



Daffodil
International
University

**A Video Steganography using LSB Technique with AES algorithm to
improve robustness against visual attack**

Submitted By

Nowrin Islam Nishat

ID: 193-35-483

Department Of Software Engineering

Supervised By

Nadira Islam

Lecturer

Department Of Software Engineering

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

Fall 2023

©All right reserved by Daffodil International University

APPROVAL

This thesis titled on "A video steganography technique with AES algorithm to improve robustness against visual attack", submitted by Nowrin Islam Nishat (ID: 193-35-483) 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 Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS



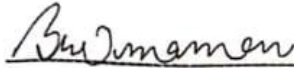
Chairman

Dr Md. Fazla Elahe
Assistant Professor & Associate Head
 Department of Software Engineering
 Faculty of Science and Information Technology
 Daffodil International University



Internal Examiner 1

A.H.M Shahariar Parvez
Associate Professor
 Department of Software Engineering
 Faculty of Science and Information Technology
 Daffodil International University



Internal Examiner 2

Khalid Been Budruzzaman Biplob
Lecturer (Senior Scale)
 Department of Software Engineering
 Faculty of Science and Information Technology
 Daffodil International University



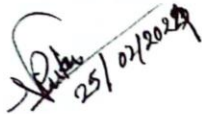
External Examiner

Md Mostafiz Khan
 Managing Director
 Tecognize Solutions Limited

DECLARATION

This thesis was completed under the supervision of Nadira Islam Ruku, Lecturer, 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:



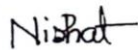
Nadira Islam Ruku

Lecturer

Department of Software Engineering

Faculty of Science & Information Technology

Daffodil International University



Name: Nowrin Islam Nishat

Student ID: 193-35-483

Batch: 30

Department of Software Engineering

Faculty of Science & Information Technology

Daffodil International University

ACKNOWLEDGEMENT

I had experienced some problems when i writing my thesis. That being said, it would not have been feasible without the kind support and cooperation of multiple people. I could feel the need tobroaden my attention because of all of them. I have an obligation of gratitude to Daffodil International University for all of their help with this assignment, including crucial information onthe adventure and constant supervision from Ms. Nadira Islam. I might want to offer my thanks toall for their coordinated effort and comfort in assisting us with completing this work. I should needto offer my genuine appreciation and recognize the people who have contributed a comparative measure of time and thought as me. My partner in setup likewise has my gratitude and appreciation.

APPROVAL	ii
DECLARATION	iii
ACKNOWLEDGEMENT	iv
TABLE OF CONTENT	v
LIST OF TABLE	vi
LIST OF FIGURE	vii
ABSTRACT	viii
CHAPTER 1: INTRODUCTION	1
1.1 Background	1
1.2 Motivation of the Research	4
1.3 Problem Statement	5
1.4 Research Questions	5
1.5 Research Objectives	6
1.6 Research Scope	6
1.7 Thesis Organization	7
CHAPTER 2: LITERATURE REVIEW	7
CHAPTER 3: METHODOLOGY	11
3.1 Encrypting Secret Message	11
3.2 Pixel Filtering Algorithm	12
3.3 Randomization Frame Selection Method	13
3.4 Algorithm for embedding and retrieving.	16
CHAPTER 4: RESULTS AND DISCUSSION	27
CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS	37
REFERENCES	38

Table 1: PSNR for selected videos	Error! Bookmark not defined.
Table 2: Quality measurement metrics of the projected method using different standard sized payload	31
Table 3: Comparison among 2 recent steganographic techniques	32
Table 4: Comparative histogram for cover and stego frames	35

LIST OF FIGURES

Figure 1: AES Encryption and Decryption process	13
Figure 2: Frame Selection Based on Fisher Yeats	15
Figure 3: 8 direction pixel selection positions	17
Figure 4: Embedding Process	18
Figure 5: Retrieving Process	19
Figure 6: Embedding technique for 8 direction pixel position	25
Figure 7: Retrieving technique for 8 direction pixel position	26
Figure 8: Cover Images	28

ABSTRACT

To get the mysterious correspondence a strong video steganography calculation is my motive. The significant targets of the model strategy are: Embedding and extracting stego-video using Advanced Encryption Standard (AES) and Least Significant Bit (LSB) approach with a more secure pixel selection methodology known as the Sobel edge detection pixel selection technique. And use Fisher-Yates Shuffle algorithm for frame shuffling. Proposed method use to improve robustness of the Cover video against visual attack. The productivity of the proposed model is assessed with regards to the perceptual robustness and visual quality. From exploratory outcome, it is seen that the proposed model beats contemporary techniques by accomplishing critical result.

Key-Words: Video Steganography, LSB, AES, Sobel Edge Detection.

CHAPTER**INTRODUCTION****Background**

In the contemporary era marked by rapid technological advancements and the prevalent use of cloud databases managed by trusted third parties, ensuring the security of confidential data has become paramount [1]. A potential resolution to this challenge involves adopting a two-tiered approach to data protection, combining cryptography with steganography. The term "steganography" originates from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing," collectively forming "covered writing." Steganography, an age-old technique, encompasses both data concealment and extraction processes. The embedding system is a crucial component of steganography, representing one of its fundamental elements. This covert form of communication has been utilized for centuries, highlighting its enduring significance in safeguarding information.

The term "cryptography" found its origin in a book on steganography and cryptography authored by the German cryptographer Johannes Trithemius in 1499, wherein he assumed the guise of a magician [2]. Video steganography, a specific form of data hiding, involves concealing communications within cover material. This method finds applications in diverse fields such as access control, medical systems, law enforcement, and copyright protection [3]. Video steganography serves as a technique to embed data discreetly within videos, leveraging the limited sensitivity of the human visual system to subtle changes in digital media, particularly in digital video transmissions. Video steganography, a method employed to conceal data within videos, capitalizes on the inherent limitations of the human visual

system, which is relatively insensitive to subtle alterations in digital media, particularly in the context of digital video transmissions. Moreover, two key factors contribute to the increasing popularity of video steganography. Primarily, the escalation of information security concerns aligns with the rapid proliferation of computer applications. Video, as a microelectronic medium, possesses distinct advantages, making it more suitable than other hypermedia. Its compact size, coupled with potent transmission capabilities, renders it an optimal choice for concealing digital video contents. A steganographic technique typically comprises three fundamental components: the secret data, the cover file (prior to the integration of the secret data), and the stego-file (the cover file post the concealment of secret data). The primary objectives of an effective steganographic system revolve around preserving and enhancing three essential characteristics: payload capacity, imperceptibility, and robustness. Steganography finds application in two distinct domains: the spatial and frequency domains [4]. Spatial domain techniques involve manipulating the pixels of the cover file to embed secret data, while frequency domain techniques utilize the frequencies of the cover file for concealing the secret data. However, relying solely on steganographic techniques for security is not foolproof, as it hinges on anonymity. An individual with access to the stego file and knowledge of the process might successfully extract confidential information. To mitigate this risk, we propose the integration of robust encryption and steganographic technologies into an automated system. This approach aims to provide dual-layered security for user-supplied secret data post an automated process. The Advanced Encryption Standard (AES) method, employing 128 bits for enhanced security and performance, is utilized to encrypt the secret data [5]. Employing binary coding to hide secret bits in the LSB of select RGB cover picture frame pixels. The advantage of LSB lies in its ability to store more information in a cover file while minimizing the risk of

deterioration to the original cover file [12]. Inserting message bits directly into the LSB position of the cover file not only simplifies the process but also yields higher-quality stego files when employing the LSB technique. Additionally, the method of pixel selection is gaining significance, given that hackers have become familiar with common steganographic techniques, making techniques like zig-zag, edges-based, and corner-based pixel selection too recognizable. To address this, our proposed model utilizes Prewitt pixel selection techniques, considered more secure than traditional approaches [13].

The overarching objective of integrating reliable encryption and steganographic technology into an automated system is to conceal secret communications efficiently and error-free. This integration aims to enhance resilience, imperceptibility, and payload capacity while maintaining high video quality.

1.1 Motivation of the Research

Originates from the problems with data security and authentication in online service delivery, as well as the changing terrain of edge industrial activity. Businesses now face greater risks of unwanted access and interference as a result of the transition from traditional software organization to internet hosting, especially when it comes to user interaction with online platforms. The knowledge that conventional word-based identification methods, although useful in identifying people connected to illegal activity, may have drawbacks and be vulnerable to interference tactics serves as additional incentive. This vulnerability raises the possibility of theft, misuse, or loss of confidential data. Designing a more resilient security solution that tackles these issues and offers improved protection for sensitive data is therefore clearly needed. The reason centers on image steganography, which shows up as a workable way to improve security. The method entails concealing data inside pictures, and because of its intricacy, it is difficult for unauthorized parties to find or access concealed data. The research endeavors to reduce the vulnerability gap and provide a more robust method of protecting sensitive data in the ever-changing realm of online industrial operations by implementing image steganography.

1.2**Problem****Statement**

The study focuses on a significant issue with the way that both encryption and steganography are currently used in identity verification systems. The vulnerabilities associated with the conventional steganography pixel selection techniques, which are known for their ease of use and detection susceptibility, are the main points of emphasis. Furthermore, cryptographic techniques that use hash functions like MD5, SHA-0, BASE64, or SHA-1 are identified as having exploitable flaws that allow rainbow table attacks to take advantage of them. The main problem highlights the vital need for increased statistical resilience in video steganography. By combining cutting-edge methods like LSB, 3-XOR, and Prewitt Pixel Selection, the research attempts to address these issues by presenting a novel two-level safe data hiding strategy that improves security and resilience in identity verification procedures in online industrial settings.

1.3 Research Questions

1. Is the proposed advanced data hiding model effective against visual attacks?
2. How does the proposed authentication approach, integrating LSB, 3-XOR, and Pixel Selection, perform in terms of preventing unauthorized access and ensuring secure identity verification?

1.4 Research Objectives

1. To successfully implement this methodology.
2. To evaluate and contrast the approach model's output with that of the most recent model currently in use.

1.5 Research Scope

Online services necessitate secure user identification and authentication, yet they face challenges from cyber-attacks and evolving hacking techniques. Visual attacks, including

Histogram analysis, pixel value analysis, and frequency analysis, pose threats to data security. It is imperative to counteract these risks and establish resilient authentication systems to ensure the security of online services.

1.6 Thesis Organization

The analysis in this publication employs the IEEE representation system and is organized into five chapters.

Chapter 1 encompasses the context of the investigation, the provocation, the problem statement, and the research objectives.

In Chapter 2, the focus is on identifying the exploration gap and establishing relevance.

Chapter 3 delves into the exploratory strategies and techniques that will be employed throughout the research.

The comparison of experiment results with current approaches is presented in Chapter 4.

Lastly, Chapter 5 discusses the findings of the exploration, outlines any limitations, and proposes the future direction of the investigation.

CHAPTER 2

LITERATURE REVIEW

This section comprises papers addressing various aspects of steganography, including video steganography, random video frame selection, pixel selection techniques, and XOR with LSB approaches. Many of these studies focus on the LSB approach, a widely used technique in steganographic technology [11]. In the context of geographical domains, these

investigations leverage the least significant bit (LSB) approach.[14], Karthikeyan B, et al. (2020) presented a technique that uses only common LSBs and random frame selection to conceal secret data, like one-time passwords (OTPs), in carrier video files. The first frame contains metadata, like frame number and length, that appears to be the secret information. Then, another picture with no pixel selection methods and no security talk conceals the sensitive data and achieves a great peak signal noise ratio (PSNR).As a consequence, a simplistic random frame selection algorithm lacks robust information security, and relying solely on LSB represents a basic pixel selection strategy. MB Tuieb et al. (2020) [15] observed that while their proposed model exhibited superior quality performance in both carrier and stego files, it relied on only one layer of protection, rendering it less secure compared to other models examined. The objective of this work is to enhance data security in video steganography through the use of basic LSB and recurrent random frame selection. In another study, Patil A et al. (2018) [16] developed a technique to securely transfer confidential data by employing the AES and LSB algorithms.Before integrating the encrypted ciphertext into each segmentation using the LSB approach and the 1-1-1 strategy to frame the cover video, the plaintext undergoes sequential encryption using AES. However, the details of the frame selection mechanism and the features of the employed observation technique were not adequately explained. While the quality measurement metrics may show excellent results, the application of suitable frame and pixel selection methods can further enhance security.A method for ensuring data security through video steganography was proposed by Manohar N. and Kumar PV (2020) in [17], utilizing the AVI format as the cover video [28]. While the model achieves a good peak signal-to-noise ratio and employs a secure base LSB approach, neural network, and fuzzy logic, it has several flaws that hinder it from providing enhanced security. These drawbacks include pixel and frame selection errors and unclearly presented video and frame format information. Additionally, Singh N (2019) in [18] presents two convergent approaches to text obfuscation using two distinct techniques—"XOR of information with LSBs" and "XOR of messages with symmetric keys."In terms of measurement metrics, the first approach, named "XOR with LSB," closely resembles the original cover carrier in structure; however, "XOR of text with symmetric cryptography" provides more robust data encryption security. The primary drawback of the present approach is its use of progressive data concealment for each frame. Ajmera A, et al. (2019) suggested a method [19] that mitigates errors in spatial domain processes susceptible to different attacks by utilizing steganography in the transformation domain. The main flaw in the model is that DCT and DST approaches yield lower PSNR values than LSB techniques, as demonstrated by Brindha NV and Meenakshi VS (2018) [20]. Moreover, they neglected to explicitly mention the crucial steganography step of choosing frames and pixels. Thus, they used the Scrambling-AES

encryption method and applied DCT and DST techniques to the cover video, yielding a respectable outcome.

A methodology for concealing sensitive information in audio cover carriers and improving security was presented by Hashim J et al. (2018) [21], using LSB and AES-256 algorithms for bit insertion at random locations. One potential drawback of this design is that AES-256 Bytes takes longer than AES-128 to encrypt confidential data, even if the AES method is impenetrable with the shortest key size of 128 bits [22]. Their model's security can be strengthened by encrypting confidential data first with a powerful method like AES. To address these flaws and inaccuracies, we employed the 1-bit least significant bit (LSB) methodology, a spatial domain method for embedding secret data. We used the Advanced Encryption Standard (AES) encryption technology with a randomly generated 128-bit secret key before embedding the secret data into the cover carrier. The XOR method with LSB was employed during embedding to achieve improved performance in random permutation. Additionally, we used a random approach for frame selection based on the "Fisher Yates" principle. Choosing the more appropriate AVI video format for cover carriers and employing BMP images for video frames ensured security. We also used metrics such as mean square error (MSE), root mean square error (RMSE), peak signal-to-noise ratio (PSNR), mean

absolute error (MAE), signal-to-noise ratio (SNR), and embedding time for quality assessment, providing a more effective method than previous models.

CHAPTER 3

RESEARCH METHODOLOGY

The security of the system is enhanced through the implementation of an encryption system that incorporates randomized frame selection based on the "Fisher-Yates" concept. However, it is imperative to address potential vulnerabilities posed by statistical attacks, where adversaries may utilize methods such as histogram analysis, pixel value analysis, and frequency analysis to identify patterns or anomalies introduced during the steganographic process. Consequently, the subsequent sections will provide a comprehensive examination of the encryption system, the randomized frame selection process, and the steganography implementation, emphasizing strategies to mitigate the associated risks attacks. More detail in the subsections:

3.1 Encrypting the Secret Message

The user has to send the secret data (which is automatically encoded once it is received) using our recommended tool. It is secured with the popular and secure symmetric encryption method AES [29]. AES uses symmetric keys with progressively larger bits—128, 192, or 256—to encode data blocks. It also uses the same encryption key to decrypt sensitive information. However, in this investigation, the secret data was encrypted using a 128-bit key length, which yields better results quickly and requires less RAM [5]. While a 128-bit key size is currently unbreakable [22], it is generated automatically by a computer program. Consequently, 128-bit AES was employed to guarantee data security regardless of Shown in "Figure 1," the key is 128 bits long, with 10 cycles in each repeating cycle. SubBytes, MixColumns, MixColumns, and AddRoundKey are the four stages that are carried out in

Each round [30]. In the Sub-Bytes step, every byte is subjected to a different algorithm, producing a new value. The S-box table is then used to change this value according to its hexadecimal code. Every row in the cipher's 128-bit internal state moves during the AES Shift-Rows stage, which makes Shift-Rows operation an essential module for AES circulation. Because of its branch number, the AES is resistant to disparity and linear cryptanalysis, guaranteeing that there are at least 25 active S-Boxes in every four rounds of AES. Then message is encrypted, the cover video carrier is extracted into frames that are formatted as BMP images using a video divider function that is integrated into C#.

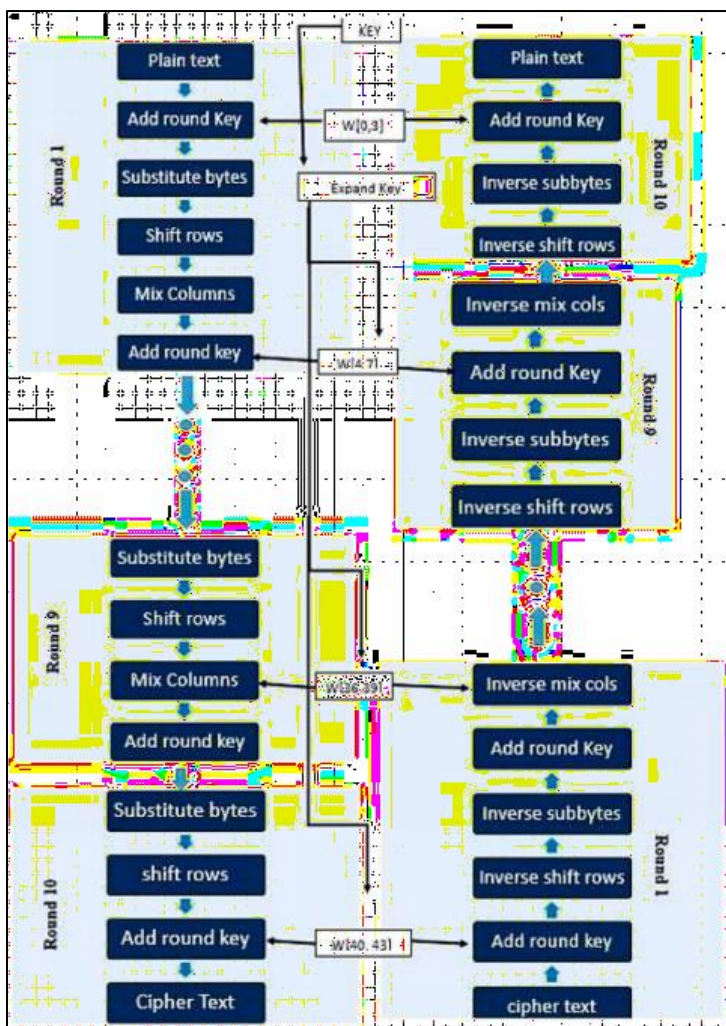


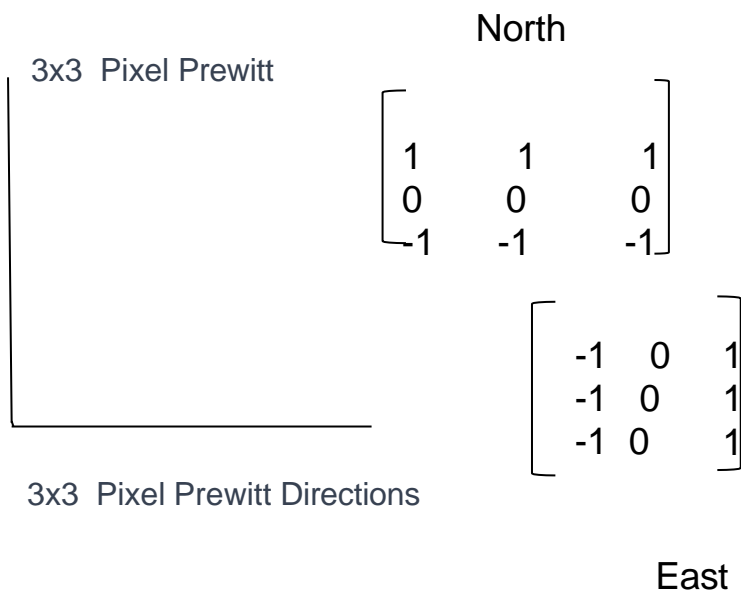
Figure 1 : AES (Encryption and Decryption Process)

3.2 Prewitt Pixel Filtering Algorithm

Pixel filtering is a versatile and user-selected method employed in image processing to achieve specific effects or extract desired features. One prominent technique within pixel filtering is the use of the Prewitt operator, a widely adopted method for edge detection. The Prewitt operator calculates the gradient of image intensity, emphasizing rapid changes in intensity that correspond to edges or boundaries. Additionally, for edge identification, dynamic algorithms like the Canny edge detection algorithm can be employed as part of the pixel filtering process. This allows users to tailor the filtering approach based on the specific requirements of image analysis or feature extraction.

In the process, both gradient magnitude and gradient direction are crucial components. The FXr function is employed for red value retrieval, while the FXB function is utilized for binary conversion. These functions play integral roles in the calculation and transformation steps of the process, contributing to the overall effectiveness of the image processing technique.

The 3x3 Prewitt operator is widely employed for edge detection in image processing applications.



3.2 Randomization Frame Selection Method

The selected frames in BMP format are determined through a random sampling mechanism following Fisher-Yates principles. The quantity of frames (N_f) needed for embedding is calculated based on the length of the secret encrypted message ($S_m L$) and the dimensions (D_v) of the cover video, as computed using equations 1 and 2.

Additionally taken into account is the Complete Direction (CD), which is equal to eight directions. The total amount of pixels that can be inserted in a single frame is the product of $MaxD_v$ and 4 CD. A single pixel's 3-bit embedding capacity is also shown by the 3-bit value. Figure 3 presents a permutation based on the input key and the number of frames, illuminating the fundamental framework. Frames are produced by the permutation, and the procedure uses the first $(N_f + 1) > 1$ frame. Notably, systematic collecting allows for reverse shuffling with the same key, which facilitates data extraction from frames. The shuffle key and the length of the secret data are stored in the first frame together with metadata, and the actual encrypted messages are gradually embedded in the following frames.

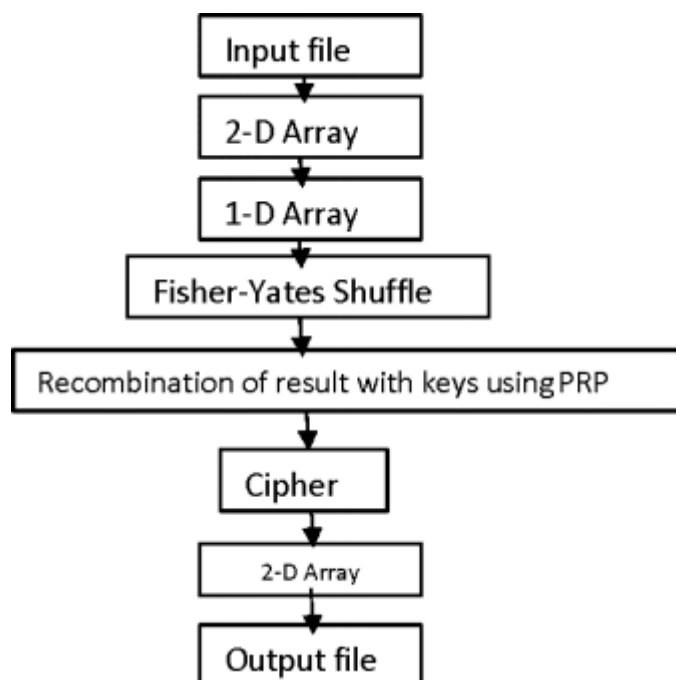


Figure 3.2 : Frame Selection Based on Fisher-Yates

3.4 Steganographic Process

The process involves two main phases: retrieval and embedding, as illustrated in Figure 4. Subsequently, images are extracted from the cover carrier, and the pixel selection system processes these images, selecting less than 1% of the pixels in a frame. In the third phase, a triple XOR operation decodes the secret message into 8-bit binary data, which is embedded within the filtered pixels at the 1-bit LSB location. To bolster security, it is crucial to address potential vulnerabilities posed by statistical attacks, such as histogram analysis, pixel value analysis, and frequency analysis, which adversaries may employ to detect patterns or anomalies in the steganographic process.

1st-pixel	position	$(X_1, Y_1) = (H - \frac{1}{2} - 3, 1)$1
2nd-pixel	position	$(X_2, Y_2) = (H, W - \frac{1}{2} - 3)$2
3rd-pixel	position	$(X_3, Y_3) = (H - \frac{1}{2} + 3, W)$3
4th-pixel	position	$(X_4, Y_4) = (1, H - \frac{1}{2} + 3)$4

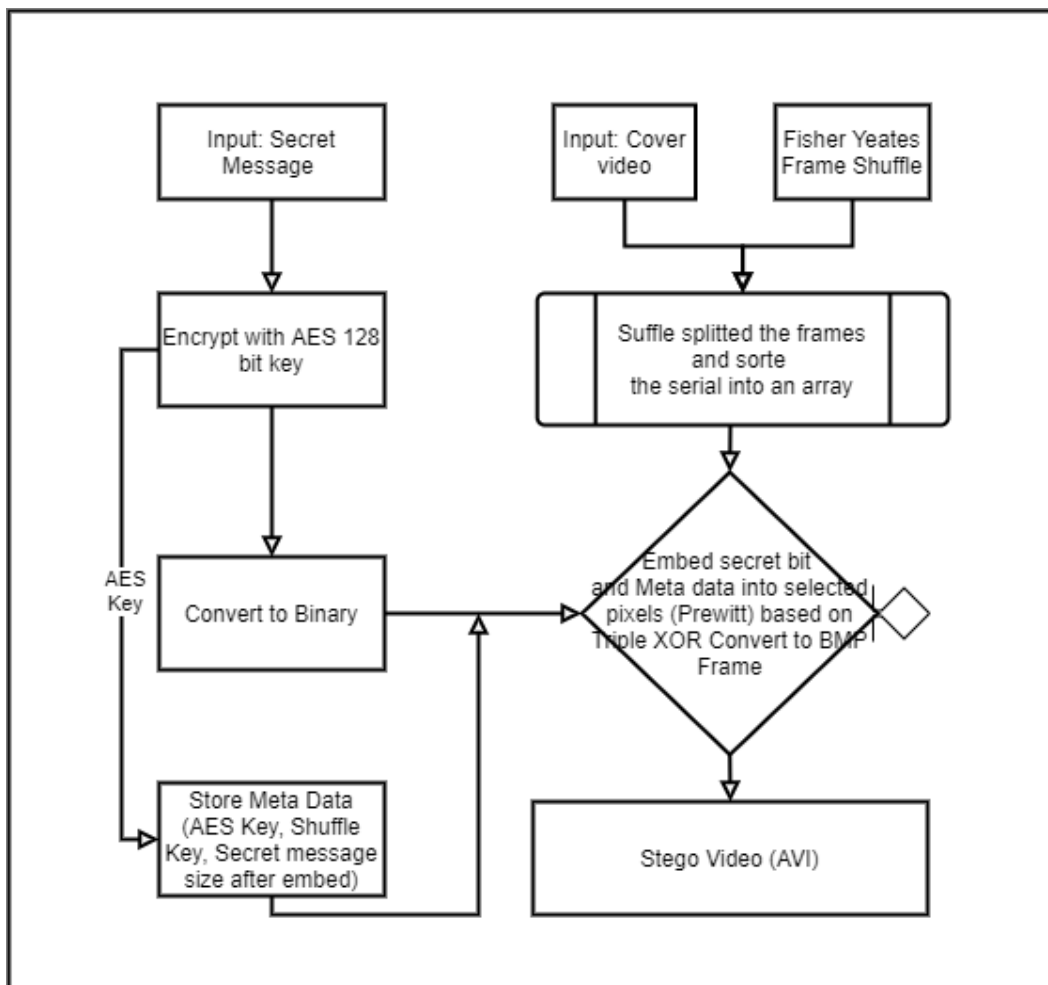


Figure3.3: Embedding Process

The retrieval process is depicted in Figure 5. To successfully extract secret data, the initial step involves understanding the metadata. The fixed four pixels are then saved using the specified equation, enabling the extraction of the embedded secret data.

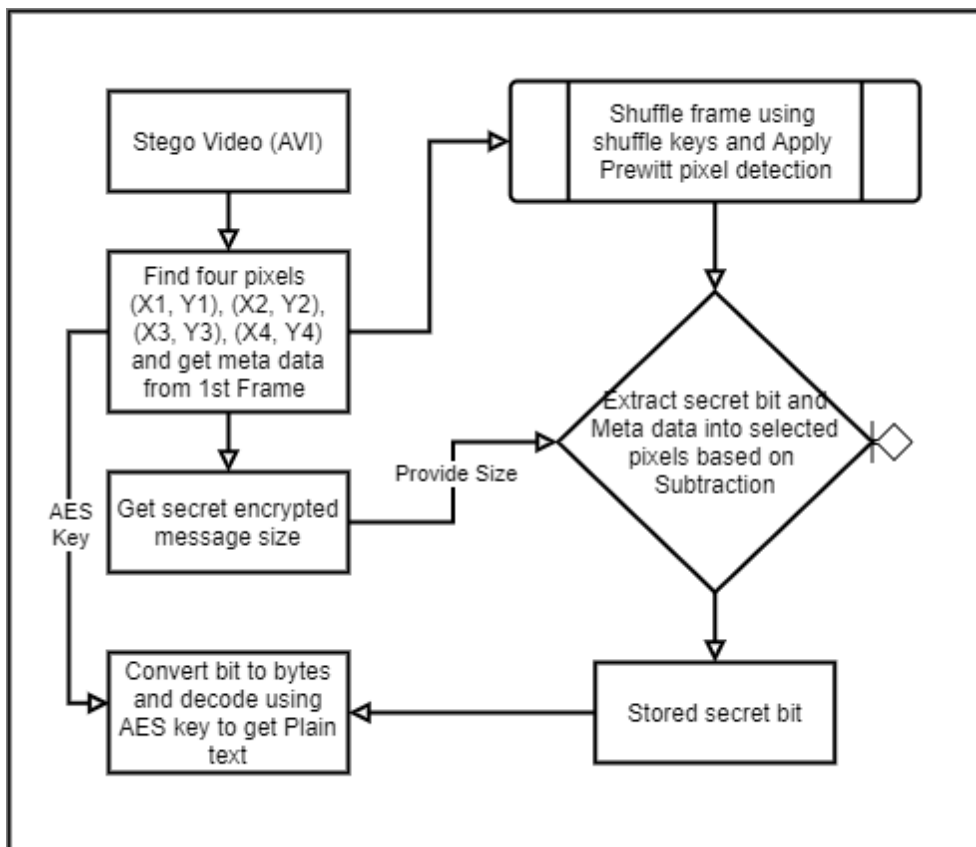


Figure 3.4 : Retrieving Process

3.5 Algorithm for embedding and retrieving

Embedding and retrieving algorithms are vital components for safeguarding and concealing data through frame selection and encryption. Users provide the cover video and secret message, initiating encryption with the AES function and a 128-bit key. Simultaneously, frames are extracted into BMP formats, and the FisherYeatsShuffle function generates a permutation (FLp[]) for selecting a specific frame (SF). The remaining frames employ a triple XOR strategy to embed the remaining secret data, while the first frame uses an XOR approach to embed additional metadata (MD) into Prewitt-based pixel selection.

In the retrieval algorithm, the user submits a stego video, which is then extracted into BMP formats. The model selects the required frames based on the total message bit length after obtaining a random permutation using the shuffle key.

To safeguard against attacks, the algorithm employs robust encryption, meticulous frame selection, and effective counseling techniques, thwarting adversaries attempting statistical assaults such as frequency analysis, pixel value analysis, and histogram analysis. These measures ensure the protection of private data and prevent unauthorized access in the dynamic landscape of internet-based business operations.

Embedding Algorithm:

Result: Stego Video

$S_m \leftarrow \text{input}$

$C_v \leftarrow \text{input}$

$C_t = 128\text{-bit AES}(S_m, \text{key});$

$FE [] = \text{Extract_Frames}(C_v);$

$v = 0;$

 If $MEMB < SMB$

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

 else

$W = \text{Frame Width};$

$H = \text{Frame Height};$

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

$\text{embed}((C_x, C_y));$


```

BL= Length of M;

Ppn= Prewitt Edge Detection(I);

SMBL←length (SMB)

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

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

```
TotalSecretMessageLength = MD.MLength
```

```
FLp[] = FisherYeatsShuffle (FE[], ShuffleKey);
```

```
v = 0;
```

```
For □ Sf[1 to N-1]
```

```
If MEMB<TotalSecretMessageLength
```

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

$S_D[] = \text{retrieveSecretDataTripleXOR}(S_F[v], S_{MBL})$

else

W = Frame Width;

H = Frame Height;

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

retrieve $((C_x, C_y));$

BL = Length of M;

$P_{pn} = \text{Prewitt Edge Detection}(I)$

$S_{MBL} \square (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$

a = 0;

while a $\leq P_{pn}$ **do**

$D_s = (C_{x \pm a}, C_{y \pm a})$

$S_D[] = \text{retrieveTripleXOR}(D_s, S_{MBL});$

a++;

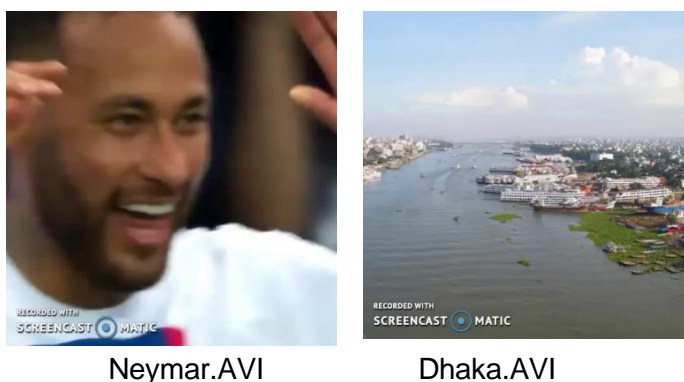
secretData.Add (S_D)

CHAPTER 4

RESULTS AND ANALYSIS DISCUSSION

4.1 Result And Analysis Discussion

This section provides a comparative analysis and visual representation of the results between the stego video frames and the cover. Further substantiation of the proposed method's effectiveness is derived from the comparison with outcomes from other established steganographic techniques [9,10]. The statistical evaluation in the research encompasses six quality assessment metrics: Mean Absolute Error (MAE), Root Mean Square Error (RMSE), Mean-Square Error, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Signal-to-Noise Ratio (SNR). The experimental test utilizes two selected movies, Neymar and Dhaka, as depicted in Figure 6. These videos are in the 512 x 512 AVI format, sharing the same frame rate of 25 frames per second and having a duration of 5 seconds each. The proposed solution involves concealing extensive text within a video clip.



Neymar.AVI

Dhaka.AVI

Figure 3.5 : Cover Videos

Eqs. 5 to 10 provide a scientific explanation of the six necessary frame quality assessment

matrices: PSNR, SSIM, MAE, SNR, RMSE, and MSE. These matrices are used to evaluate the efficacy and security of the steganographic process.

The Mathematical explanation for PSNR is [28]

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \dots\dots\dots 5$$

In this context, the PSNR is reliant on the Mean Squared Error (MSE) and is expressed in decibels (dB). Numerous studies indicate that the concealment method is deemed acceptable when the PSNR between the stego frame and cover exceeds 40 dB. SSIM The Scientific definition is[29]

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1) + (2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \dots\dots\dots 6$$

In this context, the variables x and y represent the dimensions of the image. The denominator uses the averages of x and y, denoted by (x + y)/2. The constants K1 and K2 typically have default values of 0.01 and 0.03, respectively. Additionally, L signifies the dynamic range of pixel values. For simplification, two variable quantities are introduced: C1 = (K1 * L)^2 and C2 = (K2 * L)^2. These variables contribute to the structural similarity calculation in the SSIM formula.

MAE The Mathematical explanation is[30]

$$MAE = \frac{1}{3MN} \sum_{i=1}^M \sum_{j=1}^N [C(x, y) - S(x, y)]_1 \dots\dots\dots 7$$

In this instance, the terms "pixel position" and "picture dimension" represented by M and N correspond to the coordinates (x, y). These elements are integral to the evaluation of the structural similarity index (SSIM). SNR The Mathematical elucidation is [31]

$$SNR = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \hat{f}(x, y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x, y) - \hat{f}(x, y)]^2} \dots\dots\dots 8$$

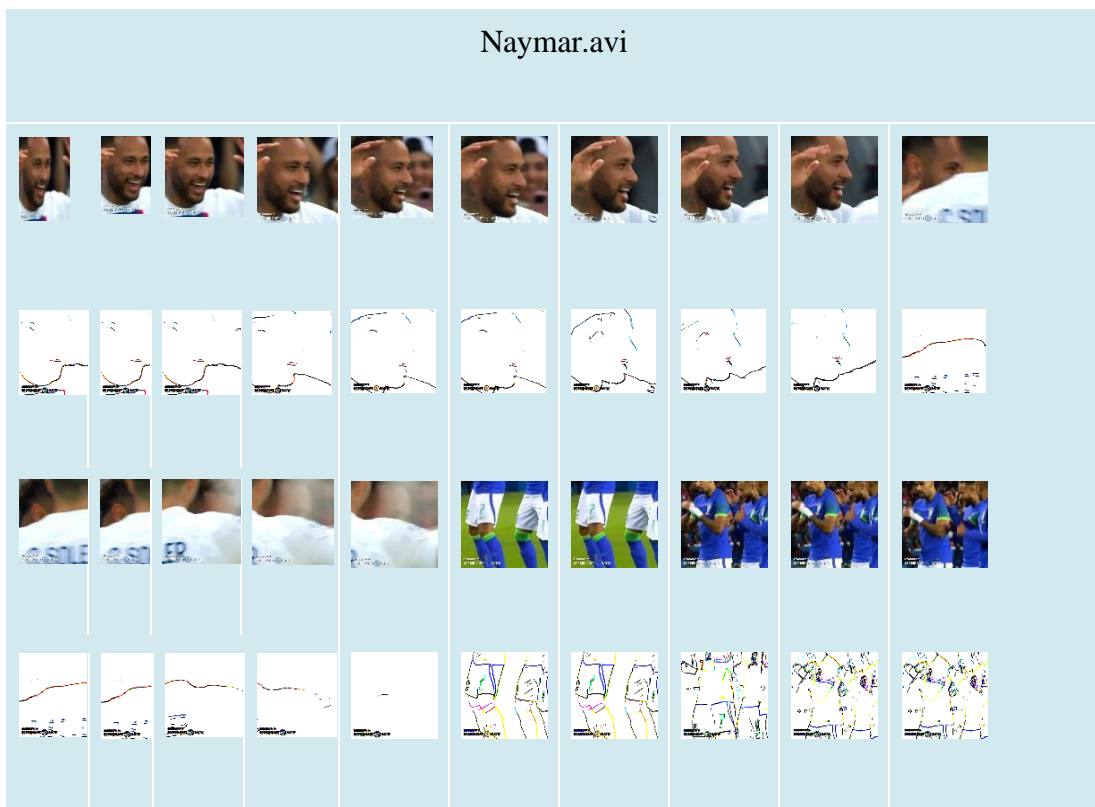
In this case, the pixel position and the picture dimension denoted by M&N pertain to (x, y).

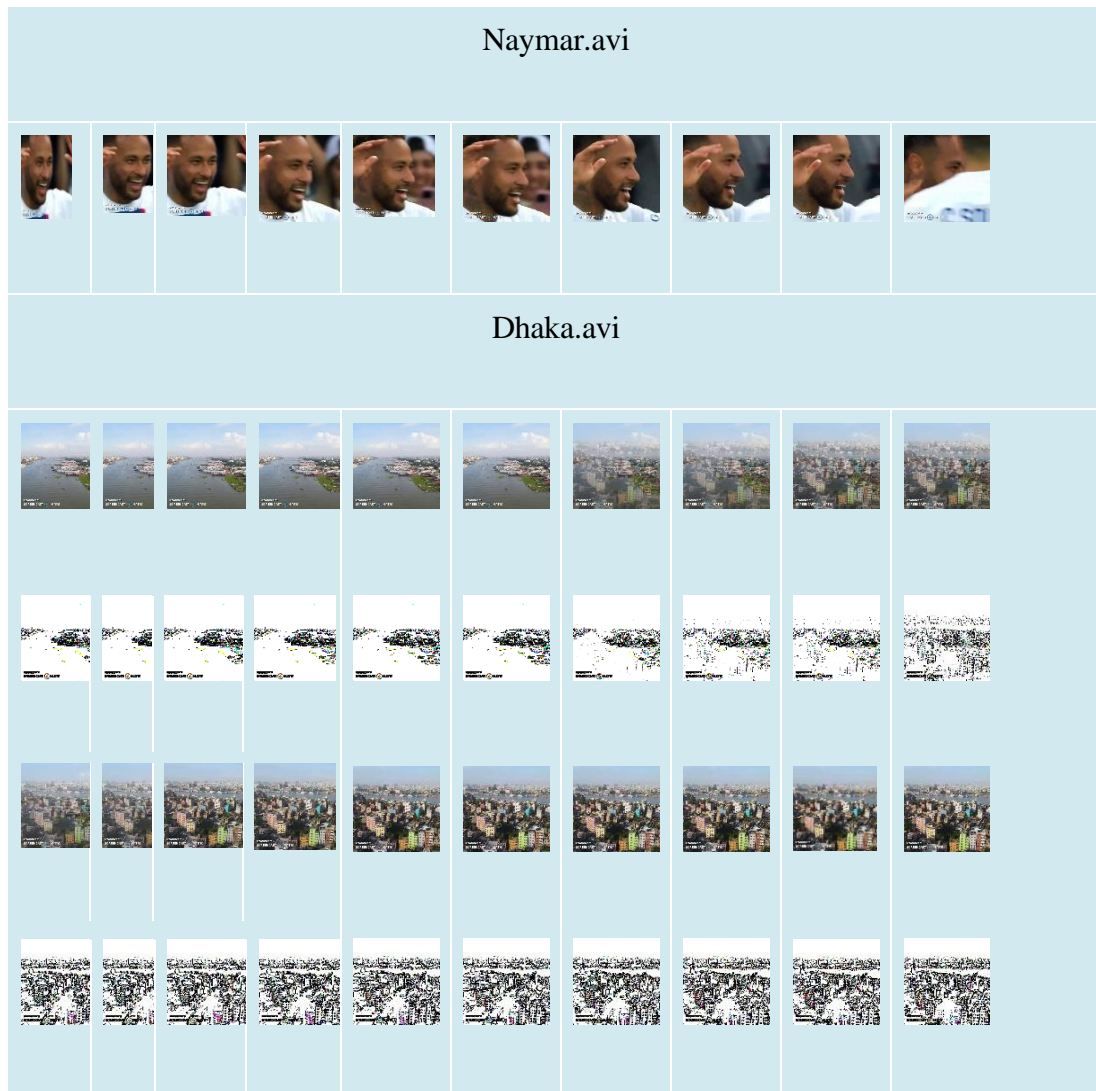
The squared root base of the mean MSE, or RMSE, as defined by science

$$RMSE = \sqrt{MSE} \dots\dots\dots 9$$

MSE The Scientific definition is[32]

$$MSE = (1xMxN) \sum_{i=1}^M \sum_{j=1}^N (a_{ij} - b_{ij})^2 \dots\dots\dots 10$$





The suggested method's results are constrained to a payload of 15 kilobites on four chosen video frames.

Table 1. PSNR values

Frame No	Neymar.AVI(PSNR)	Dhaka.AVI(PSNR)
01 (S_{MB})	89.23	88.64
02S_(MB)	72.74	72.55
03(S_{MB})	72.45	72.35

04 (S_{MB})	72.77	72.98
05(S_{MB})	72.78	72.98
06(S_{MB})	72.45	72.65
07(S_{MB})	72.78	72.32
08(S_{MB})	72.76	72.86
09(S_{MB})	72.78	72.21
10(S_{MB})	72.63	72.87
11(S_{MB})	72.78	72.45
12(S_{MB})	72.78	72.43
13(S_{MB})	72.74	72.43
14(S_{MB})	72.78	72.12
15(S_{MB})	72.53	72.23
16(S_{MB})	72.66	72.53
17(S_{MB})	72.45	72.97
18(S_{MB})	72.47	72.42
19(S_{MB})	72.63	72.13
20(S_{MB})	75.94	72.34

21(SMB)	75.94	75.89
----------------	--------------	--------------

For Neymar and Dhaka videos, frames of size 512 x 512 were utilized, and the payload for concealing data was 15 Kilobytes (15000 bytes). The system employed 21 frames for embedding all secret data, with each frame gradually concealing more than 700 bytes. In the case of Neymar's frames, the PSNR values were slightly higher compared to other selected video frames.

Table 2. Using various standard sized payloads, the proposed method's quality measurement metrics

Frame	Dimension	Payload	PSNR	SSIM	MAE	SNR	RMSE	MSE	TCEP
NA	512X512	512 Bytes	74.015 45	0.9999 92913	0.0026	68.641 512	0.0509	0.0026	9.47s
NA	512X512	256 Bytes	77.542 112	0.9999 97723	0.0012	71.654 5221	0.0352	0.0012	7.45s
NA	512X512	128 Bytes	80.543 513242 1	0.9999 99726	0.0006	74.845 34	0.0248	0.0006	5.52s
DA	512X512	512 Bytes	74.215 454	0.9999 95854	0.0026	68.321 31	0.0509	0.0026	10.23s

DA	512X5	256	77.453	0.9999	0.0012	70.945	0.0351	0.0012	8.93s
	12	Bytes	41112	99646		335			
DA	512X5	128	80.564	0.9999	0.0006	74.537	0.0249	0.0006	5.45s
	12	Bytes	5341	99867		865435			

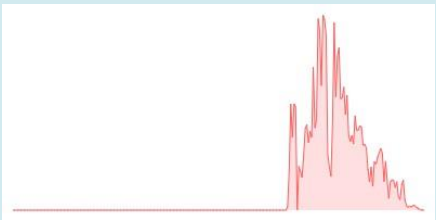
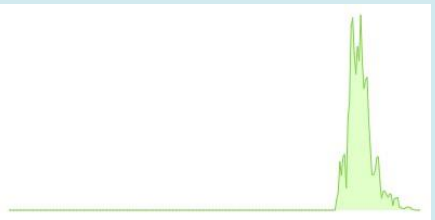

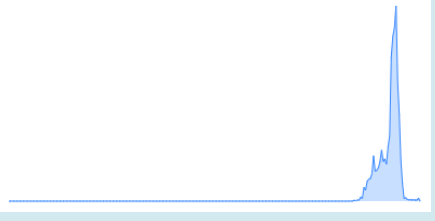
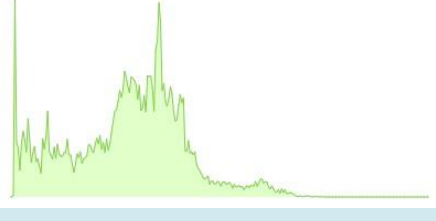
In this table, 512 x 512 video frames with varying payload sizes of 512 bytes, 256 bytes, and 128 bytes, respectively are used in this table to illustrate where we obtain higher PSNR values for Neymar's video. Table 3 provides the results of a comparison between two existing steganographic methods using 512 X 512 sized frames and 512 Bytes of payload [12, 13].

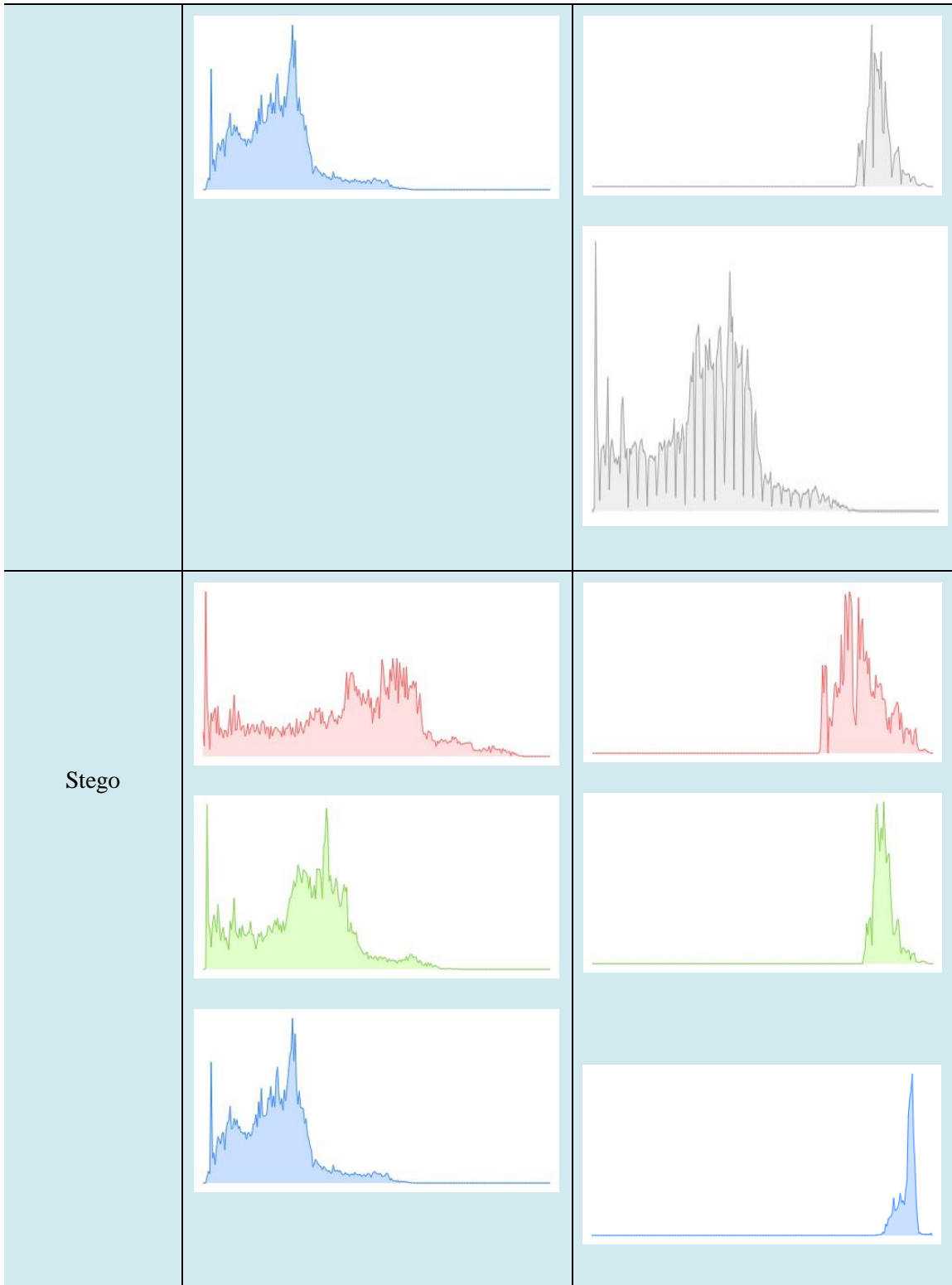
Table 3. Comparison of the two 2 recent steganographic security techniques.

Techniques	Frame	PSNR	SSIM	MAE	RMSE	SNR	MSE	TCEP
Model 1	DV	70.74	0.999984985	0.0029	0.0539	65.4785	0.0029	8.4545s
Model 2	DV	73.13	0.99991956	0.0027	0.0520	68.8686	0.0027	5.9646s
P- Model	DV	74.52	0.999992913	0.0026	0.0509	69.5991	0.0026	9.4754s
Model 1	SM	71.09	0.999989566	0.0029	0.0539	66.1299	0.0029	8.2331s
Model 2	SM	73.87	0.999991023	0.0027	0.0508	68.2094	0.0027	5.5413s
P- Model	SM	74.53	0.999995854	0.0026	0.0509	69.3356	0.0026	10.231s

The Proposed Model (P-Model) demonstrates superior performance compared to Models 1

and 2, with PSNR values of 74.534131 and 74.5242 for the Neymar (NA) frame, respectively, as indicated in the first column of Table 3. Across all columns, our suggested model consistently outperforms the existing models, even though it incurs a slightly longer time to complete the embedding process (TCEP). This trade-off between security and embedding time underscores the enhanced security features against statistical attacks of our proposed approach.

Frames Type	NA	DA
Cover		
		
		



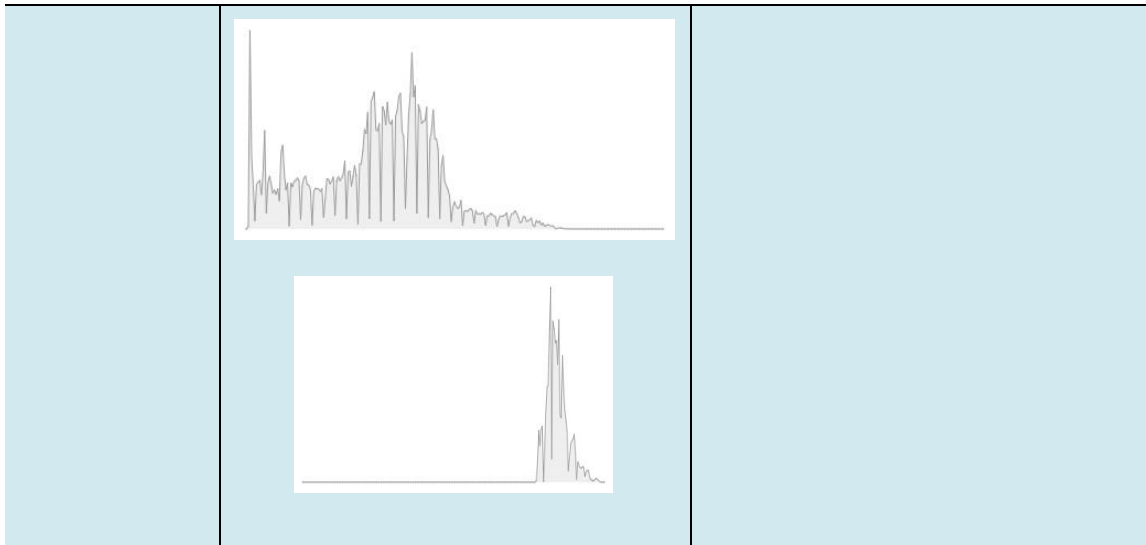


Table 4. Comparative cover and stego frame histogram

The histogram analysis reveals minimal differences between the cover and stego frames, indicating that the changes introduced by the data hiding technique are subtle and unpredictable.

The experiment employing the proposed procedure demonstrates superior performance compared to similar algorithms.

As depicted in the screenshot, our suggested system is currently in beta testing and undergoing further development to incorporate additional features.

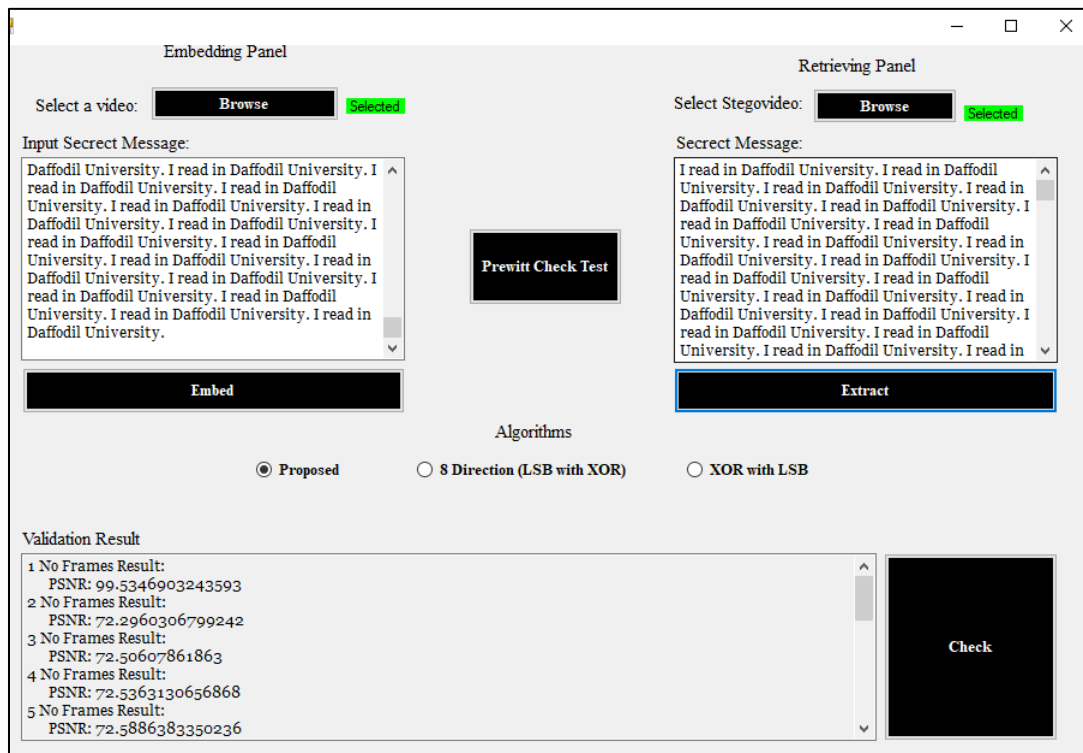


Figure 7 : Screenshot of proposed system

CHAPTER 5

RECOMMENDATIONS AND CONCLUSIONS

This approach ensures robust security against statistical attacks through an automated two-level secure data hiding mechanism in video steganography. The method conceals secret information within cover videos using robust 128-bit AES encryption. Furthermore, this model has the capability to conceal up to 100 KB of secret data in a 512 by 512 cover video playing at 25 frames per second for 5 seconds. It's worth noting that these limitations are expected to be addressed in future work.

REFERENCES

- [1] zhou, h, zhang, w, chen, k, li, yu, n, three, dimensional, mesh, steganography, steganalysis, review, iee, transactions, visualization, computer, graphics, 2021, apr, 22
- [2] nyo, oo, secure, data, transmission, video, steganography, using, arnold, scrambling, dwt, international, journal, computer, network, information, security, 2019, 1, 11, 6
- [3] alam, st, jahan, n, hassan, mm, new, 8, directional, pixel, selection, technique, lsb, based, image, steganography, international, conference, cybersecurity, computer, science, 2020, 15, pp, 101, 115
- [4] narula, m, gupta, garg, implementation, hybrid, technique, spatial, frequency, domain, steganography, along, cryptography, withstand, statistical, attacks, 2020, 2nd, international, conference, advances, computing
- [5] harba, secure, data, encryption, through, combination, aes, rsa, hmac, engineering, technology, applied, science, research, 2017, 7, 4,);, 1781, 5

- [6] ansari, mohammadi, parvez, comparative, study, recent, steganography, techniques, multiple, image, formats, international, journal, computer, network, information, security, 2019, 11, 1,),: 25
- [7] pilania, gupta, analysis, implementation, iwt, svd, scheme, video, steganography, electronics, telecommunication, engineering, 2020, pp, 153, 162
- [8] mstafa, rj, elleithy, km, compressed, raw, video, steganography, techniques, comprehensive, survey, analysis, multimedia, tools, 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, aes, linear, congruential, generator, international, seminar, research, information, technology
- [10] astuti, rachmawanto, eh, sari, ca, simple, secure, image, steganography, using, lsb, triple, xor, operation, msb, international, conference, information, communications, technology, icoiact, 2018, 6
- [11] bhuiyan, t, sarower, karim, r, hassan, m, image, steganography, algorithm, using, lsb, replacement, through, xor, substitution, international, conference, information, communications, technology, icoiact, 2019, 24, pp.
- [12] alam, st, jahan, n, hassan, mm, new, 8, directional, pixel, selection, technique, lsb, based, image, steganography, international, conference, cybersecurity, computer, science, 2020, 15, pp, 101, 115
- [13] karthikeyan, b, raj, yuvaraj, d, sundar, hybrid, approach, video, steganography, stretching, secret, data, communication, computational, technologies, 2020, pp, 1081, 1087
- [14] tuiieb, mb, abdullah, mz, Abdul, razaq, ns, efficiency, secured, reversible, video, steganography, approach, based, lsb, significant, j, cellular, automata, 2020, apr, 16, 17
- [15] patil, keshkamat, sm, desai, vv, arlimatti, t, embedding, advanced, encryption, standards, encoded, data, video, using, least, significant, bit, algorithm, international, conference, recent, innovations, electrical, electronics
- [16] manohar, n, kumar, pv, data, encryption, decryption, using, steganography, 4th, international, conference, intelligent, computing, control, systems, iciccs, 2020, may, 697, 702, ieee
- [17] singh, xor, encryption, techniques, video, steganography, analysis, international, conference, intelligent, systems, design, applications, 2018, 6, pp

[18] ajmera, divecha, m, ghosh, raval, chaturvedi, r, video, steganography, using, scrambling, aes, encryption, dct, dst, 2019, ieee, pune, section, international, conference, punecon

[19] brindha, nv, meenakshi, vs, comparison, analysis, bio, watermarking, using, dwt, dct, lsb, algorithms, computational, vision, inspired, computing, 2018, pp, 849, 863

[20] hashim, hameed, abbas, awais, m, qazi, ha, s, lsb, modification, based, audio, steganography, using, advanced, encryption, standard, aes, 256, technique, 12th, international, conference, mathematics, actuarial, scienc

