFrame.Add (SF)

stegoVideo □ videoAssembler (stegoFrame [])

Retrieving Algorithm

Result: Secret Message

SV □ input

FE [] = Extract_Frames (Sv); MD = Retrive (FE [0]) ShuffleKey = MD.ShuffleKey

EncryptionKey = MD.EncryptKey

TotalSecretMessageLength = MD.MLength

FLp [] = FisherYeatsShuffle (FE [], ShuffleKey); SF = selectedFrame (FLp [], MD.MLength)

$v = 0;$

For \square SF [1 to N-1]

If MEMB < TotalSecretMessageLength

SMBL (x1, y1), (x2, y2), (x3, y3), (x4, y4)

SD [] = retrieveSecretDataXOR (SF [v], SMBL)

else

W = Frame Width;

H = Frame Height;

(Cx, Cy) = (H/2, W/2);

retrieve ((Cx, Cy)); BL= Length of M;

Tnp= BL/3;

Ppn= (Tnp-1)/8;

SMBL \square (x1, y1), (x2, y2), (x3, y3), (x4, y4) a = 0;

while a \leq Ppn do

Ds = (Cx \pm a, Cy \pm a)

SD [] = retrieveXOR (Ds, SMBL); a++;

+ 19 + @ + 128) = QDmOaAcgJAHrttSp@19@128 which converts to binary and produces an output that is 185 bits long with trim space, such as "01010001 01000100 01101101 01000001 01000001 01000001 01100011 01100111 0110010 01110100 01110100 01010011 01110000 01000000 00110001

00111001 01000000 00110001 00110010 00111000". Here, salt is employed as a barrier to help our system identify itself. As a result, the output will be embedded in the first frame in an 8-direction location, and its length will be added to the frame's four specific pixels using the XOR approach. To embed into 8 directions, the algorithm first finds the (C_x, C_y) , T_{np} , and P_{pn} . Where $(C_x, C_y) = (H/2, W/2) = (512/2, 512/2) = (256, 256)$ is our initial pixel where our first 3-bit secret meta data will be hidden, and T_{np} and P_{pn} values will be 62 and 7 progressively where 5 pixels will survive which will be connected into final direction. Therefore, each direction has 7 pixels, and each pixel works. Figure 6 shows two comparables in this manner.

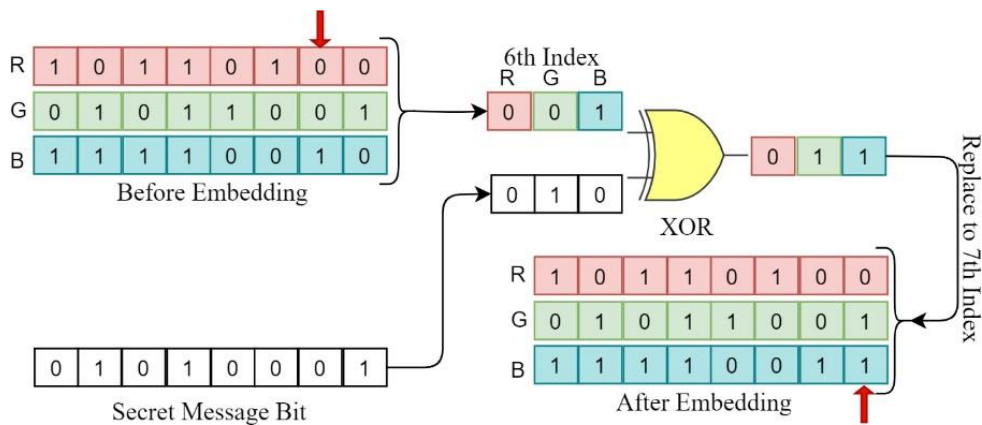


Figure 3.4.1 : Embedding technique for 8 direction pixel position.

After all secret meta data bits have been embedded into the first frame, the length of the meta data will be buried into four specified pixels that are required in the recovery operation. Every secret message bit will be concealed in all relevant frames using this method. The frames are then sent into the video assembler function, which generates stego video in the AVI format. Second, during the retrieval process, the system will take the stego video file (AVI format) and extract the BMP frames. And the first frame will be utilized to get the encryption, shuffle key, and total message length, where four specific pixels

(x1, y1), (x2, y2), (x3, y3), and (x4, y4) assist us in determining the length of meta data which is retrieved from the eight direction pixel positions shown in figure 7.

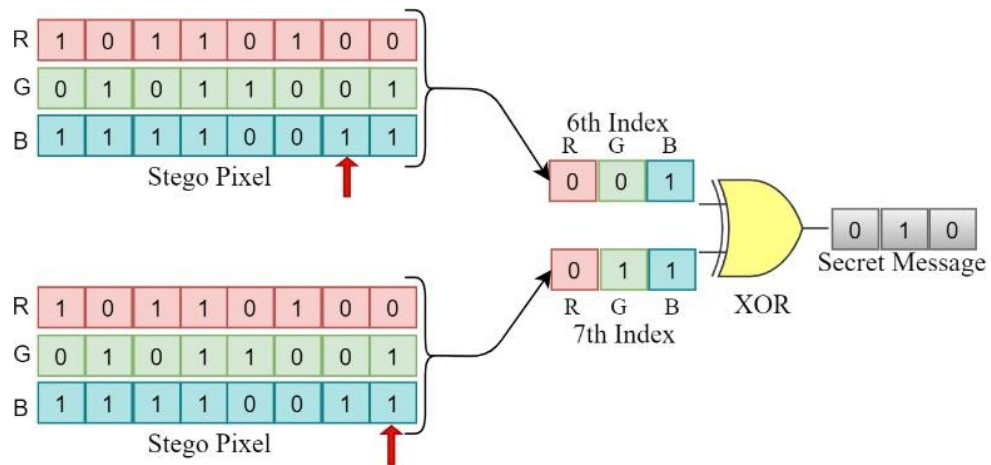


Figure 3.4.1 : Retrieve technique for 8 direction pixel position.

After acknowledging receipt of the shuffled key, decryption key, and original message length, our system may use the following equation to compute the frame permutation based on the shuffle key and the required frame that was used to disguise the secret message bit length during the embedding session (2). The remaining frames are then used to extract hidden information from certain four-pixel and eight-direction points for each frame. All secret data will be recovered, converted to bytes, and encrypted using a key created from the first frame of the stego video.

Chapter 4

RESULTS AND DISCUSSION

4.1 Result Discussion

In this area, the comparison and visual description of the results between the cover and stego video frame are shown. The effectiveness of the proposed technique is further supported by the results obtained using other [12, 13] well-known steganographic approaches. Six quality assessment indicators, including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Absolute Error (MAE), Signal-to-Noise Ratio (SNR), Root Mean Square Error (RMSE), and Mean-Square Error, are included in the statistical analysis of the research (MSE). Embedding Time, also known as Time to Complete the Embedding Process, is taken into account to assess the effectiveness of the proposed solution (TCEP).



DaffodilVarsity.avi



SaintMartin.avi



Bali.avi



Hobbit.avi

Two videos are selected (DaffodilVarsity, SaintMartin, Bali, Hobbit) for experimental test which are shown in figure 8. The format of two videos is AVI and their dimension is (512 x 512). Their duration

is 5 seconds, and FPS (25) are same. A text with large size is hidden within video file via proposed approach. The implementation of the technique and test the results are furnished via .NET Framework version 4.5.2 of c# language.



Figure 8. Cover Videos

The scientific explanation for the specified six frame quality measurement matrices (i.e., PSNR, SSIM, MAE, SNR, RMSE, and MSE) are illustrated in Eq. 11 to 15 which are the commonly used factor to measure the efficiency and safety of the steganographic process [12, 13, 31-33]

The Mathematical explanation for PSNR is [34]

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (11)$$

Here the unit of PSNR is dB which depends on MSE. Several research prove that if the value of PSNR between cover and stego frame become more than 40 dB then it considers as acceptable.

The Scientific definition for SSIM is [35]

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1) + (2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (12)$$

Here, the image dimension is denoted by x and y. $C_1 = (k_1L)^2$ and $C_2 = (k_2L)^2$ are two variable

quantities to alleviate the partition where μ_x and μ_y are the average of x ,

$$MAE = \frac{1}{3MN} \sum_{i=1}^M \sum_{j=1}^N [C(x, y) - S(x, y)]_1 \quad (13)$$

y with weak denominator where $K1 = 0.01$ and $k2 = 0.03$ by default, in addition, the dynamic range of the pixel-values defined as L . The Mathematical explanation for MAE is [36]

Here, the image dimension denoted by $M \times N$, the position of pixel refers as (x, y) . The cover frame is epitomized by C and S denotes the stego frame and $[\cdot]_1$ signifies the city-block ordinary.

The Mathematical elucidation for SNR is [37]

$$SNR = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \hat{f}(x, y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x, y) - \hat{f}(x, y)]^2} \quad (14)$$

The formula is from Digital Image Processing Here, the noisy frame represented by \hat{f} , the original frame denoted by f and x, y refers the location of a pixel.

The Scientific definition for RMSE which is the squared root base of MSE [38],

$$RMSE = \sqrt{MSE} \quad (15)$$

The Scientific definition for MSE is [39]

$$MSE = (1xMxN) \sum_{i=1}^M \sum_{j=1}^N (a_{ij} - b_{ij})^2 \quad (16)$$

In this formula, the pixel value of the location i and j of the cover frame refers as a_{ij} where b_{ij} refers to the pixel value of the location i and j of stego frame.

Result of the proposed method are restrained with 15 Kilobytes payload on the selected four video frames. Table 1. signifies the results of PSNR quality measurement matrices for given frames.

Table 4.1: PSNR for selected videos

Frame No	Daffodil Varsity (PSNR)	SaintMart in (PSNR)	Bali (PSNR)	Hobbit (PSNR)
01 (Mb)	79.23 90	78.92 69	78.6890	78.55 97
02 (SMB)	72.41 23	72.32 63	72.2630	72.25 30
03 (SMB)	72.43 43	72.35 78	72.2835	72.25 84
04 (SMB)	72.50 01	72.34 94	72.2958	72.25 94
05 (SMB)	72.49 52	72.32 09	72.2094	72.25 47
06 (SMB)	72.47 71	72.32 87	72.2906	72.23 45
07 (SMB)	72.45 63	72.39 12	72.2523	72.22 85
08 (SMB)	72.41 09	72.48 44	72.2712	72.29 76
09 (SMB)	72.48 89	72.32 42	72.2944	72.22 34
10 (SMB)	72.50 99	72.32 33	72.2203	72.25 67
11 (SMB)	72.49 11	72.32 74	72.3965	72.24 93
12 (SMB)	72.42 86	72.36 88	72.2945	72.26 87
13 (SMB)	72.50 13	72.31 27	72.2099	72.22 34
14 (SMB)	72.51 09	72.41 01	72.2506	72.26 56
15 (SMB)	72.30 99	72.33 09	72.2054	72.27 87
16 (SMB)	72.40 19	72.32 17	72.2470	72.24 05
17 (SMB)	72.50 88	72.32 98	72.2694	72.24 56

18 (SMB)	72.48 63	72.31 34	72.2547	72.24 59
19 (SMB)	72.41 28	72.34 95	72.2231	72.25 69
20 (SMB)	72.47 13	72.36 07	72.3458	72.39 55
21 (SMB)	75.97 88	75.72 65	74.9949	75.16 97

In this table, 512 X 512 sized frames were used for DaffodilVarsity, StaintMartin, Bali, and Hobbit where payload was 15 Kilobytes or 15000 bytes, to embed all secret data our system used 21 frames where each frame concealed maximum 765 bytes gradually where the frames of DaffodilVarsity achieved slightly higher PSNR values than other selected video frames. Table 2. signifies the results of six quality measurement matrices values with different payloads such as 512 bytes, 256 bytes and 128 bytes for a certain frame and embedding time of the stego frame. Here, DaffodilVarsity denoted as DV, SaintMartin denoted as SM, Bali denoted as BA, and Hobbit presented as HO.

Table 4.2: Quality measurement metrics of the projected method using different standard sized payload

Parameter	Dimension	Payload	PSNR	SSIM	MAE	SNR	RMS E	MSE	TCEP
DV	512 X 512	512 Bytes	74.082	0.999992913	0.0026	68.5991	0.0509	0.0026	6.47s
		256 Bytes	77.185	0.999997723	0.0012	71.7794	0.0352	0.0012	5.45s
		128 Bytes	80.2390	0.999999726	0.0006	74.8299	0.0248	0.0006	4.52s
SM	512 X 512	512 Bytes	74.079	0.999995854	0.0026	68.3356	0.0509	0.0026	6.23s
		256 Bytes	77.1467	0.999999646	0.0012	70.9540	0.0351	0.0012	5.93s
		128 Bytes	80.053	0.999999867	0.0006	74.8168	0.0249	0.0006	4.45s
		512 Bytes	74.189	0.999997803	0.0026	67.7820	0.0509	0.0026	6.12s
BA	512 X 512	256 Bytes	76.467	0.999999125	0.0013	70.6099	0.0367	0.0013	5.59s
		128 Bytes	80.1678	0.999999650	0.0006	73.9368	0.0250	0.0006	4.56s

HO	512X 512	512 Byte s	74 .0 11 2	0.999 99740 3	0.00 26	67.72 34	0.05 09	0.0026	6.73 s
		256 Byte s	76 .7 43 8	0.999 99892 5	0.00 13	70.52 83	0.03 71	0.0013	5.98 s
		128 Byte s	80 .0 44 3	0.999 99935 0	0.00 06	73.85 48	0.02 52	0.0006	4.56 s

In this table, DV, SM, BA, and HO video frames are used with 512 X 512 dimension where different payload size of 512 bytes, 256 bytes, and 128 bytes correspondingly had been taken for contemplation. PSNR values 74.0082, 77.1885, and 80.2390 were found for different payloads of DV. For SM the PSNR were 74.0079, 77.1467, 80.2053 gradually where the PSNR were 74.0189, 76.8467, and 80.1678 for BA and HO got 74.0112, 76.7438, and 80.0443 PSNR value progressively where DV provided better PSNR than other frames. The value of SSIM for DV were 0.999992913, 0.999997723, and 0.99999726 gradually where 0.999995854, 0.99999646, and 0.99999867 SSIM value was founded for SM, in addition BA provided 0.999997803, 0.999999125, and 0.999999650 SSIM value respectively, and 0.999997403, 0.999998925, 0.999999350 values were provided from HO. The value of MAE for DV were 0.0026, 0.0012, and 0.0006 gradually where all other frames provided quite similar value. For SNR, 68.5991, 71.7794, and 74.8299 values were provided by DV where 68.3356, 70.9540, and 74.8168 were founded from SM, furthermore, BA was provided 67.7820, 70.6099, and 73.9368 gradually and 67.7234, 70.5283, 73.8548 were founded from HO frame. For RMSE and MSE the value of all frames is quite similar. However, HO provides the better quality for embedding process which received 6.73s, 5.98s, and 4.56s increasingly to embed 512 Bytes, 256 Bytes, and 128 Bytes secret data gradually and the performance for other three frames are quite similar.

Table 3. provides the result of comparison among 2 recent steganographic techniques with 512 Bytes payload and 512 X 512 sized frame [12, 13]. XOR substitution [12] model denotes as Model1, 8 directional based model [13] denotes as Model2 and our proposed model denotes as P-Model in this table and the selected frames such as DaffodilVarsity denoted as DV, SaintMartin denoted as SM, Bali denoted as BA, and Hobbit presented as HO also.

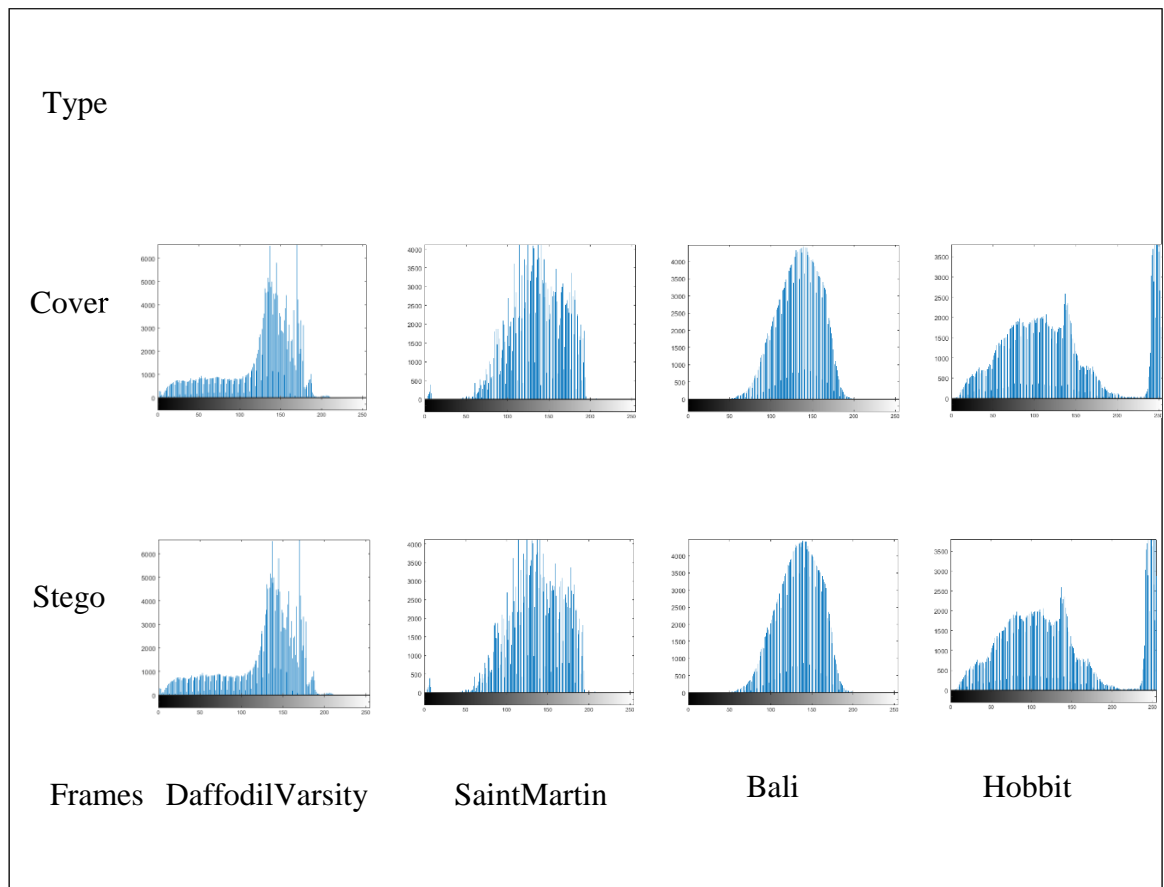
Table 4.3: Comparison among 2 recent steganographic techniques

Techniques	Frame	PSNR	SSIM	MAE	SNR	RMSE	MSE	TCEP
Model 1	DV	69.74 83	0.999 98498 5	0.002 9	64.47 85	0.05 39	0.002 9	8.4545 s
Model 2		73.18 45	0.999 99195 6	0.002 7	67.86 86	0.05 20	0.002 7	5.9646 s
P-Model		74.00 82	0.999 99291 3	0.002 6	68.59 91	0.05 09	0.002 6	6.4754 s
Model 1	SM	70.09 66	0.999 98956 6	0.002 9	65.12 99	0.05 39	0.002 9	8.2331 s
Model 2		73.95 65	0.999 99102 3	0.002 6	67.20 94	0.05 08	0.002 6	5.5413 s
P-Model		74.00 79	0.999 99585 4	0.002 6	68.33 56	0.05 09	0.002 6	6.2311 s
Model 1	BA	70.98 56	0.999 98980 3	0.002 8	65.78 20	0.05 29	0.002 8	7.4546 s
Model 2		73.67 34	0.999 99385 4	0.002 7	66.99 43	0.05 19	0.002 7	5.5112 s
P-Model		74.01 89	0.999 99780 3	0.002 6	67.78 20	0.05 08	0.002 6	6.1241 s
Model 1	HO	70.95 68	0.999 98740 3	0.002 8	65.84 55	0.05 29	0.002 8	7.5465 s
Model 2		73.88 96	0.999 99309 6	0.002 7	67.19 59	0.05 19	0.002 7	5.1445 s
P-Model		74.01 12	0.999 99740 3	0.002 6	67.72 34	0.05 09	0.002 6	6.7365 s

In this table, the 1st column shows the result of PSNR value where the performance of P-Model (Proposed Model) is better than the Model1 and Model2 where their values were 69.7483, 73.1845, and 74.0082 gradually for DV frame. The result for each column is better for proposed model than the existing models without TCEP result. Cause, our proposed model provides more security than the existing model that's why it takes slight bit extra time than the existing model.

The Table 4 shows the histogram for both 512×512 sized cover and stego frames for the above four selected video frames.

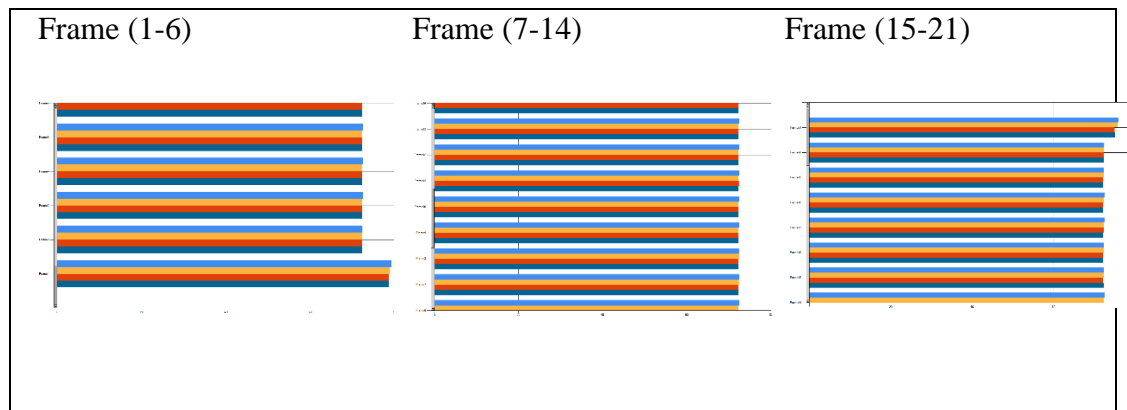
Table 4.4: Comparative histogram for cover and stego frames



Consistent with result of histogram, the difference between two frames is inconsequential which alteration cannot be predictable with naked eye.

The table 5 shows the bar graph for PSNR quality measurement matrices for given frames.

Table 4.5: Bar Chart for PSNR values of selected frames



Consistent with result of bar chart, the difference among 4 selected frame is inconsequential which alteration is quite similar although the result for DaffodilVarsity's (Frame) performance is quite better than other frames.

This data hiding approach is applied in this experiment which shows projected procedure works better as compared to other related algorithms as well.

Here is the Screenshot of our proposed system which is implemented and still under development for few features and beta release.

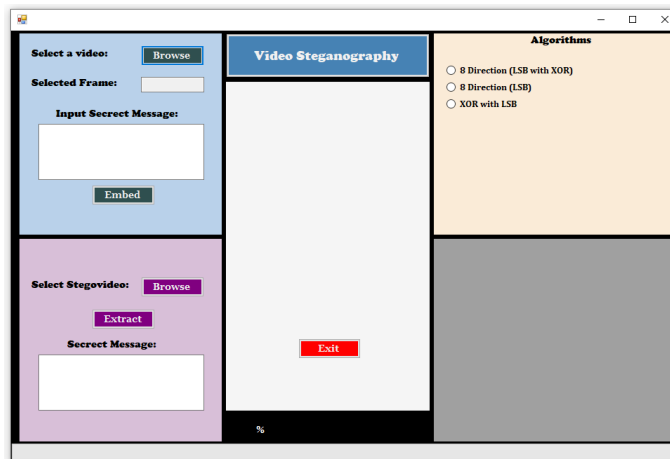


Figure 4.1 : Screenshot of proposed system

Chapter 5

CONCLUSIONS AND RECOMMENDATIONS

The secret message is hidden with robust 128-bit AES encryption in the cover movie using an automated two-level safe data concealing system for video steganography that is given in this work. The suggested steganography data concealing approach offers more security and less imperceptibility than certain other current data concealing strategies, as shown by the overhead discussion and reasonable result analysis. However, this model can hide up to 95,625 bytes of secret data in a cover movie that is 512 by 512 in size and runs for 5 seconds at 25 frames per second. We will remove such restrictions our next work.

References

- [1] Nyo HL, Oo AW. Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT. *International Journal of Computer Network & Information Security*. 2019 Jun 1;11(6).
- [2] Zhou H, Zhang W, Chen K, Li W, Yu N. Three-Dimensional Mesh Steganography and Steganalysis: A Review. *IEEE Transactions on Visualization and Computer Graphics*. 2021 Apr 22.
- [3] "Video-HiDef Audio and Video". hidefnj.com. Archived from the original on 2017-05-14. Retrieved 2017-03-30
- [4] Narula M, Gupta M, Garg M. Implementation of hybrid technique from spatial and frequency domain steganography: Along with cryptography to withstand statistical attacks. In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) 2020 Dec 18 (pp. 803-808). IEEE.
- [5] Harba ES. Secure data encryption through a combination of AES, RSA and HMAC. *Engineering, Technology & Applied Science Research*. 2017 May 7;7(4):1781-5.
- [6] Ansari AS, Mohammadi MS, Parvez MT. A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security*. 2019;11(1):11-25.
- [7] Ma K, Teng L, Wang X, Meng J. Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory. *Multimedia Tools and Applications*. 2021 Apr 10:1-21.
- [8] Mstafa RJ, Elleithy KM. Compressed and raw video steganography techniques: a comprehensive survey and analysis. *Multimedia Tools and Applications*. 2017 Oct;76(20):21749-86.
- [9] Rachmawanto EH, Prasetyo K, Sari CA, De Rosal IM, Rijati N. Secured PVD Video Steganography Method based on AES and Linear Congruential Generator. In 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI) 2018 Nov 21 (pp. 163-167). IEEE.
- [10] Pilania U, Gupta P. Analysis and implementation of IWT-SVD scheme for video

- steganography. In *Micro-Electronics and Telecommunication Engineering 2020* (pp. 153-162). Springer, Singapore.
- [11] Astuti YP, Rachmawanto EH, Sari CA. Simple and secure image steganography using LSB and triple XOR operation on MSB. In *2018 International Conference on Information and Communications Technology (ICOIACT) 2018 Mar 6* (pp. 191-195). IEEE.
- [12] Bhuiyan T, Sarower AH, Karim R, Hassan M. An image steganography algorithm using LSB replacement through XOR substitution. In *2019 International Conference on Information and Communications Technology (ICOIACT) 2019 Jul 24* (pp. 44-49). IEEE.
- [13] Alam ST, Jahan N, Hassan MM. A New 8-Directional Pixel Selection Technique of LSB Based Image Steganography. In *International Conference on Cyber Security and Computer Science 2020 Feb 15* (pp. 101-115). Springer, Cham.
- [14] Karthikeyan B, Raj MA, Yuvaraj D, Sundar KJ. A Hybrid Approach for Video Steganography by Stretching the Secret Data. In *Inventive Communication and Computational Technologies 2020* (pp. 1081-1087). Springer, Singapore.
- [15] Tuieb MB, Abdullah MZ, Abdul-Razaq NS. ‘An efficiency, secured and reversible video steganography approach based on lest significant. *J. Cellular Automata*. 2020 Apr;16(17).
- [16] Patil A, Keshkamat SM, Desai VV, Arlimatti T. Embedding of Advanced Encryption Standards Encoded Data in Video using Least Significant Bit Algorithm. In *2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE) 2018 Jul 27* (pp. 617-621). IEEE.
- [17] Manohar N, Kumar PV. Data Encryption & Decryption Using Steganography. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) 2020 May 13* (pp. 697-702). IEEE.
- [18] Singh N. XOR Encryption Techniques of Video Steganography: A Comparative Analysis. *International Conference on Intelligent Systems Design and Applications 2018 Dec 6* (pp. 203-214). Springer, Cham.
- [19] Ajmera A, Divecha M, Ghosh SS, Raval I, Chaturvedi R. Video Steganography: Using Scrambling-AES Encryption and DCT, DST Steganography. In *2019 IEEE Pune Section International Conference (PuneCon) 2019 Dec 18* (pp. 1-7). IEEE.

- [20] Brindha NV, Meenakshi VS. Comparison Analysis of Bio watermarking Using DWT, DCT and LSB Algorithms. In Computational Vision and Bio Inspired Computing 2018 (pp. 849-863). Springer, Cham.
- [21] Hashim J, Hameed A, Abbas MJ, Awais M, Qazi HA, Abbas S. LSB Modification based audio steganography using advanced encryption standard (AES-256) technique. In 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) 2018 Nov 24 (pp. 1-6). IEE
- [22] Andriani R, Wijayanti SE, Wibowo FW. Comparison Of AES 128, 192 And 256 Bit Algorithm For Encryption And Description File. In 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE) 2018 Nov 13 (pp. 120-124). IEEE.
- [23] Karthikeyan, B., Deepak, A., Subalakshmi, K. S., Anishin Raj M M, & Vaithiyanathan, V. (2017). A combined approach of steganography with LSB encoding technique and DES algorithm. 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). doi:10.1109/aeicb.2017.7972388
- [24] Sousi, Ahmad-Loay, Dalia Yehya, and Mohamad Joudi. "AES Encryption: Study & Evaluation." (2020).
- [25] Alyousuf FQ, Din R, Qasim AJ. Analysis review on spatial and transform domain technique in digital steganography. Bulletin of Electrical Engineering and Informatics. 2020 Apr 1;9(2):573-81.
- [26] Ahmed A, Ahmed A. A Secure Image Steganography using LSB and Double XOR Operations. IJCSNS. 2020 May;20(5):139.
- [27] Astuti, Y. P., Setiadi, D. R. I. M., Rachmawanto, E. H., & Sari, C. A. (2018). Simple and secure image steganography using LSB and triple XOR operation on MSB. 2018 International Conference on Information and Communications Technology (ICOIACT). doi:10.1109/icoiact.2018.8350661
- [28] Yang Y, Xu Z, Liu L, Sun G. A security carving approach for AVI video based on frame size and index. Multimedia Tools and Applications. 2017 Feb 1;76(3):3293-312.
- [29] Patel K. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. International Journal of Information Technology. 2019 Dec;11(4):813-9.

- [30] Hoomod HK, Radi AM. New Secure E-mail System Based on Bio-Chaos Key Generation and Modified AES Algorithm. In *Journal of Physics: Conference Series* 2018 May 1 (Vol. 1003, No. 1, p. 012025). IOP Publishing.
- [31] Mikhailiuk A, Perez-Ortiz M, Yue D, Suen WS, Mantiuk R. Consolidated Dataset and Metrics for High-Dynamic-Range Image Quality. *IEEE Transactions on Multimedia*. 2021 Apr 29.
- [32] Zhai G, Min X. Perceptual image quality assessment: a survey. *Science China Information Sciences*. 2020 Nov;63:1-52.
- [33] Kazemi M, Ghanbari M, Shirmohammadi S. The performance of quality metrics in assessing error-concealed video quality. *IEEE Transactions on Image Processing*. 2020 Mar 31; 29:5937-52.
- [34] Mozhaeva A, Streeter L, Vlasuyk I, Potashnikov A. Full Reference Video Quality Assessment Metric on Base Human Visual System Consistent with PSNR. In *2021 28th Conference of Open Innovations Association (FRUCT) 2021 Jan 27* (pp. 309-315). IEEE.
- [35] Tang Y, Ren F, Pedrycz W. Fuzzy C-means clustering through SSIM and patch for image segmentation. *Applied Soft Computing*. 2020 Feb 1; 87:105928.
- [36] Abdel-Basset M, Chang V, Mohamed R. A novel equilibrium optimization algorithm for multi-thresholding image segmentation problems. *Neural Computing and Applications*. 2020 Mar 16:1-34.
- [37] Ma L, Sun J, Jiang P, Liu D, Zhou X, Wang Q. Signal extraction algorithm of Gm-APD lidar with low SNR return. *Optik*. 2020 Mar 1; 206:164340.
- [38] Xu S, Amira O, Liu J, Zhang CX, Zhang J, Li G. HAM-MFN: Hyperspectral and multispectral image multiscale fusion network with RAP loss. *IEEE Transactions on Geoscience and Remote Sensing*. 2020 Jan 28;58(7):4618-28.
- [39] Wang D, Gan W, Yan C, Huang K, Wu H. Inception Model of Convolutional Auto-encoder for Image Denoising. In *International Conference on Mobile Computing, Applications, and Services 2020 Sep 12* (pp. 174-186). Springer, Cham.
- [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.