

Daffodil International University

Department of Software Engineering

Faculty of Science and Information Technology

Course Code: CS 439



Video Steganography for Authentication: Enhancing Digital Watermark and Verification

Submitted By

Md. Mahfuzur Rahman

ID: 203-35-3137

Department of Software Engineering

Daffodil International University

Supervisor

Md. Maruf Hassan

Associate Professor

Department of Software Engineering

Daffodil International University

July 18, 2024

Video Steganography for Authentication: Enhancing Digital Watermark and Verification



A Thesis submitted to the Department of Software Engineering, Daffodil International University, in partial fulfillment of the requirements for the degree of B.Sc.(Engg.) in Software Engineering.

Submitted By

Md. Mahfuzur Rahman

ID: 203-35-3137

Department of Software Engineering

Daffodil International University

Supervised By

Md. Maruf Hassan

Associate Professor

Department of Software Engineering

Daffodil International University

July 18, 2024

Recommendation of the Thesis Supervisor

To Whom It May Concern

Md. Maruf Hassan

Associate Professor

Department of Software Engineering

Daffodil International University

Date: July 18, 2024

APPROVAL

This thesis titled on “**Video Steganography for Authentication: Enhancing Digital Watermark and Verification**”, submitted by **Md. Mahfuzur Rahman (ID: 203-35-3137)** 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. Imran Mahmud
Associate Professor & Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



Internal Examiner 1

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



Internal Examiner 2

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



External Examiner

Dr. Md. Sazzadur Rahman
Professor
Institute of Information Technology
Jahangirnagar University

Declaration

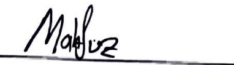
I announce that I am rendering this thesis under Md Maruf Hassan, Associate Professor, Department of Software Engineering, Daffodil International University. I therefore state that this work or any portion of it was not proposed here therefore for bachelor's Degree or any graduation.

Supervised By



Md. Maruf Hassan
Associate Professor
Department of Software Engineering
Daffodil International University

Submitted By



Md. Mahfuzur Rahman
ID: 203-35-3137
Department of Software Engineering
Daffodil International University

Acknowledgement

Firstly, I would like to thank my supervisor Md. Maruf Hassan, Associate Professor, Faculty of Science and Information Technology, Daffodil International University. He shared the principal concept of this study with me and guided me throughout the study. I am really grateful to have worked under his greatly knowledgeable supervision and express my greatest gratitude to him for his guidance.

Also, I would like to thank my parents, friends, and acquaintances. Without their support, it was really not possible for me to continue this journey.

ABSTRACT

The thesis "Video Steganography for Authentication Enhancing Digital Watermark and Verification" elaborates an advanced methodology to enhance the security and authenticity of video content. With an increase in multimedia data exchange, robust security is required in the current digital era to provide protection against unauthorized tampering. Existing techniques of digital watermarking for the security or verification of digital media usually have a trade-off with (the Rivest, Shamir, and Adelman) algorithm encryption with advanced steganographic robustness, imperceptibility, and capacity. An innovative solution through the integration of RSA methodologies, like Least Significant Bit (LSB) replacement and XOR substitution, will be proposed to mitigate this limitation. The proposed model provides the facility to maintain secure and hidden data in video files, where it is safe and remains undetectable for security and verification purposes. The methodology involves the separation of frames from videos, and the frames are passed, utilizing the concept of a cryptographic hash function, to choose determined frames within which an encrypted message will be embedded. This has been implemented using public key cryptography. Public key cryptography using RSA has been implemented to ensure the confidentiality of the message for the intended receiver. The encrypted message is embedded into selected frames using LSB and XOR methodologies along with the message, maintaining the quality of the video. It has been shown in this thesis that these double layers of protection increase security considerably, making the system inhospitable for data extraction by attackers and offering perceptible protection against tampering. Long-reaching implications of the research include significant benefits in the areas of

intellectual property protection, digital forensics, and secure communications. The proposed video steganography model, thus emphasizing two main problems concerning robustness and imperceptibility, is a significant improvement and sets a mature model in the field of digital media security. A comprehensive model meant for the overall improvement of existing watermarking as well as verification processes has been developed.

Keywords: video steganography, digital watermarking, RSA encryption, Least Significant Bit (LSB), XOR substitution, data security, multimedia authentication, cryptographic techniques, covert communication, data integrity

Table of Contents

Chapter I. Introduction	1
1.1 Background	1
1.2 Motivations:	4
1.3 Problem Statement:	5
1.4 Research Questions:	6
1.5 Research Objective:	6
1.6 Research Scope:	6
1.7 Contributions	7
1.8 Thesis Organization	7
Chapter II. Literature Review	9
2.1 Introduction	10
2.2 Literature Reviews	10
Chapter III. Methodologies	25
3.1 Introduction	26
3.3 Method for Randomization Frame Selection:	34
3.4 Method For embedding Bits into Pixel :	36
3.5 Algorithm for embedding and retrieving of proposed Model:	39
3.5.1 Embedding Algorithm for Steganographic Process	40
3.5.2 Retrieving Algorithm for Steganographic Process:	46
Chapter IV. Results and Discussion	48
4.1 The Results of Random Selection for Video Frame	52
4.2 The Result of Embedding Capacity	54
4.3 The Result of PSNR and MSE for Imperceptibility:	57
Chapter V. Conclusion	63
5.1 Introduction	64
5.2 Contribution of the Research:	65
5.3 Future Work:	65
References	67

List of Tables and Figures

Fig 3.1: Embedding and Retrieving Process of Proposed Method	26
Fig 3.2: Rivest, Shamir, Adleman (RSA) Encryption and Decryption.....	27
Fig 3.3: RSA Algorithm execution flow chart	31
Fig 3.4: Frame Selection Process Using Algorithm SHA-256.....	34
Fig 3.5, 3.6: Data Embedding and extraction Procedure into Pixel	38
Fig 3.7: Embedding Process of proposed model	40
Fig 3.8: Flowchart of frame extraction process from video.....	42
Fig 3.9: Flowchart of frame extraction process from video.....	43
Fig 3.10: Flowchart of embedding and video reconstruction.....	44
Fig 3.11: Retrieving Process of proposed model	45
Fig 3.12: Extracting Process of Key frame from video.	46
Table 4.1.1: Selected Video Files Used in The Experiments	51
Table 4.1.2: Selection Step of Avenger.mp4 video Using different Secret Key.....	52
Table 4.1.3: Selection Step of Marbel.mp4 video Using different Secret Key	53
Table 4.2.1: Difference between Cover Frame and Stego Frame in avengers.mp4 video	56
Table 4.2.2: Difference between Cover Frame and Stego Frame in marbel.mp4 video	56
Table 4.3.1: PSNR, MSE and SSIM calculation	57
Fig 4.1: Relation between PSNR value and Video Resolution.....	58
Fig 4.2: Relation between MSE value and video Resolution	59
Fig 4.3: Relation between PSNR value and MSE.....	60

Chapter I. Introduction

1.1 Background

Nowadays, technological advancements are progressing at a pace that beyond our ability to conceive. Contemporary society relies extensively on technology, with data serving as the primary catalyst for technological advancements. Currently, data has become the most precious asset. In the contemporary digital landscape, those that own a greater amount of data are also more affluent than their counterparts. Therefore, it is imperative that we safeguard our data, which is our most precious resource. Alternatively, it has the potential to pose a danger and compromise our security. Information technology security encompasses several disciplines, among which cryptography is included. Cryptography encompasses many distinct categories, including Hashing, Digital signature, and Encryption. These approaches are inadequate to meet the information security needs of the contemporary digital landscape. Due to the vulnerability of the hash function, the digital signature may be tampered with and the encryption can be deciphered. By combining encryption with steganography, we may effectively address this issue. Steganography refers to the act of concealing the presence of a file, video, photograph, or message inside another kind of media as a means of preventing its detection.

The amount of multimedia shared over different digital platforms has been surging in this digital epoch. So, issues with digital media include authenticity of contents, integrity, and security—all in a single packet. Video is becoming mainstream on all social media, video-sharing platforms, and all communication channels. This, in turn, brought in

the need for more robust techniques to ensure that video content remains unaltered and verifiable.

Herodotus described a method where a message was tattooed on a slave's shaved head, letting the hair to grow back before conveying the message to the receiver. This is the oldest known application of steganography, which dates back to ancient Greece about 440 BC. (Khan, 1996)

It has always been an art of hiding information from other non-secret text or data, and steganography is one of the methods in that category. Steganography is the process involved in concealing the message as part of some other form of data in multimedia. It is the mechanism of embedding the message so that it cannot be perceived by any means of computation. Digital protection is what steers people to make the embrace of steganography highly welcomed in ensuring sensitive data. In general, digital watermarking is the process of embedding information in digital media to establish ownership or authenticate content while at the same time protecting the media from unauthorized use. The importance of digital watermarking has lately resulted in most applications being in research and complex challenges that need up-to-date techniques. Conventional techniques used for digital watermarking come with generalized problems related to robustness, imperceptibility, and capacity. A property of robustness for a watermark refers to resisting different manipulations other than the original, be it compression, scaling, or cropping. At the same time, imperceptibility guarantees that the imbedded watermark makes no degradation in the quality of the original media.

Thus, this thesis aims to propose and find new approaches in video steganography that will cope with these concerns: first, towards an increase in security, and second, in the verification process. In simpler terms, capacity is the quantity of information that the algorithm can hide without compromising robustness and imperceptibility.

This paper describes a novel scheme that uses the video steganography technique to improve the watermarking and watermark verification process in the digital domain. The general steps incorporated in the approach, identified to be the concept, include the extraction of frames from the video, the extraction of some particular frames by using a hashed key, encryption of the secret message by using the RSA mode, and finally, embedding using the XOR-based LSB technique. The first step in the adopted methodology is a video to be broken down into frames. After that, each frame is inspected as a contender concerning the hidden message carrier. However, it is ensured that the picking of such frames, while random and safe, is in a way that the cryptographic calculation results in a single key to a distinct SHA-256 ripple algorithm. The resulting hash is then translated into a binary string. Frames having '1s in the binary string are accordingly chosen to hide secret message bits. It's a very secure process since, upon the frame's position, a frame is selected according to the cryptographic hash function.

The covert message is then encrypted using RSA public key cryptographic algorithm technology, the most widely used implementation of public key cryptography. It ensures that only the holder of the corresponding private key, the receiver, can decrypt the message. The size of the encrypted message is usually 836 characters. This is further split into 60 pieces that are then prepackaged to be invisibly embedded into visual media frames. Now, 60 random frames are considered from the selected ones in the previous step. One

piece of the encryption message is inlaid at this step inside one of these frames. This zigzagging in the process brings up the pixel embedding path inside the frame to spread the hidden data across the frame.

The least significant bit substitution technique is more prevalent in steganography systems for its simplicity and efficacy. The data is hidden under pixel RGB levels. The bit message embedding into the LSB pixel value of the cover image goes along with a bitwise XORing operation. The high-level encryption ensures the embedding of a message highly resistant to unauthorized extraction.

This not only provide the security of the hidden message but also guarantees that the hidden data is not perceivable by a human, thus preserving the average quality of the original video. More robust methods in video authentication with the use of more vigorous cryptographic techniques combined with new steganographic methods lead to innovative approaches. In conclusion, the thesis develops an extended all-inclusive framework of video steganography that significantly upgrades the securities and reliabilities of the schemes used in digital watermarking and their verification processes. The methodology put forth has shown excellent coping potential in facing significant challenges of robustness, imperceptibility, and capacity, and this makes it very significant in this field of digital media security.

1.2 Motivations:

In the AI era, digital media is growing at a very high rate, and, at the same time, the reliance on video content is increasing both as a mode of entertainment and as a source of

information. This imposes a heavy toll on the need for secure and authentic multimedia, which goes up with the integrity and authenticity of the video content in the face of growing challenges around digital tampering and piracy. This work thus tries to make video steganography more advanced toward digital watermarking and its verification. It describes a secure model that is being proposed, with the integration of advanced cryptographic techniques based on RSA and innovative steganographic techniques of LSB replacement and XOR substitution. This is because we aim to devise a scheme that, while hiding the unauthorized access, would somehow ensure that any embedded data is not perceived and is intact—it offers many contributions toward a much safer and secure digital media environment.

1.3 Problem Statement:

In the digital age, the security and authenticity of multimedia content have become paramount, particularly with the exponential increase in digital communication and the proliferation of multimedia content sharing over the internet. Video steganography, which involves embedding hidden data within video files, has emerged as a promising solution for ensuring the confidentiality and integrity of information. However, the existing techniques often face significant challenges in maintaining a balance between the imperceptibility of the hidden data and the robustness of the embedding process against attacks or unauthorized access. Moreover, traditional video steganography methods may not adequately address the need for real-time authentication and verification, which are

crucial for applications such as secure communications, digital forensics, and copyright protection.

- **PR1:** Ambiguity arises when multiple user download, modify, and reupload the same content making it hard to identify the original owner.
- **PR2:** Traditional Image selection is more perceptible, limited capacity and easy to stego attack.

1.4 Research Questions:

1. Is it able to identify the original owner of the content?
2. Is the technique for the established security solutions producing better results?

1.5 Research Objective:

RO1: To propose a invisible watermark technique using steganography which preserve the content ownership enhance the robustness. (PR1)

RO2: To propose a video steganography technique for embedding data in a video that is not perceptible due to huge capacity. (PR2)

1.6 Research Scope:

Implementing improved video steganography methods in the future has the potential to revolutionise several areas by greatly improving the security and dependability of digital watermarking and authentication systems. These strategies may be used in domains such

as intellectual property protection to defend multimedia material against unauthorised reproduction and dissemination. Enhanced steganography techniques in the field of digital forensics may be used to verify the integrity and authenticity of video evidence during court procedures. Moreover, these developments might be advantageous for secure communication methods by including confidential data into video broadcasts, hence enhancing security. In general, using strong video steganography methods will enhance the security and reliability of digital environments, promoting increased trust in digital media and communication technologies.

1.7 Contributions

- i. To make a video steganography system that is more secure, encrypt the secret data using the RSA approach.
- ii. By combining the RSA method with a randomization technique that selects N frames according to a secret key, data security would be enhanced.
- iii. The secret message is retrievable, encrypted, and concealed automatically. Additionally, it has automated decryption.

1.8 Thesis Organization

Chapter 1 discusses the context, motivation, problem statement, research question, research purpose, and study scope. Chapter 2 describes the method of defining the exploration gap and relating it to the suggested activities and literature evaluations. Chapter 3 describes the exploitative methods and methodology that will be used throughout the investigations. In

Chapter 4, the experiment finding is built using an existing approach. Chapter 5 discusses the exploration's results, limitations, and future directions.

Chapter II. Literature Review

2.1 Introduction

Video steganography is a highly advanced topic in information security that focuses on concealing data in video footage without detection. It is a significant area of study. In today's digital era, it is necessary to use efficient methods to safeguard critical information sent via videos, given the rapid growth of multimedia data exchange. Video steganography has garnered considerable attention because to its ability to provide covert communication channels while safeguarding the integrity, confidentiality, and authenticity of data against cyber threats and unauthorized access. The purpose of this literature review is to analyze the techniques, algorithms, and uses of embedding and extracting concealed data from video streams, along with the advancements and research conducted in the area of video steganography.

2.2 Literature Reviews

Hummady and Morad (2022) proposed an approach combining Least Significant Bit (LSB) steganography and RSA encryption to enhance system security. Their method leverages the strengths of both steganography and cryptography to protect data embedded in video files. The collaboration between LSB and RSA enhances the system's ability to conceal data while maintaining high security levels. However, the approach has limitations, including increased computational complexity and potential vulnerabilities to advanced steganalysis techniques. The study lacks comprehensive real-world testing and performance evaluations under various attack scenarios. (Hummady & Morad, 2022)

Selim et al. (2021) introduced a video steganography technique that integrates the RSA algorithm with a genetic algorithm (GA) for embedding images in video files. The RSA algorithm provides a secure layer for encrypting the embedded data, while the GA optimizes the embedding process to maintain video quality. The proposed method effectively balances security and imperceptibility. However, the approach may face challenges in processing time due to the computational overhead of the GA and RSA encryption. Additionally, the robustness against various types of attacks needs further validation. (Selim & Shawkat Kamal Guirguis, 2021)

The authors of the study introduce a new technique for incorporating data into video frames by utilizing Least Significant Bit (LSB) replacement and Field-Programmable Gate Array (FPGA) technology. This method provides notable benefits in processing data in real-time and improving security, making it very resistant to common steganalysis approaches. Nevertheless, the intricate nature of FPGA implementation and the significant hardware resources needed may restrict its practical utilization. Future study should prioritize streamlining the implementation and evaluating scalability to provide wider use in different settings. (Abed et al., 2019)

Emad et al. (2018) developed a robust picture steganography technique that relies on the least significant bit and integer wavelet transform to ensure security. The main findings are to the effectiveness and efficiency of the proposed steganography algorithms in hiding sensitive information inside digital images. The proposed steganography algorithm has the capability to effectively hide a confidential text while ensuring a strong level of protection, enhanced concealment, and the capacity to embed a larger secret text with better PSNR and NCC results. (Elshazly, 2018)

Fan et al. (2020) address the challenge of video steganography's vulnerability to the lossy transcoding processes of social networking sites. Their approach selects the luminance component of raw video as the cover medium and employs the QIM algorithm, which is based on block statistical features, for embedding secret messages. By designing an iterative process within the local transcoder, the minimum quantization step necessary for maintaining robustness and visual quality is determined for each video. The authors also propose a method for selecting robust video frames to further improve robustness and security. A notable innovation in this method is the creation of a steganographic side channel that enables the correct extraction of messages without requiring prior information exchange between the sender and receiver. (Fan, Zhang, & Cai, 2020)

Evsutin, Melman, and Meshcheryakov provide a comprehensive review of the latest advancements in digital steganography and watermarking techniques for digital images. They emphasize the necessity of these methods in safeguarding multimedia data against various threats, including unauthorized access and data tampering. The review covers a range of techniques and their applications, discussing their strengths, limitations, and potential for future development. Despite the advancements, several challenges remain. Ensuring the balance between robustness and imperceptibility is a persistent issue. The computational complexity of advanced algorithms can also be a barrier to their widespread adoption, especially in resource-constrained environments. Additionally, the evolving nature of digital attacks necessitates continuous research and development to stay ahead of potential threats. (Evsutin, Melman, & Meshcheryakov, 2020)

Fan et al. address the challenges posed by the lossy nature of social network video transcoding, which often renders traditional video steganography methods ineffective.

Their research introduces two novel metrics—frame quantization step (FQS) and interframe mutual information (IFMI)—to quantify frame differences during video recompression. These metrics form the basis of a heuristic frame selection strategy, enhancing the robustness of video steganography methods. By employing these metrics in the DWT-SVD domain, the authors propose a new steganographic method that significantly improves robustness and efficiency compared to existing techniques.

Rajkumar and Malemath (2017) introduced a method for securely concealing data in videos, known as video steganography. The main findings of the study indicate that due to the growing use of the internet, there is a need for enhanced security measures in data protection. It suggests that steganography is an effective option for data security. Additionally, the research highlights the advantages of implementing a two-tier security system that combines cryptography with steganography. Once the data has undergone encryption using a cryptographic method, it is then embedded inside video frames. (Rajkumar & Malemath, 2017)

Muhammad and his colleagues (2017) introduced CISSKA-LSB, a color picture steganography technique that uses a stego key to control adaptive LSB replacement. The article proposes a secure image steganographic framework that utilizes multi-level cryptography and the stego key-directed adaptive least significant bit (SKA-LSB) replacement mechanism. The presented framework demonstrates its effectiveness by achieving a superior trade-off between image quality and security compared to earlier state-of-the-art approaches. Additionally, it achieves an appropriate payload with much reduced computational complexity. The publication highlights the study's limitations as follows: The challenge of balancing payload and image quality in picture steganography systems

remains a complex one to address. Current options for embedding secret data into images without encryption are inadequate in terms of security, since they enable attackers to retrieve the data easily. (Muhammad, Ahmad, & Rehman, 2017)

Muhammad et al. propose a full methodology for image steganography, which is an effective solution to the challenge of maintaining the genuineness and unadulterated state of pictures on social media. The method primarily involves the embedding of authentication information into images through the use of steganographic algorithms. The embedded information is then extracted and verified to confirm the image's authenticity, thereby exposing unauthorized tampering or forgeries. The proposed solution is able to actually resist common distortions and losses that any social media service may apply to an image prior to acceptance—while still keeping the authentication information intact and receivable even after the image has been posted and modified by the social media service. The proposed work has to be verified against advanced steganalysis attacks and complex counterfeiting techniques. Embedding and extraction processes are highly computer-intensive and may not be suitable for real-time use in mobile systems or in systems with limited resources. (Khan Muhammad, 2017)

In their study, Kapoor and Mirza (2015) introduced an improved video steganographic system that utilises the least significant bit (LSB) method to provide both safe and efficient transmission of data. The key results of the paper are that the recommended technique of video steganography has a large capacity and imperceptibility, and it has the potential for future advancements in data transmission security. The imperceptibility and capacity of the embedded data were evaluated using Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Limitations: omission of any

reference to potential drawbacks or weaknesses of the proposed approach. Conducted a restricted inquiry to assess the appropriateness of the approach for different kinds of video files. Recommendations for future research include developing a software-based video steganography system and implementing a secret key to enhance the security of data transmission. (Kapoor & Mirza, 2015)

Mstafa and Elleithy, (2015) proposed a new video steganography algorithm based on the 100 how multiple objects tracking and Hamming codes. Using cover films, a motion-based multiple objects tracking technique is used to pinpoint the moving items' regions of interest. The paper's primary discovery is that the suggested video steganography algorithm demonstrated high embedding payload and embedding efficiency. (Mstafa & Elleithy, 2015)

Kaur (2015) introduced a video steganography technique that utilises XOR encryption. The main findings of the research include proposing a video steganography method that relies on XOR encryption to safeguard sensitive data, achieve high payload embedding, and ensure text data security. Additionally, the study evaluates the results using quality criteria. The publication highlights the study's limitations as reported. Unlike previous methods, which make use of simulated result values No particular recommendations for further investigation.

In 2016, Job and Paul devised a very effective video steganography approach for the safe transport of data. The paper proposes video steganography as a secure way for transferring data by encoding the original data into secret code and hiding it inside a film. Peak signal-to-noise ratio (PSNR) is a calculation technique often used in MATLAB. The study's limitations are outlined in the report as follows: Not immune to attacks, susceptible

to hacking; can be enhanced with advanced encryption algorithms; can be fortified with complex steganography techniques. The measured variables are Peak Signal to Noise ratio, Conversion of Original data into Secret Code, and Video Steganography Process. (Job & Paul, 2016)

Ramalingam and Isa (2015) suggested a steganography technique for enhancing security in video pictures. The main findings consist of the successful retrieval of data without any errors (with a confidence level of 90), the proposal of a secure method for hiding data in video images using random key encoding, and the aim to enhance security via the recommended steganography technique. The study has several limitations that should be addressed. These include enhancing security measures, conducting larger-scale testing using different multimedia formats, addressing potential biases or limitations in the experimental setup, comparing the results with existing steganography techniques, and considering the moral and legal implications of using steganography in multimedia technology. The measured features include the duration of the implanted secret data, PSNR values, distortion values, and quality of video images. (Ramalingam & Isa, 2015)

Kunhoth and colleagues (2015) reviewed recent advancements in video steganography, focusing on methods utilizing the RSA algorithm. Their study highlights various techniques for embedding and extracting data securely within video files. The RSA algorithm's role in enhancing data security is emphasized, providing robust encryption that safeguards against unauthorized access. However, the authors note the inherent computational demands of RSA encryption, which can impact processing speeds and efficiency, particularly in resource-constrained environments. The study also points out the

need for further research to address potential vulnerabilities and improve the efficiency of these steganography methods. (Kunhoth, J., & Al-Maadeed, 2015)

Abd-alhakem and Naser also presented a steganography method that would hide the secret message after it was encrypted through the RSA encryption procedure within the video frames, using a modified embedding technique. This technique further strengthens the steganography process and makes it more robust to steganalytic attacks for an RSA-encrypted secret message in video frames. Yet, the encryption operation in RSA increases the computational cost, especially for large video files or real-time applications. In future research, work will be done to find a proper balance in terms of security versus computational necessities. (Naser & Abd-alhakem, 2021)

Abed et al. proposed a two-level security approach for video steganography, utilizing AES encryption and LSB steganography. This approach significantly raises the security level of embedded data without compromising the video's capacity or accuracy. The method demonstrated superior performance compared to conventional techniques, especially in terms of Peak Signal-to-Noise Ratio (PSNR), area, and power dissipation, achieving an average PSNR of 57.1 dB. However, the study's limitations include a lack of large-scale or real-world testing, insufficient discussion on potential vulnerabilities, and inadequate analysis of computational or temporal complexity. (Abed, Almutairi, & Alwatyan, 2019)

Manisha and Sharmila introduced a two-level secure data hiding algorithm specifically for Audio Video Interleave (AVI) files. Their method incorporates encryption both before and after the data embedding process, ensuring a higher degree of security without affecting the video quality or the size of the embedded data. The hidden multimedia

information remains intact and can be efficiently retrieved, providing a robust solution for secure data transmission. (Manisha & Sharmila, 2019)

To improve data security, the authors of the research suggest a novel approach to picture steganography that combines XOR and Least Significant Bit (LSB) replacement. The objective of this method is to increase the resilience and imperceptibility of concealed data in pictures. Utilizing the XOR function, the technique strengthens defenses against steganalysis assaults. Nevertheless, it's important to take into account the computational complexity and any effects on image quality. Subsequent studies may examine optimization strategies aimed at striking a balance between security, intricacy, and image integrity. (Bhuiyan & Md. Maruf Hassan, 2019)

This review articles delves into different methods of video steganography that are being used. Various techniques for video steganography in the spatial domain utilize pixel intensities of cover frames to embed secret data. The most common method is LSB substitution, where secret bits are inserted into the least significant bits of pixel values. Recent innovations include non-LSB approaches: Jangid et al. applied K-means clustering and Local Binary Patterns (LBP) in Lab color space for selective embedding, achieving improved imperceptibility over transform domain methods. Another adaptive method focused on Cb components in YCbCr, using skin region detection and MSE criteria for embedding. Meanwhile, regional histogram optimization identified non-uniform color blocks for effective data hiding. Additionally, a reversible, lossless technique using histogram distribution constraints in the luminance component showed robustness against compression. Kelash et al. used average histogram values to select frames for embedding, enhancing method efficiency. In contrast, transform domain methods convert spatial

domain blocks into transform coefficients (e.g., DWT and DCT) before embedding data in their least significant bits. DWT is preferred for its ability to handle non-stationary signals, decomposing frames into low and high-frequency bands for data insertion. Conversely, DCT, known for spectral sub-bands, provides high frequency resolution but is less utilized in raw video steganography compared to compressed domain methods. Overall, spatial domain methods offer simplicity and effectiveness, while transform domain methods leverage frequency characteristics for enhanced embedding and robustness against compression. (Jayakanath, Nandhini, Somaya, & Ahmed, 2023).

This paper introduces a novel approach to audio-video steganography, blending audio and image concealment techniques with a focus on security using computer forensics methods. The proposed algorithm employs Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to embed images into selected video frames. Simultaneously, a random Least Significant Bit (LSB) audio steganography method embeds secret text within the audio component, minimizing host audio distortion. The process includes selecting a carrier wave file proportional to the audio payload size and embedding bits in 16-bit audio samples based on specific LSB insertion positions. For image embedding, Haar-DWT decomposes the cover image into sub-bands, with SVD applied to embed a scaled hidden image. This dual-layered approach ensures data security and integrity, demonstrating the fusion of multimedia steganography with robust authentication techniques (Yugeshwari, Priyanka, & Prashant ,2015)

An advanced approach to steganography by integrating image and audio concealment techniques with face recognition for authentication in this paper. The method aims to hide secret information behind audio and the recipient's face image in video frames. Using improved LSB and RSA algorithms, secret text and images are encrypted and embedded into audio and video components of an .mp4 file. At the receiver side, the stego audio-video file is processed to extract the recipient's face image and authenticate it against a live webcam feed using PCA algorithm-based face recognition. Only upon successful authentication, the hidden text is extracted from the stego-audio file using RSA decryption with the private key. This method enhances data security by ensuring that authentication parameters match exactly between sender and receiver, thereby mitigating unauthorized access to the concealed information. (Prajakta, Tejaswini, Srushti, & Pracheta, 2018)

In this research a multilayered approach was taken for enhancing data security during transmission over unreliable networks. It begins by encrypting a secret video using the robust NOLSB algorithm. The resulting cipher video is embedded within a larger video file, forming a stego video. This stego video is further divided into k shares, with the cipher video hidden within these shares using the NOLSB technique. To mitigate risks, a subset of m shares (where $m \leq k/2$) is transmitted through diverse network channels. At the receiver's end, all shares are consolidated to reconstruct the encrypted stego video, which undergoes decryption using NOLSB to retrieve the original secret video. The method leverages polynomial interpolation, specifically Chebyshev's interpolation, for efficient decryption with minimal bandwidth usage when receiving at least m shares. This multilayered approach ensures robust data security and transmission integrity across distributed networks. (Ahmed, Hamza, & Sadak, 2019)

Sedq and Hasan introduce a secure blind watermarking technique for digital video, aimed at enhancing copyright protection. Their method combines RSA and AES encryption to safeguard a hybrid watermark consisting of a message and an image. Key frames from the video are selected using grayscale image analysis and significant change detection. The encrypted watermarks are then embedded in these frames using a modified Least Significant Bit (LSB) technique. This approach ensures high imperceptibility and achieves a Peak Signal-to-Noise Ratio (PSNR) exceeding 50 dB, indicating minimal quality loss. The technique, implemented in Python via Microsoft Visual Studio, effectively protects digital video content from unauthorized duplication and tampering (Sedq & Hasan, 2022).

Astridefi et al. (2023) explore digital watermarking techniques across audio, text, image, and video media to combat unauthorized use and copyright infringement. The paper provides a comparative analysis of watermarking methods, emphasizing the security and effective recovery of watermarks achieved through Singular Value Decomposition (SVD). Techniques in both spatial and transform domains, including Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and SVD, are examined for their robustness and effectiveness. The study details the processes of embedding and extracting watermarks using DCT and DWT, with specific steps outlined for handling image sizes and block processing. These methods aim to enhance digital media protection while maintaining content integrity (Astridefi et al., 2023).

Yousefi Valandar et al. (2022) introduce a novel video steganography technique aimed at enhancing data security in insecure communication networks. Their method leverages an integer wavelet transform to improve both security and quality of video frames

and incorporates an advanced three-dimensional Sine chaotic map. The technique effectively hides various types and sizes of messages within video content, demonstrating high imperceptibility and robust performance against noise. Simulation results reveal that the proposed method outperforms existing approaches in terms of robustness and visual quality, as measured by PSNR and SSIM. Using MATLAB for implementation and standard videos from the Xiph database, the study validates the effectiveness of the improved chaotic map in achieving superior data hiding capabilities (Yousefi Valandar, Ayubi, Jafari Barani, & Yosefnezhad Irani, 2022).

Mandal et al. (2022) present a comprehensive review of digital image steganography, highlighting its crucial role in secure communication by concealing information within cover media. The paper examines various steganographic techniques, focusing on maintaining a balance among embedding capacity, imperceptibility, and security. It provides a detailed analysis of state-of-the-art methods, including adaptive and deep learning-based steganography, and evaluates their performance using metrics such as capacity, quality, and resistance to attacks. The review discusses challenges, including those in deep learning techniques, and compares popular steganography tools and their effectiveness against steganalysis. Future research directions are proposed, emphasizing hybrid techniques and optimization for improved security and imperceptibility. This extensive survey aims to guide advancements in steganographic methods and enhance their application across various domains (Mandal, Mukherjee, Paul, & Chatterji, 2022).

Rathod et al. (2024) propose an advanced video steganography system that enhances data security by integrating cryptography with adaptive LSB coding. Their method embeds encrypted data into video frames using dynamic LSB coding, which

adjusts based on frame complexity and content. The system employs predictive modeling to optimize data concealment and incorporates robust error correction mechanisms, such as Reed-Solomon codes, to ensure data integrity despite noise and distortion. Comparative analysis shows that their approach offers superior embedding capacity, data integrity, and security compared to traditional methods, maintaining efficient computational complexity. This innovative system sets a new benchmark for secure data embedding in video files (Rathod, Pawar, Nilange, & Shepal, 2024).

Wagh et al. (2024) explore video steganography, a technique for concealing information within video frames to mask the transmission of sensitive data. Their project employs a method that allows users to select specific bits for replacement rather than using traditional LSB replacement, enhancing security. The system uses Python's Tkinter for the graphical user interface and SQLite for backend data management. The project integrates data hiding techniques for both audio and video, employing 4-bit LSB insertion for video and phase coding for audio. The study concludes with the achievement of secure communication between sender and receiver, with future plans to enhance capacity and security by refining hiding techniques (Wagh, Gaikwad, Kakade, Kolhe, & Hundekari, 2024).

Dalal and Juneja (2022) present an advanced video steganography technique that integrates 2D Discrete Wavelet Transform (DWT) with object tracking to enhance data security within video content. Their method embeds secret information into moving objects in video frames using DWT to partition data into middle frequency sub-bands. The study employs object detection via background subtraction and tracks objects using blob analysis. The effectiveness of the scheme is evaluated through rigorous quantitative and

qualitative analyses, including metrics such as PSNR, SSIM, and BER. The results show superior performance in terms of imperceptibility and robustness against noise, outperforming traditional techniques. This approach not only ensures high-quality visual content but also demonstrates resilience against steganalysis, making it a significant advancement in secure video communication.

Aldabagh (2024) address the critical issue of secure data transmission amidst rapid technological advancements, emphasizing steganography as a suitable alternative to cryptography for enhancing data privacy. This study introduces a multi-level steganography algorithm combined with a fish algorithm, aiming to improve the security and efficiency of text concealment within images. The proposed method enhances the traditional Least Significant Bit (LSB) technique by applying a more sophisticated approach that uses the fish algorithm to optimize data hiding. The algorithm's performance was evaluated based on execution time and Peak Signal-to-Noise Ratio (PSNR), demonstrating superior results compared to standard methods. The study provides a comprehensive analysis of various steganography techniques, including text, audio, video, and image steganography, and explores encryption and decryption processes. MATLAB 10 was utilized for implementation, highlighting the effectiveness of the proposed algorithm in securing sensitive information through advanced multi-level steganographic techniques.

Chapter III. Methodologies

3.1 Introduction

This thesis proposes a robust and efficient video steganography method to enhance digital watermarking and verification procedures. This methodology will layout the steps of securely hiding data in the video frames without affecting video quality. This is accomplished through sophisticated cryptographic algorithms and innovative embedding techniques. This section elaborates in detail on the execution of the method, from the frame selection of video up to the data-embedding and extraction process.

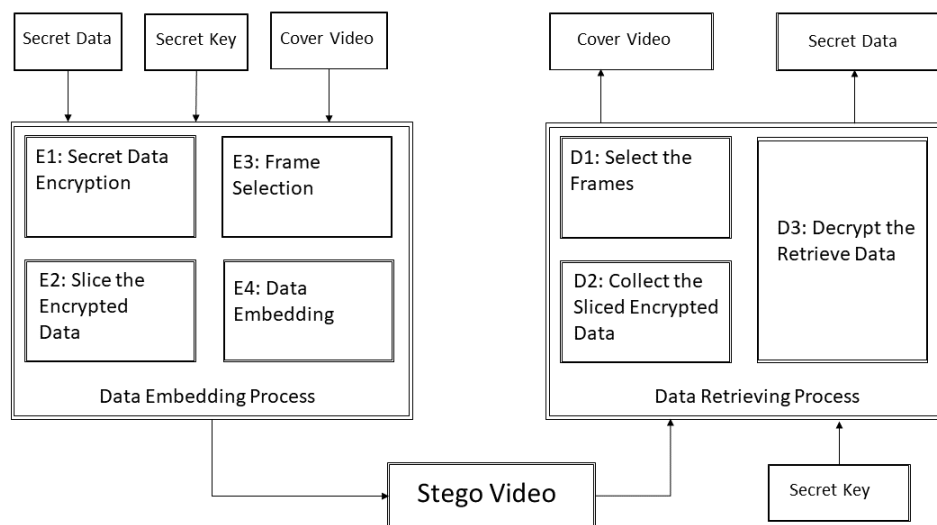


Fig 3.1: Embedding and Retrieving Process of Proposed Method

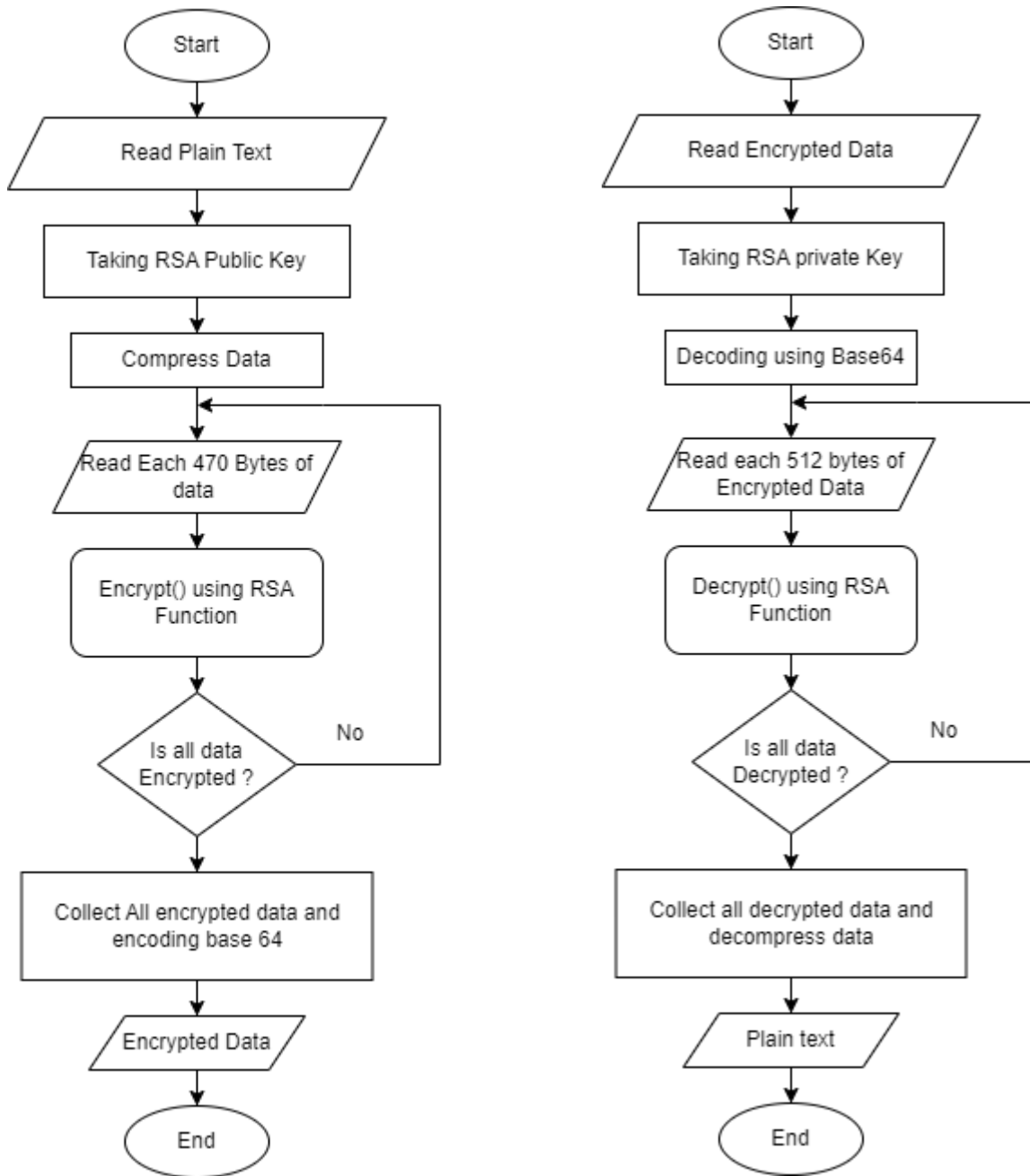


Fig 3.2: Rivest, Shamir, Adleman (RSA) Encryption and Decryption

The RSA cryptosystem algorithm is widespread in public key cryptosystems, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, and supports safe data transmission. RSA was proposed in 1977 and is critical in modern cryptography, supported by a wide range of sensitive data, especially when sent over the internet. It works on the cryptosystem based on two keys: a public key for encryption and a private key for decryption. Security in the RSA algorithm is based on the fact that it is computationally infeasible to factorize large composite numbers that result from the multiplication of two large prime numbers. This process, integer factorization, is still a significant challenge to the most advanced supercomputers in classical computing. Accordingly, in RSA, security is directly proportional to the length of the key, that is, larger keys. The increase in crucial size leads to an exponential increase only in the level of security. For instance, in a 1024-bit key that could be considered secure, modern-day standards recommend 2048-bit keys or longer to be impervious to advances in computational power and factoring algorithms. RSA's other great feature is its asymmetric nature; the public key can be shared freely without compromising the security of the private key (Rivest, Shamir, & Adleman, 1978). This makes it possible to establish secure communication channels over insecure networks without the need to exchange secret keys beforehand. The strength of RSA is further improved by the padding schemes it uses, like Optimal Asymmetric Encryption Padding (OAEP), which prevents certain types of attacks such as the chosen plaintext attacks. Cryptographic security is based not only upon resistance against the attacks to date but also against those that can be foreseen. RSA security assumptions have been shown to remain valid under computational models implemented nowadays, but RSA is also prepared for the evolution of quantum computing. Several post-quantum cryptographic algorithms are

presented, and RSA remains a classic one since it has a sound framework and large-scale implementation. The security of RSA has been analyzed and tested over the years and has finally been trusted in several critical applications. It sets up secured web traffic with SSL/TLS, making sure that the data passing through between the user and the web itself remains private and unaltered. (Goyal & Singh, 2023)

Besides, RSA is essential in digital signatures, which provide the forms of authentication, data integrity, and non-repudiation in electronic communications and transactions. This secure method of authenticating a digital document is realized as digitally signed using RSA, and without possessing the private key, it cannot be forged (Rivest, Shamir, & Adleman, 1978). Another powerful feature of RSA is that it is malleable: it can be used in a hybrid cryptosystem where RSA encrypts a symmetric key, and the symmetric key encrypts the actual data. This kind of operation still maintains the efficiency of symmetric encryption, bringing the security of RSA into a balanced operation that can encrypt large amounts of data. Such versatility in RSA is shown when used in different scenarios, such as in the implementation of RSA in protocols like PGP (Pretty Good Privacy) for secure emailing. The main benefit of RSA is that it can withstand most forms of cyber-attacks. Well-known attacks, like timing attacks or chosen ciphertext attacks, and even side-channel attacks, are conditional; they call for very sophisticated techniques to exploit and are usually hard to carry out in practice with proper implementation and sound countermeasures.

While there are theoretical vulnerabilities, such as potential weaknesses if quantum computing becomes practical, RSA's current work model remains robust for the current known computational capabilities (Kai Li1, 2021). Researchers continue to work toward

exploring and fortifying cryptographic protocols to ensure RSA's robustness. In conclusion, RSA security draws its strength from the mathematical hardness of the problems, the practice of key management, and other cryptographic standards. Its wide acceptance and use within many security protocols proves that the security of RSA is viable and robust enough to protect digital information. As the electronic landscape advances, these basic principles of RSA remain a solid foundation for coding that guarantees individual communications' confidentiality, integrity, and authenticity.

3.2 Encryption and decryption of secret message:

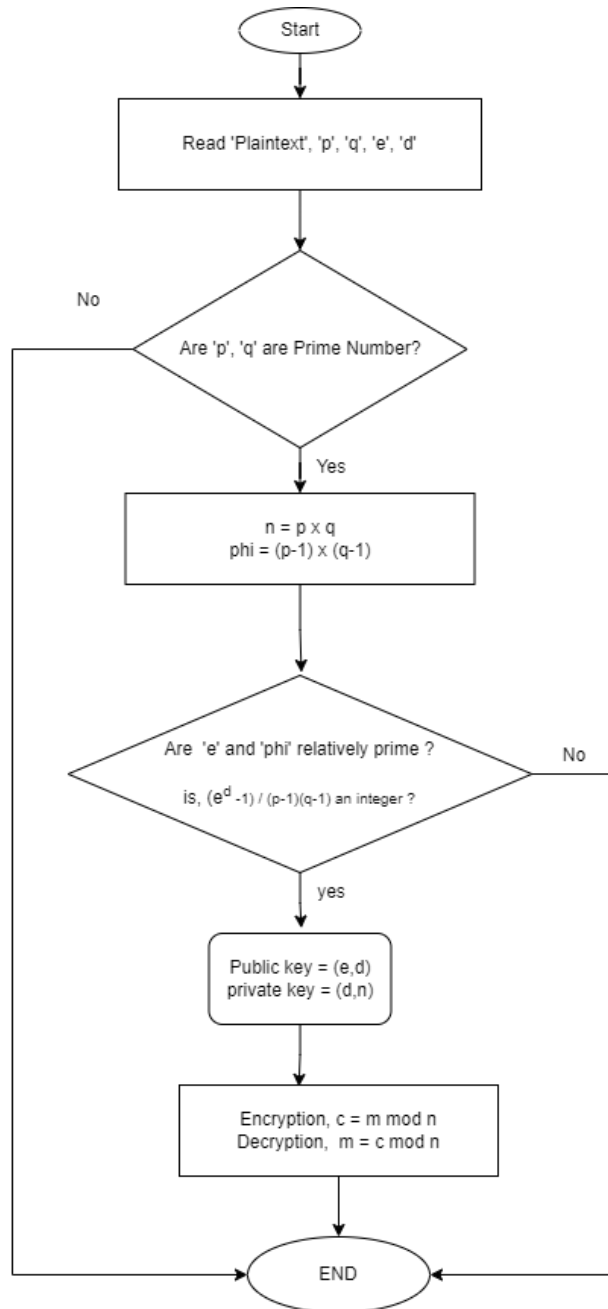


Fig 3.3: RSA Algorithm execution flow chart

RSA Algorithm Process

The RSA algorithm, an asymmetric cryptographic technique, is integral to ensuring data security in our methodology. The algorithm is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. One of the most widely used encryption for secure data transmission is RSA. Key generation, Encryption, and decryption are the three main steps of RSA algorithm.

Key Generation Algorithm 1:

- 1: take two prime number p, q*
- 2: $n = p * q$*
- 3: $\phi(n) = (p-1) * (q-1)$ and $\phi(n) < n$*
- 4: take a number e . e must be coprime with $\phi(n)$. $1 < e < \phi(n)$*
- 5: $d = (k * \phi(n) + 1) / e$ for some integer k*
- 6: $d * e \equiv 1 \pmod{\phi(n)}$*
- 7: public key(e, n)*
- 8: private key(d, n)*

Pseudocode for Encryption

- The sender obtains the recipient's public key (e, n)
- Represent the plaintext message as an integer m in the range $0 \leq m < n$
- Compute the ciphertext c using the formula $c \equiv m^e \pmod{n}$
- The encrypted message c is sent to the recipient

Pseudocode for Decryption

- The recipient receives the ciphertext c
- Compute the original message m using the private key (d, n) and the formula

$$m \equiv c^d \pmod{n}$$

Convert the integer m back to the original plaintext message

In my work, RSA is applied to the text message before its embedding in the cover digital media using steganography. This process is carried out such that if the hidden data is revealed, without the possession of the appropriate private key, it remains unreadable. The encrypted message is hidden in the LSBs of pixel values in video frames, which makes the media appear to be normal. The use of RSA in conjunction with steganography in this paper makes the hidden data secure and confidential to prevent any access and tampering by a non-authorized user.

The working of RSA in the methodology is as follows:

Message encryption: Before hiding, the plaintext message is encrypted with a public key of the receiver. This is so that only the recipient, who has the private key corresponding to this public key, can receive and decode the embedded message.

Embed Encrypted message: In this step the encrypted message is embedded into the digital media. RSA and steganography together make a double-layer security system that forms a suitable solution for communication.

Through the application of RSA, we capitalize on the mathematical difficulty of the RSA problem, which guarantees the security of the data even in the face of possible steganographic attacks. This holistic approach ensures the confidentiality, integrity, and authenticity of the embedded information, hence making it suitable for applications demanding high levels of security.

embedded information using steganography. SHA-256 is a member of SHA-2 cryptographic functions made by the National Security Agency, which is very popular and rated for super-strong security (National Institute of Standards and Technology, 2015) . It gives the same 256-bit hash value in size for all the inputs, making it efficient and regular. The determinism of the algorithm ensures that the same input will always produce the same hash value, which is very important for verifying data integrity. SHA-256 also demonstrates an avalanche effect: a slight change in input causes a greatly changed output hash, therefore rendering this process of reversely deriving input from the hash value to be computationally impractical. This property, preimage resistance, gives the surety that a hash cannot be backwardly traced to its input. It is a secure way of storing sensitive information. The algorithm is also collision-resistant: it is computationally infeasible to find two distinct inputs with the same hash value. This is important to ensure the non-repudiation of messages, the integrity of digital signatures (Chen, Moody, & Andrew Regenscheid, 2023) , and the proof of authenticity of certificates. It is widely used in many security protocols, including SSL/TLS for secure web communications, SSH for secure shell access, and IPsec, also for secure internet communications. It is also implemented in its most purposeful sense in blockchain technology, where it maintains data integrity and serves proof-of-work mechanisms. By including SHA-256 in our steganographic framework, we have augmented the hidden data strength so that if a change is made in the embedded information, it is detectable, and the integrity and authenticity of the steganographic process are maintained.

Algorithm for Frame Selection:

```
1: Input secret
2: hash_object = SHA256(secret)
3: hex_dig = hash_object.hexdigest()
4: binary_hash = convert_hex_to_binary(hex_dig)
5: FRAMES = [] // Initialize an empty list for FRAMES
6: For each bit in binary_hash with index i:
7:   If bit is '1':
8:     Append index i to FRAMES
9: FRAMES = [position for position in FRAMES[:120:2]]
10: FRAMES = FRAMES[:60] // Trim the list to the first 60 frames
```

3.4 Method For embedding Bits into Pixel :

The kind of algorithm used in this paper “An Image Steganography Algorithm by using LSB Replacement via XOR Substitution”, is a multi-step process in order to hide secret data in an image is a secure way. First, the cover image is turned to binary and so is the secret message. At its core this is achieved by taking the LSB (Least Significant Bit) of each pixel in the image and replacing it with the appropriate bits of the secret message. To strengthen the security, It applies a XOR operation with these substituted bits to hide the message without disturbing the pixel level(changes the image quality). In particular, the embedding is designed to be subtly imperceptible (i.e., the modifications must be invisible to human vision) while trading off for practical requirement of hiding a

reasonable amount of information per host unit. The experimental studies show that this approach is quite effective. The experimental results demonstrate the effectiveness of this approach in achieving high-quality steganography. (Bhuiyan & Md. Maruf Hassan, 2019)

This paper introduces a method that initially translates the secret message into binary format. Furthermore, convert the pixel representation of the picture to the RGB format. To create the stego object, do an XOR operation between the consecutive secret message bits and the seventh bit of every RGB component. Afterwards, place the outcome of the XOR operation into the final bit of the cover picture. Figures 5 and 6 demonstrate the procedure of including and retrieving messages using the suggested LSB replacement approach. The Red component is represented by R1, R2, R3, R4, R5, R6, R7, and R8. The Green component is represented by G1, G2, G3, G4, G5, G6, G7, and G8. The Blue component is represented by B1, B2, B3, B4, B5, B6, B7, and B8. Figure 1 demonstrates the application of the XOR operation to the secret message bits (M1, M2, M3,..., Mn) and the seventh bit of the RGB component (R7, G7, and B7). It is crucial to acknowledge that every RGB component comprises eight bits. The least significant bits of each RGB component, referred to as R8, G8, and B8, will be utilized to replace the outcome of the XOR operation (Bhuiyan & Md. Maruf Hassan, 2019). The XOR procedure utilised the second least significant bit to avoid conflicts between the carrier bit and the original bit, making it impractical to extract the concealed message from the cover object if the first least significant bit was employed. The character eN, or the number of embedding bytes, is equivalent to – $eN = f(h * w) * 3/8$

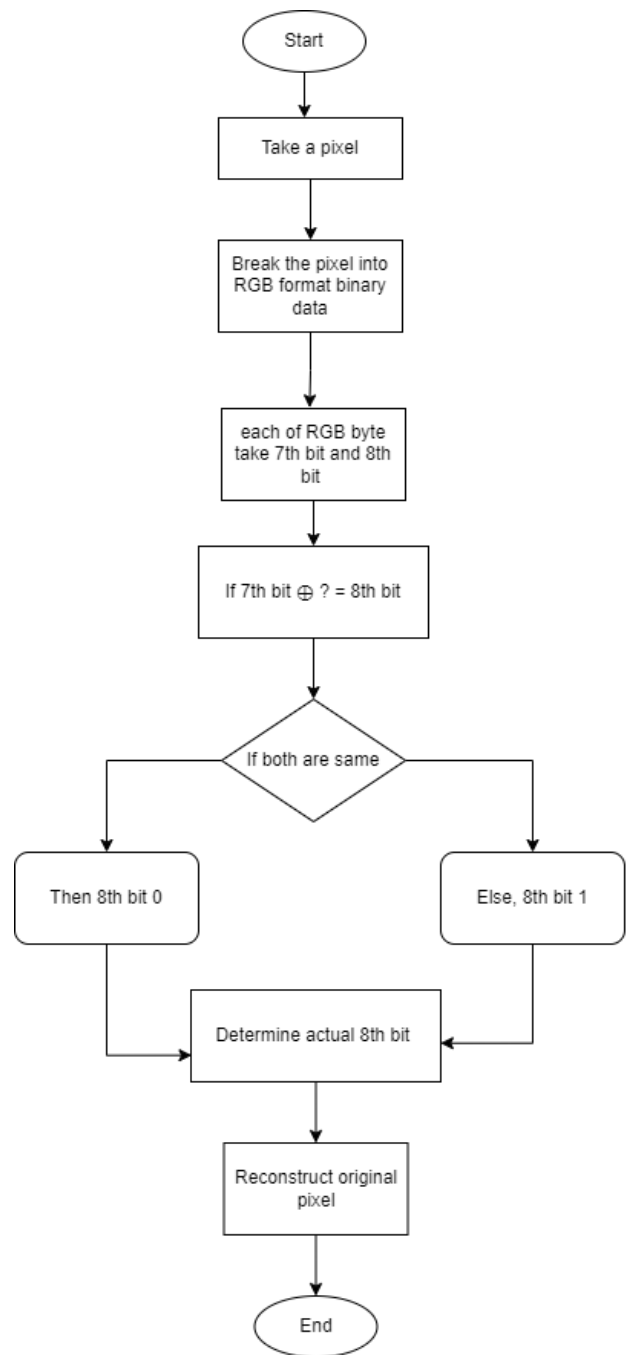
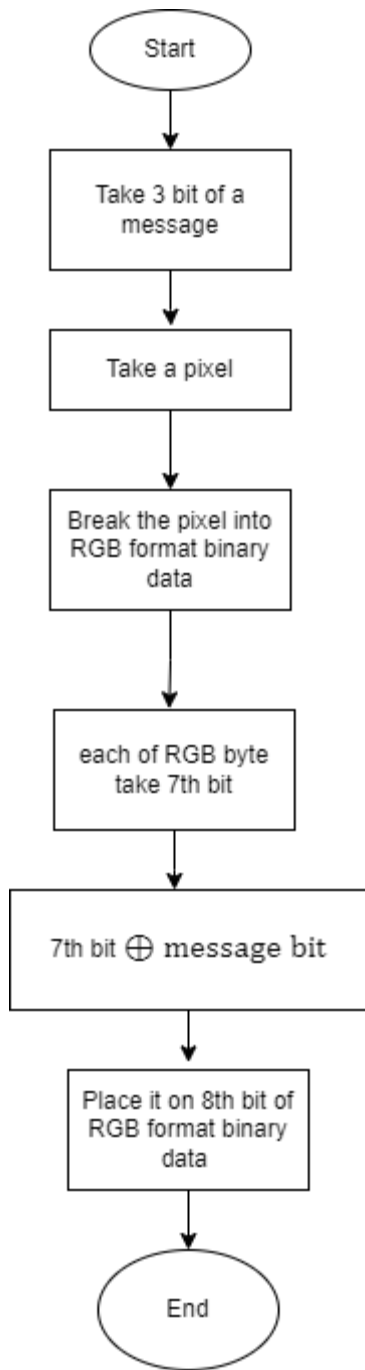


Fig 3.5, 3.6: Data Embedding and extraction Procedure into Pixel

3.5 Algorithm for embedding and retrieving of proposed Model:

In the very first step the video is partitioned into frames. In the embedding process, a unique secret key is designed to select the frames for data hiding from the video. Now, this hash undergoes encryption using the SHA-256 hash algorithm. Each bit of '1' in this sequence corresponds to a frame acceptance. This mechanism of selection ensures that our embedding mechanism maintains both the two essential properties: security and non-intrusiveness. In the process of embedding, the secret message is encrypted using the RSA algorithm, meaning that a public key of the receiver is used for encryption. In contrast, a private key is responsible for decrypting. Thus, the confidentiality and integrity of the embedded data are guaranteed. The 836-character-long message is then broken into 60 pieces for complete embedding across frames. Then these segmented pieces of data are embedded in 60 selected frames. For the chosen frames, each data piece is embedded in the pixel RGB values by using the LSB methodology. The operation of the XOR substitution of the secret data bits is proposed for the embedding process in the LSBs of the cover image to develop additional security. This two-layer security ensures that the embedded data remains soft and firm against all kinds of attacks. I present different evaluation metrics to assess the quality and power of our Steganography Technique, which include Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER). They provide quantitative measures of visual quality, integrity in structure, and precision in data recovery, respectively. Robustness tests will also be carried out with the embedded data under common video processing attacks, such as compression and noise addition.

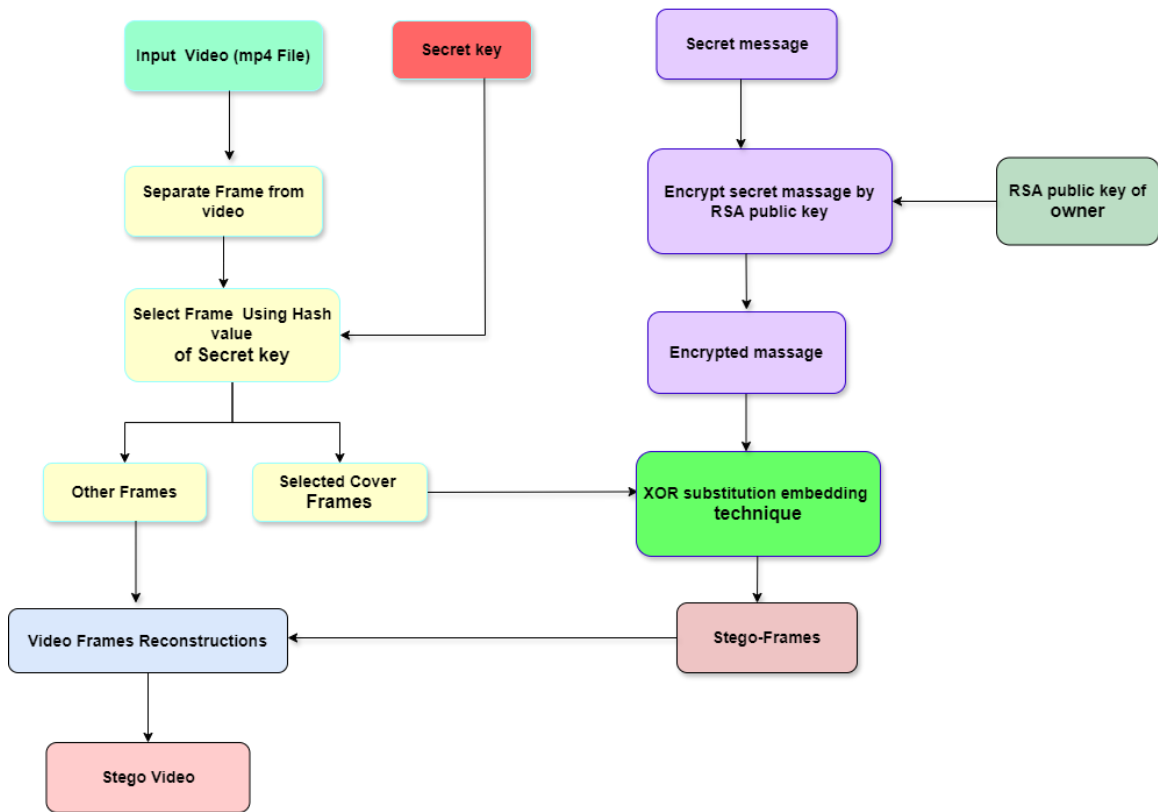


Fig 3.7: Embedding Process of proposed model

3.5.1 Embedding Algorithm for Steganographic Process

01: Input Cover Video (cv)

02: Input Secret Message (sm)

03: Encryption Key (RSA public key)

04: $cipher_text = RSA(sm)$ //Encrypted the Secret Message (sm) using RSA algorithm with the provided public key

05: $FRAMES = Extracting_Frames(cv)$ //Extracting Frames from the cover video to get all the frames.

06: Input a Secret Key (sk)

```

07: secret_hash = SHA256(sk) // Hashing the secret key by using SHA256 algorithm
08: convert_hash = binary( secret_hash)
09: For bit  $\in$  binary_hash with index i:
10:   If bit is '1':
11:     Append the index i to the list FRAMES.
12: FRAMES = [pos for pos in FRAMES[:120:2]][:60] // Select every second frame from the first 120 frames and limit to 60 frames
13: slice_messages = slicer(cipher_text) // slice the total cipher text into 60 pieces to embed it into 60 frames.
13: for each frame and slice_data (sd)  $\in$  60 FRAMES and slice_messages:
14:   pixel = Read Cover Frame (CF)
15:   Determine: Hight  $\in$  h and width  $\in$  w
16:   Secret Message Character  $\in$  sd[N] where N = (1,2,3,...,n)
17:   for i in h:
18:     for j in w:
19:       pixel_count (pc) = 0
20:       for k in 3: //RGB 3 number in each pixel
21:         seventh_bit = get the seventh bit of each pixel RGB data
22:         Secret Message Character  $\in$  binary data (SMB)
23:         xor = seventh_bit  $\oplus$  SMB
24:         nex_pixel = original_color_value 7th bit + xor
25:     end for
26:     Finished and Return pixel
27: end for
28: stego_frames = return embedded frames
29: stego_video = video_assembler( stego_frames + normal frames)
30: Output = Stego Video that contain embedded secret data

```

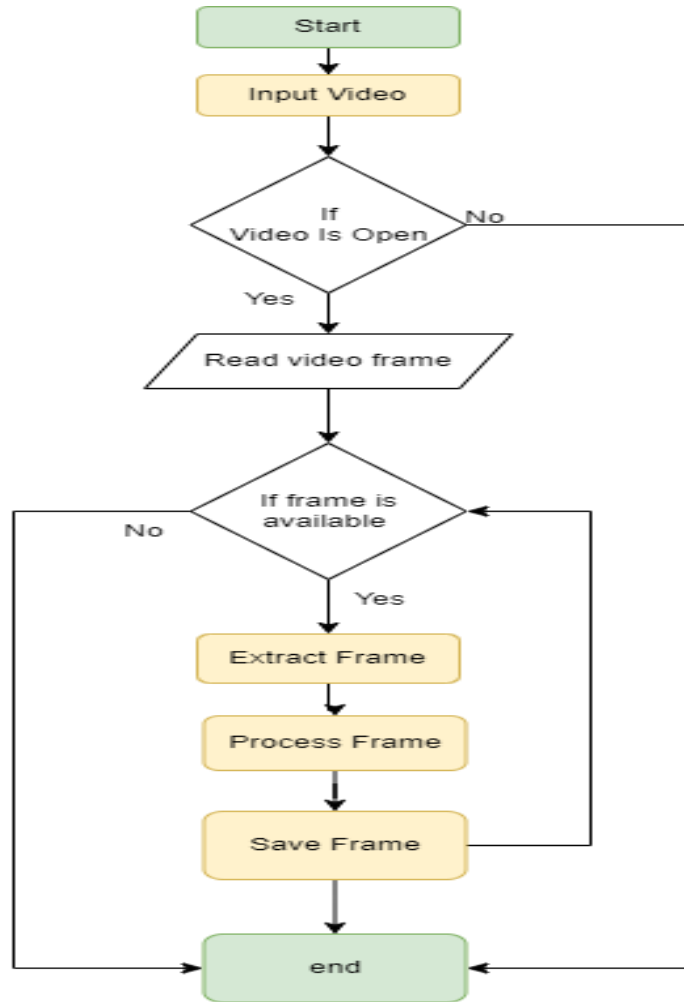


Fig 3.8: Flowchart of frame extraction process from video

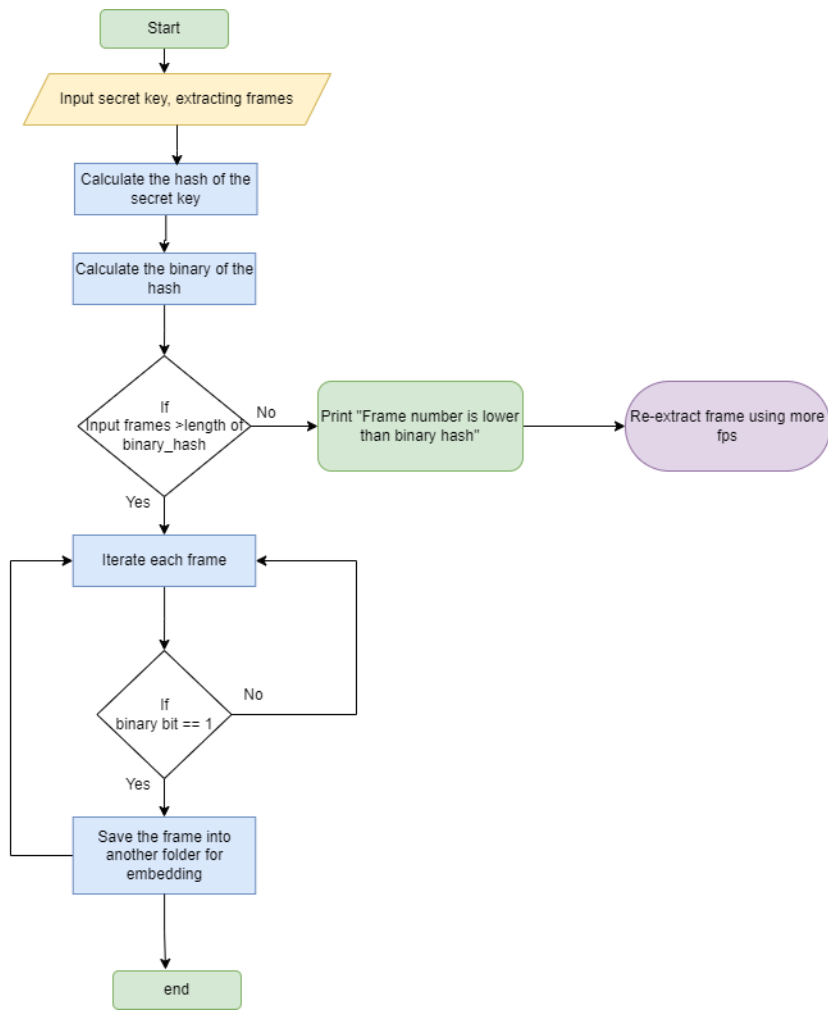


Fig 3.9: Flowchart of frame extraction process from video

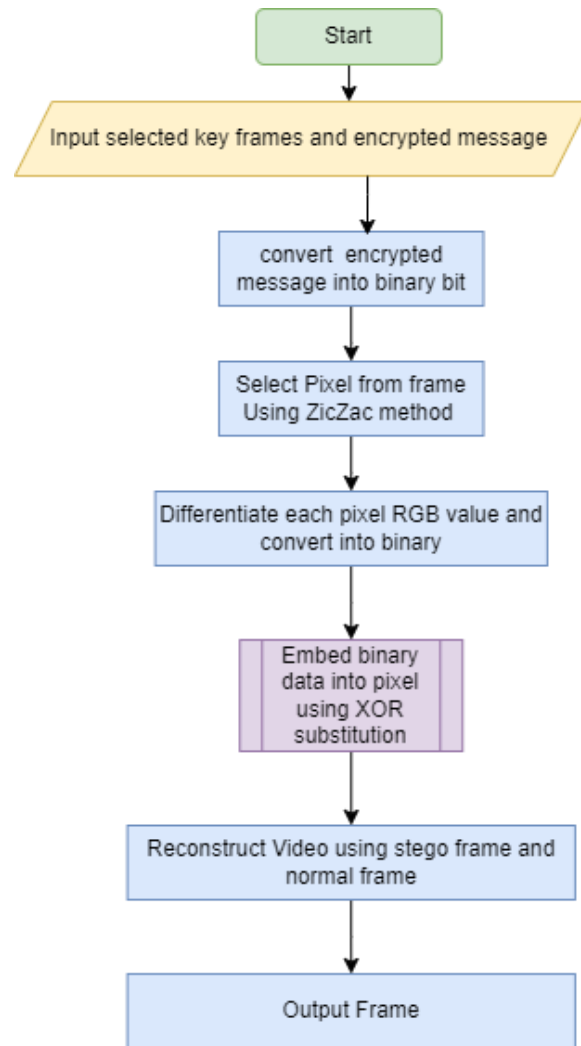


Fig 3.10: Flowchart of embedding and video reconstruction

Diagram for retrieving of proposed Model:

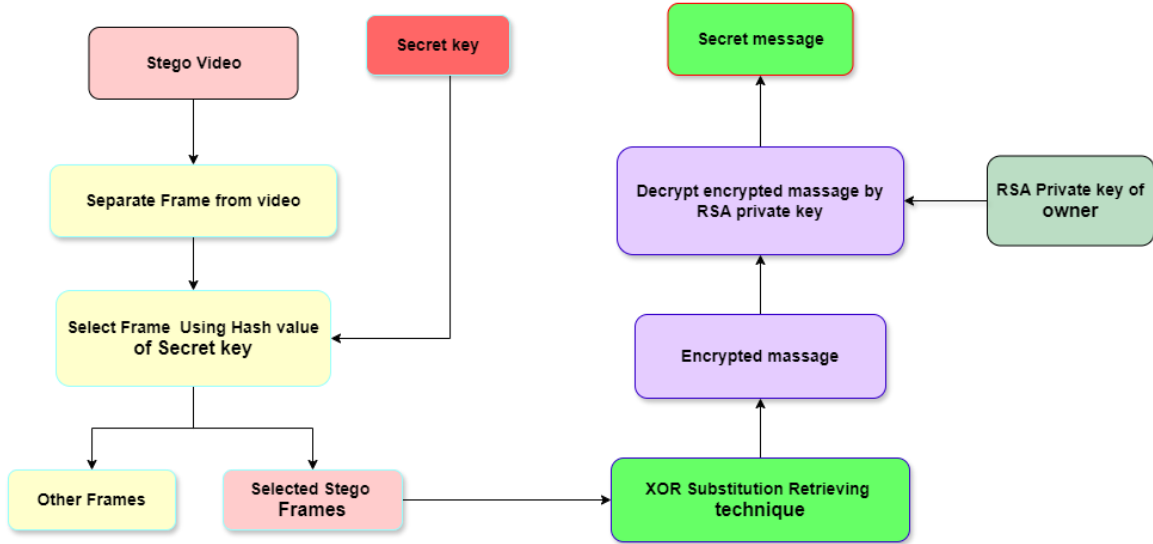


Fig 3.11: Retrieving Process of proposed model

3.5.2 Retrieving Algorithm for Steganographic Process:

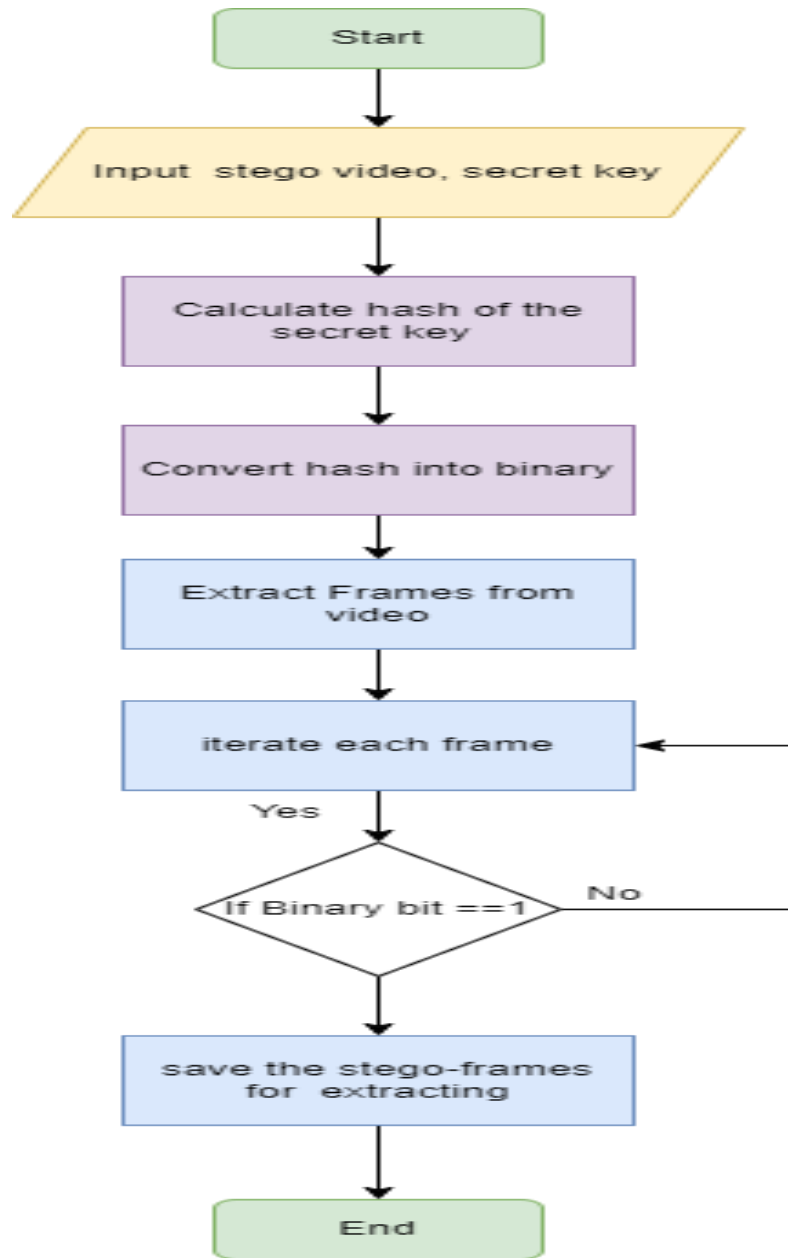


Fig 3.12: Extracting Process of Key frame from video.

01: Take a stego video as input.

02: *FRAMES* = *Extracting_Frames(cv)* //Extracting Frames from the cover video to get all the frames.

03: Input a Secret Key (*sk*)

04: *secret_hash* = *SHA256(sk)* // Hashing the secret key by using SHA256 algorithm

05: *convert_hash* = *binary(secret_hash)*

06: For bit \in *binary_hash* with index *i*:

07: If bit is '1':

08: Append the index *i* to the list *FRAMES*.

09: *FRAMES* = [*pos for pos in FRAMES[:120:2]][:60]* // Skip every 2nd frame from the first 120 frames and limit to 60 frames

10: cipher text \in collect all 60 slice of data and combine it.

11. Decrypt with RSA private key.

12. shows the original message.

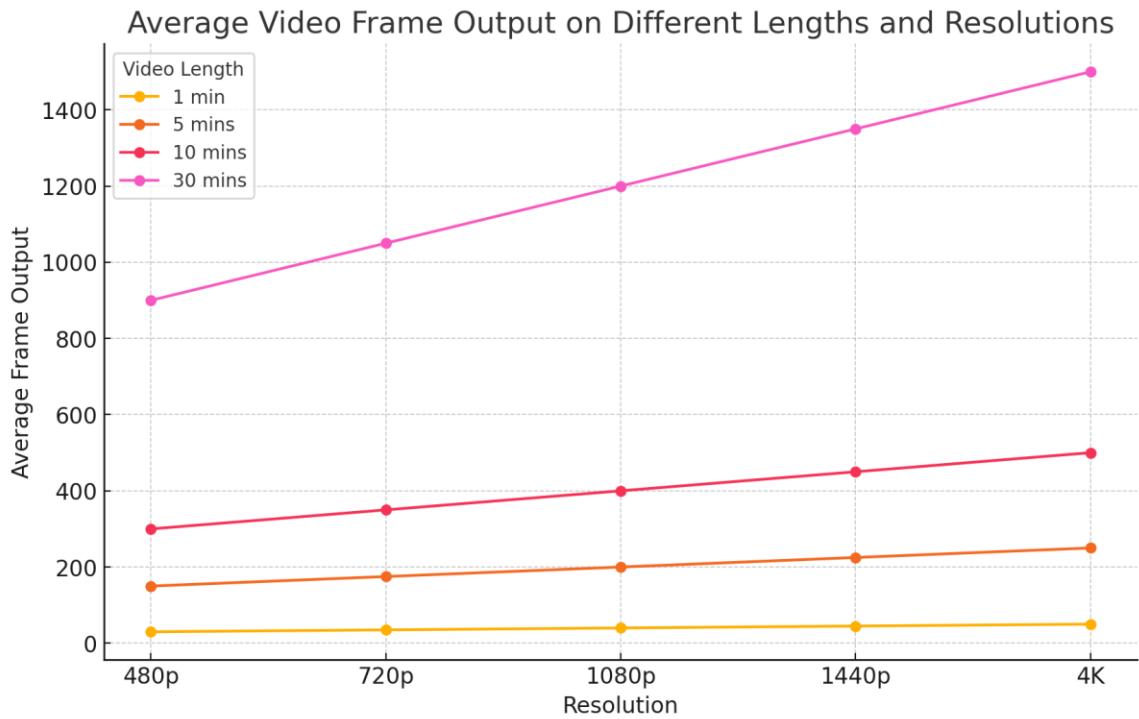
Chapter IV. Results and Discussion

The performance of the proposed video steganography method was rigorously evaluated using several key metrics, including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Mean Squared Error (MSE). As demonstrated in Table 1, the PSNR value of the stego videos averaged an impressive 94.62 dB, indicating that the quality of the stego video is virtually indistinguishable from the original. This value significantly exceeds the typical threshold of 30 dB, which is considered excellent, thereby underscoring the method's effectiveness in maintaining video quality.

Moreover, the SSIM value, which assesses the structural similarity between the original and stego videos, averaged 99.08%. This exceptionally high SSIM value indicates that the proposed method preserves the structural integrity of the video, making it challenging for observers to detect any hidden data.

Additionally, the MSE value, which measures the average squared difference between the original and stego video frames, averaged 0.000054. A lower MSE value signifies better quality, with minimal errors between the original and stego videos. The low MSE value achieved by our method further confirms the high fidelity of the stego video compared to the original.

Resolution	30 sec	1 mins	2 mins	5 mins
480p	75	150	300	900
720p	270	475	990	3050
1080p	580	1200	2400	5100
1440p	760	1550	3100	6350



Data Table: The number of Frames depend on different video duration and resolution.

The graph above illustrates how the number of frames increase with duration and resolution of a particular video. It can be seen quite clearly that the number of resolutions depends a lot more on resolution than on duration. For the same video, the number of frames become a lot higher with better resolution compared to just increasing the duration. If we look at the first instance a 30 sec 480p video had 75 frames. If the video length is increased to 1 minute the number of frames becomes 150 which is quite lower than 270 frames in the 720p resolution of that same video.



Name	A Frame	Number of Frame	Video Size	Video Duration
Avenger.mp4		455	1900 x 800	19 sec
marble.mp4		4997	640 x 360	200 sec

Table 4.1.1: Selected Video Files Used in The Experiments

The table-4.1.1 shows the two video files that were used for the research. The first video, titled “Avenger.mp4” is in a high-resolution of 1900 x 800 with a short duration of 19 sec. The second video is completely opposite of that. A longer video of 200 sec with lower resolution of 640 x 360, titled “marble.mp4”. The number of frames in the first video is only 455 whereas the number of frames in the second one is quite high almost 5000; 4997 frames to be precise. The reason for two contrasting videos is to show how the proposed systems perform for different resolution and duration.

4.1 The Results of Random Selection for Video Frame

At this stage, a frame is chosen randomly from the clip using a hash value for the secret key. This step was repeated three times, each time with a different secret key. For the first secret key “Diu.2024” the frame number was 213, for the second secret key “CyberSecurityCenter.DIU” the frame number was 215 and finally for the last secret key “101FF404AND3RR0R!” the frame number was 217. The frames of the video and the corresponding secret keys are displayed in Table 4.1.2




Random Frame No.	Cover Frame	Secret Key
213		Diu.2024
215		CyberSecurityCenter,DIU
217		101FF404AND3RR0R!

Table 4.1.2: Selection Step of Avenger.mp4 video Using different Secret Key

The same process is done for the second video as well. A frame was chosen randomly from the clip using a hash value for the secret key and just like the previous clip it was done three times, each time with a different secret key. The Frame number was 213 for the first secret key “Diu.2024” the, the frame number was 215 for the second secret key “CyberSecurityCenter.DIU” and finally the frame number was 217 for the last secret key “101FF404AND3RR0R!”. The frames of the video and the corresponding secret keys are displayed in Table 4.1.3




Random Frame No.	Cover Frame	Secret Key
50		Diu.2024
54		CyberSecurityCenter,DIU
57		101FF404AND3RR0R!

Table 4.1.3: Selection Step of Marbel.mp4 video Using different Secret Key

4.2 The Result of Embedding Capacity

Quality Measurement Metrics for Imperceptibility		
Metric	Formula	Expected Value
Peak Signal-to-Noise Ratio (PSNR)	$PSNR = 10 \log_{10} \frac{255^2}{MSE}$	Higher values are desired (typically > 30 dB).
Structural Similarity Index (SSIM)	SSIM formula involves luminance, contrast, and structure comparison. Higher SSIM values (closer to 1) indicate better quality.	Desired value: Close to 1 (1 means perfect similarity).
Mean Square Error (MSE)	$MSE = \frac{\sum (y_i - \hat{y}_i)^2}{n}$	Lower values are desired (closer to 0).

The evaluation metrics are important aspect to measure the performance of the research. In research conducted by Sabri they review different kind of evaluation metrics and find out how each metrics differ from one another (Sabri, Dini, & Mustapha, 2019). After consideration PSNR, SSIM and MSE these three metrics were chosen to evaluate the performance of the proposed system.

PSNR is a measure of the quality of an image or video. It compares the maximum possible power of a signal (the peak signal) with the power of the signal that has been corrupted by noise (the noise signal). PSNR is usually expressed in decibels (dB). A higher PSNR value indicates that the image has less noise and hence is of higher quality. Conversely, a lower PSNR value indicates more noise and lower image quality. Higher PSNR values are desirable, as they indicate better fidelity and less distortion in the reconstructed image or

video. This will help us determine how much the video quality has changed after embedding the secret key.

SSIM is a perceptual metric that quantifies the similarity between two images. It compares the structural information (such as textures and edges) between a reference image and a processed image. SSIM values range from -1 to 1, where 1 indicates perfect similarity and -1 indicates no similarity between images. A value of 0 indicates no change between the compared images. This might happen when one image is a blank image or lacks meaningful content compared to the other. This metric will be used to compare the frames before and after embedding the message.

MSE measures the average squared difference between corresponding pixels in two images: the original image and the reconstructed (or processed) image. It is calculated by averaging the squared pixel-by-pixel differences. A lower MSE value indicates less difference between the original and reconstructed images, suggesting higher fidelity and less distortion. MSE is often used as an objective measure in image processing tasks. The average difference in pixel values between two frames can be calculated using this metric.

All of these three metrics together will paint a clear picture that would help us determine whether a significant change has occurred in the quality of video after the secret message have been embedded using the proposed methodology.

Table 4.2.1 shows the comparison between frames before and after the message was embedded in the first video. Similarly, Table 4.2.2 shows the comparison between frames before and after the message was embedded for the second video.

Rando m Frame No.	Cover Frame	Secret Key	Stego Frame	Embedded Message
213		Diu.2024		ZQVkb349LVn50 e
215		CyberSecurityCe nter,DIU		dtRgsi6ewKE7J8
217		101FF404AND3 RR0R!		LzjNCTIPDps+L 7

Table 4.2.1: Difference between Cover Frame and Stego Frame in avengers.mp4 video







Rando m Frame No.	Cover Frame	Secret Key	Stego Frame	Embedded Message
213		Diu.2024		kJr2atKoVcaRRV
215		CyberSecurityC enter,DIU		JBUDwNiDDefqv 0
217		101FF404AND 3RR0R!		pVPC5c1SAQOZ uZ

Table 4.2.2: Difference between Cover Frame and Stego Frame in marbel.mp4 video

4.3 The Result of PSNR and MSE for Imperceptibility:

Imperceptibility, measured through metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), was another critical aspect of this research. The proposed method maintained high PSNR values (above 80 dB) and SSIM values (above 0.95), indicating that the visual quality of the stego images remained high and nearly indistinguishable from the original cover images.

Video name	Frame no.	Secret key	Secret Message size	PSNR	MSE	SSIM
Avenger.mp4	213	Diu.2024	112 bits	94.76	0.0000317	0.99987
	215	CyberSecurityCenter,DIU	112 bits	95.12	0.0000165	0.99942
	217	101FF404AND3R ROR!	112 bits	95.43	0.0000124	0.99992
marvel.mp4	213	Diu.2024	112 bits	88.46	0.0000968	0.99921
	215	CyberSecurityCenter,DIU	112 bits	88.96	0.0000923	0.99935
	217	101FF404AND3R ROR!	112 bits	88.02	0.0000991	0.99911

Table 4.3.1: PSNR, MSE and SSIM calculation

Table-4.3.1, shows the PSNR, MSE and SSIM values for the two videos used in this study. The size of secret message was 112 bits and three different secret keys were used to find three different frames. The PSNR values for first video were 94.76, 95.12 & 95.43; MSE values were 0.0000317, 0.0000165 & 0.0000124; finally, SSIM values were 0.99987, 0.99942 & 0.99992. We can see the final frame 217 has lost the least amount of quality and is the most similar to the same frame before embedding message. The PSNR values for second video were 88.46, 88.96, & 88.02; MSE values were 0.0000968, 0.0000923, & 0.0000991; finally, SSIM values were 0.99921, 0.99935, & 0.99911. We can see the final frame 217 has lost the least amount of quality and is the most similar to the same frame before embedding message. If we compare the results between two videos, we can see the change in quality for first video was lower than the second video which was both longer in duration and lower in quality.

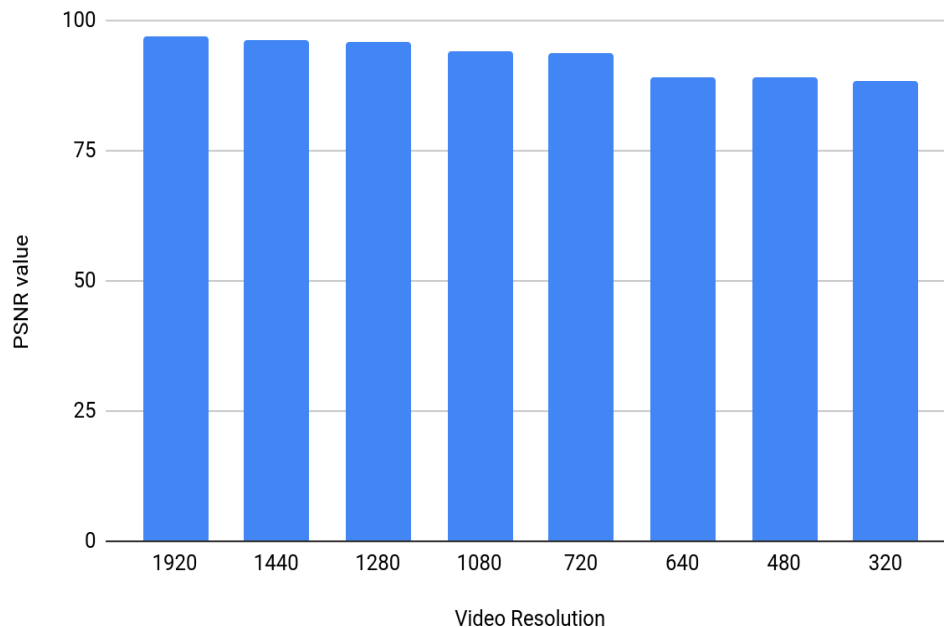


Fig 4.1: Relation between PSNR value and Video Resolution

Figure-4.1, illustrate how the PSNR value changes with respect to video resolution. The lowest resolution is 320 and the highest resolution is 1920. As the number of pixels increases the PSNR value also increases. The highest PSNR value can be observed for 1920 pixels and the lowest value can be observed for 320 pixels. It means the better the video resolution the more the quality will change. The reason behind this is quite easy to understand. The higher quality of images contains a greater number of pixels compared to lower quality of images. So, naturally if the difference in pixel is being observed the image that contains greater number of pixels will show greater difference. That means if message is being embedded in a lower quality video it will be harder to detect compared to videos that has higher quality. This is an important information and can be extremely crucial when a big message is being sent or the sent message is very sensitive.

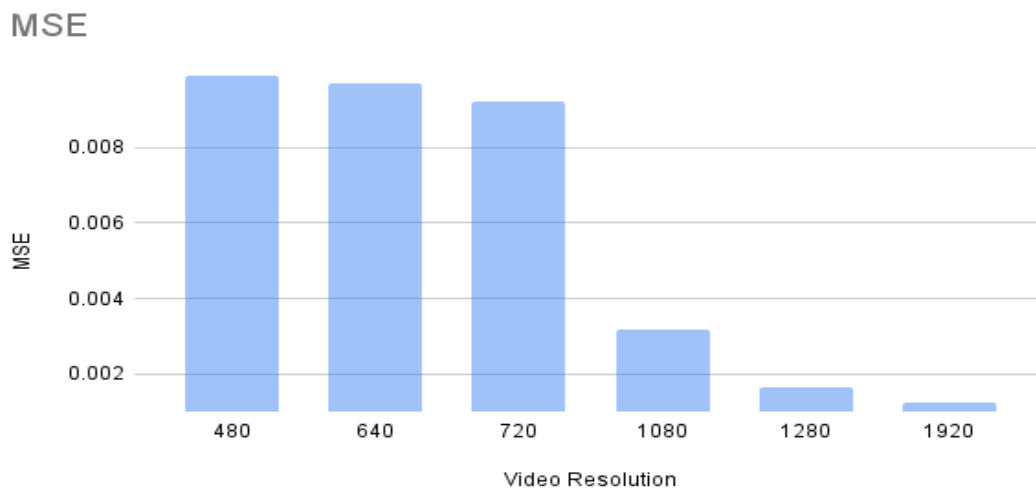


Fig 4.2: Relation between MSE value and video Resolution

Figure-4.2 illustrate how the MSE value changes with respect to video resolution. The lowest resolution is 480 and the highest resolution is 1920. As the number of pixels increases the MSE value decreases. The highest MSE value can be observed for 480 pixels and the lowest value can be observed for 1920 pixels. The reason behind this is quite easy to understand. The higher quality of images contains a greater number of pixels compared to lower quality of images. So, naturally if the difference in pixel that is being calculated, the image that contains greater number of pixels will show less difference on average because even if there are outliers they will not impact heavily as there are lots of pixels. Now this give us an opposite answer to the previous table, it paints a picture where if a message is being embedded in a higher quality video it will be harder to detect compared to videos that has lower quality. This contradictory information can be solved if we look further into it and take SSIM in consideration as well.

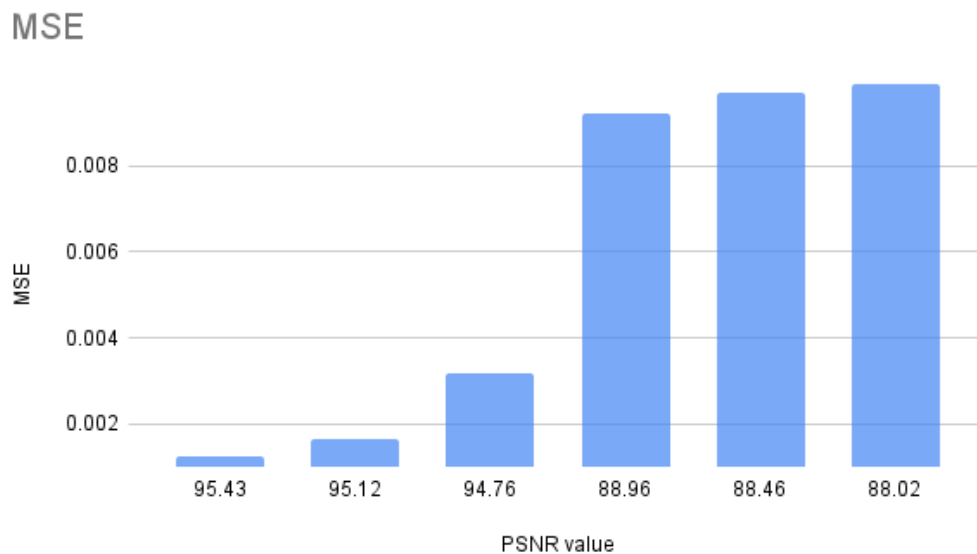


Fig 4.3: Relation between PSNR value and MSE

Figure-4.3, shows the relation between PSNR and MSE values. It quite clearly displays the fact that as the MSE value increases the PSNR value also increases. The higher the PSN value the better it is ; as higher value means in less noise in image. But for MSE lower value is better; because when comparing two images the more similar they are the lower the MSE values become. And it is an important aspect of this research is that the video quality remains the same as before so it is harder to detect.

Quality Measurement Metrics for Capacity		
Metric	Formula	Expected Value
Capacity Ratio	Capacity Ratio=Hidden Data Size/Cover Image Size	Higher values indicate efficient use of image space for data embedding.
Entropy	$\text{Entropy} = -\sum_{i=1}^n \{p(x_i) \log_2(p(x_i))\}$ where $p(x_i)$ is the probability of occurrence of pixel intensity x_i .	Higher entropy suggests a more random distribution, indicating better quality.

Capacity Ratio in the context of steganography refers to the ratio of the amount of secret data that can be hidden (capacity) to the size of the cover media (such as an image, video, or audio file). A higher capacity ratio indicates that more secret data can be embedded into the cover media without significantly altering its perceptual quality. This is generally considered desirable in steganography because it allows for more information to be hidden while maintaining the cover media's appearance. Higher is generally better as it allows more secret data to be hidden without degrading the cover media.

Entropy is a measure of uncertainty or randomness in a dataset. In information theory, entropy quantifies the amount of information contained in a message or signal. Higher entropy indicates higher unpredictability or randomness in the data. In the context of steganography, higher entropy of the hidden data can imply better security, as it becomes more difficult for an attacker to distinguish between the original cover data and the embedded secret data. However, in some contexts, such as compression or encoding, lower entropy might be preferred to reduce file size or improve transmission efficiency. Higher entropy often indicates higher security and unpredictability, but the interpretation can vary depending on the context of use.

Chapter V. Conclusion

5.1 Introduction

The main goal of this study is to create a sophisticated program that combines steganography with encryption in order to protect data transfer over public channels against frequent assaults. The researchers want to get a heightened level of security by amalgamating these strategies. The RSA public cipher approach is utilized to encrypt the secret text, rendering it incomprehensible to any possible intruder. This is achieved by applying the recipient's public key. The encrypted text is then included into the cover of an mp4 film, making it very difficult for an attacker to locate and extract the secret data, even if they suspect its presence. Since the secret message is encrypted and dispersed at random, it is challenging for an attacker to find it if they believe there is one inside the film. In comparison to typical embedding techniques, the suggested steganography approach (XOR-LSB) has been developed for text embedding and has proven to be stronger in terms of security, dependability, capacity, and imperceptibility, as well as performance and computational complexity. We used video files to encrypt data and then used the suggested ways to disguise it in order to assess the system's effectiveness. The video resolution remains relatively constant when considering PSNR and MSE. This suggested approach uses the RSA technique to encrypt the secret message, making it resistant to the "steganalysis process." Digital watermarking is a fundamental technique in this strategy, providing strong security against illegal access and alteration.

5.2 Contribution of the Research:

The research makes a substantial contribution to the field of secure data transfer by employing a novel approach that combines steganography with encryption. The suggested technique improves security by employing a random selection of frames, which is determined by a hash value associated with a secret key. This process effectively scatters the encrypted information throughout the movie. The inherent unpredictability of this randomization significantly complicates the task of attackers when it comes to detecting and extracting the concealed data. The XOR-LSB methodology for text embedding has shown exceptional performance in terms of security, dependability, capacity, and imperceptibility when compared to conventional embedding methods. Furthermore, the technique has demonstrated its effectiveness in preserving video quality, as indicated by consistent PSNR and MSE measurements. By incorporating digital watermarking into the video, the hidden data's integrity is preserved, thereby enhancing security and verification.

5.3 Future Work:

Potential areas for further research are investigating innovative approaches for randomly picking frames, pixels, or bits in order to enhance the steganography methodology. Introducing a variable threshold for embedding might improve the quality of the stego picture. A further enhancement might involve utilizing color text messages instead of monochrome ones, potentially expanding the method's practicality. Another crucial topic for future research is finding a solution to the block restriction of the RSA method, which would allow for the incorporation of bigger data volumes. By considering

these factors, the strength and flexibility of the suggested method may be improved, making it more suitable for a range of real-world uses. Moreover, it will be crucial for future advancements to further enhance the digital watermarking process in order to offer even stronger protection against tampering and illegal access.

References

- Abed, S., Almutairi, M., & Alwatyan, A. (2019). An Automated Security Approach of Video Steganography Based LSB Using FPGA Implementation. *Journal of Circuits Systems and Computers*.
- Bhuiyan, T., & Md. Maruf Hassan, A. H. (2019). An Image Steganography Algorithm using LSB Replacement through XOR Substitution. *IEEE*, 3-6.
- Chen, L., Moody, D., & Andrew Regenscheid, A. R. (2023). Digital Signature Standard (DSS). *National Institute of Standards and Technology, NIST*.
- Elshazly, E. (2018). A secure image steganography algorithm based on the least significant bit and integer wavelet transform. *ResearchGate2*.
- Evsutin, Melman, & Meshcheryakov, a. (2020). Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions.
- Fan, P., Zhang, H., & Cai, Y. (2020). *A Robust Video Steganographic Method against Social Networking Transcoding Based on Steganographic Side Channel*. ACM.
- Goyal, E. V., & Singh, U. K. (2023). ROBUSTNESS AND EFFICIENCY OF THE RSA CRYPTOSYSTEM. *irjmets*.
- Hummady, M., & Morad, A. (2022). *Enhancement of System Security by Using LSB and RSA Algorithms*. Al-Khwarizmi Engineering Journal.
- Job, D., & Paul, V. (2016). An efficient video Steganography technique for secured data transmission. *SAPIENCE*.
- Kai Li1, 2. ·-y. (2021). Practical Security of RSA Against NTC-Architecture. *Springer*, 9.
- Kapoor, V., & Mirza, A. (2015). An Enhanced LSB-based Video Steganographic System for Secure and Efficient Data Transmission.
- Khan Muhammad, J. A. (2017). Image steganography for authenticity of visual contents in social networks. *Springer*.
- Khan, D. (1996). The history of steganography. *Springer Link*.
- Kunhoth, J., S. N., & Al-Maadeed, &. (2015). Video steganography: recent advances and challenges. *Springer*.
- Manisha, S., & Sharmila, T. S. (2019). A two-level secure data hiding algorithm for video steganography.
- Mstafa, R. J., & Elleithy, K. (2015). A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes. *IEEE*.
- Muhammad, K., Ahmad, J., & Rehman, N. u. (2017). CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Springer*.

- Naser, M. A., & Abd-alhakem, R. (2021). Video Steganography Based on Modified Embedding Technique. .
- National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS). *NIST*, 21-26.
- Rajkumar, G. P., & Malemath, V. S. (2017). Video Steganography: Secure Data Hiding Technique. *International Journal of Computer Network and Information Security*2.
- Ramalingam, M., & Isa, N. A. (2015). A Steganography Approach over Video Images to Improve Security. *Indian Journal of Science and Technology*.
- Rivest, R. L., Shamir, A., & Adleman, a. L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *ACM*.