DESIGN AND DEVELOPMENT OF FRAME SELECTION BASED WATERMARKING TECHNIQUE TO ADDRESS QUALITY LOSS OF DATA

A Thesis

Submitted in partial fulfillment of the requirements for the

award of the degree of

DOCTOR OF PHILOSOPHY

in

Computer Science and Engineering

By

Chirag Sharma

41600060

Supervised By **Co-Supervised by**

Dr. Amandeep **Dr. Rajeev Sobti**

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

2021

Declaration

I hereby declare that the thesis entitled "DESIGN AND DEVELOPMENT OF FRAME SELECTION BASED WATERMARKING TECHNIQUE TO ADDRESS QUALITY LOSS OF DATA" submitted by me for the Degree of Doctor of Philosophy in Computer Science and Engineering is the result of my original and independent research work carried out under the guidance of Supervisors Dr. Amandeep and Dr. Rajeev Sobti, and it has not been submitted for to any university or institute for the award of any degree or diploma.

Place: Phagwara
Date:16/04/2021

Signature

Certificate

This is to certify that the thesis entitled “DESIGN AND DEVELOPMENT OF FRAME SELECTION BASED WATERMARKING TECHNIQUE TO ADDRESS QUALITY LOSS OF DATA” submitted by Chirag Sharma for the award of the degree of the Doctor of Philosophy in Computer Science and Engineering, Lovely Professional University Punjab, India is entirely based on the work carried out by him under our supervision and guidance, The work recorded, embodies the original work of the candidate and has not been submitted for the award of any degree, or diploma of any university and institute, according to the best of our knowledge.

Place:

Date:

Signature of Guide with Date & UID **Signature of Co-Guide with Date & UID**

ABSTRACT

The recent growth on the internet has led to the development of many applications such as digital libraries, OTT platforms, e-commerce. These applications make the digital assets, for example, digital pictures, video, audio, data source contents, etc., readily available by regular individuals worldwide for sharing, purchasing, distributing, and numerous other requirements. Lots of unauthorized persons are getting access to the data without the information of the owner. Consequently, digital items face severe difficulties as piracy, unlawful redistribution, ownership identification, forgery, theft, etc. The problem of illegal distribution enables different methods to be proposed and developed. Digital Watermarking, Steganography, and Cryptography provide practical solutions to these problems. Encryption methods can shield the information during transmission from sender to receiver; however, accepting the data, there's no assurance if the information received is correct or not. Steganography is a technique to hide a signal in the multimedia data to ensure it is not visible to any unauthorized user; however, it is not available visually. Watermarking offers the answer to these sorts of problems; the main goal is providing a technique to embed unnoticeable signal recognized as watermark in multimedia details in the type of text and image. The watermarking technology is available visibly and invisibly.

Videos are the most attacked multimedia data. The illegal distributors and unauthorized users find different ways to distribute and share videos across the internet without the owner's knowledge. Nowadays, OTT platforms are gaining popularity; many users pay for a subscription of the respective content. Unidentified users find a way to capture and distribute the data across the internet, leading to money loss to these platforms. The primary application of watermarking is in the field of copyright protection. The proposed work will focus on embedding an imperceptible signal watermark into videos to ensure ownership identification. Videos are available in the compressed and uncompressed (raw) form. Raw videos take a lot of time to process a watermark; although they will yield good quality, the time complexity is the major constraint in choosing raw videos in the research. Compressed videos have been used in this research. Video is a collection of several frames. Embedding a watermark in video poses many challenges, such as selecting frames and quality loss after insertion. Many researchers are adopting different strategies to overcome these challenges. Our proposed work will focus on choosing an appropriate number of frames from the video to embed the

watermark and ensure the watermark's embedding does not impact the watermarked frame's quality. The selection of the appropriate number of frames is an integral part of the proposed work. The watermark's embedding in every frame increases the chance of the watermark information getting concealed to an unidentified user and increases output video size. The frame selection algorithm proposed in this work works on the concept of scene change detection. There are many frames in the video, and the video is subjected to have many changes inside it. The algorithm detects changes in the video scene to identify the frames from similar and different video frames. The algorithm calculates frame differences by comparing the adjacent frames. Based on disagreements, various groups are made. The value of frame difference is going to decide if the frame will be considered the part of the same or another group. When the distinction is significant, then it'll be viewed as a part of another group. The choice parameter is dependent on the value of the threshold. The proposed algorithm selects the next group's first frame as part of the selected frames if the frame difference value exceeds the threshold value. The embedding of the watermark on selected frames is the next step. The proposed work focuses on providing security to the watermark before it is embedding. The encryption of the watermark is performed using hyperchaotic encryption. In our thesis, we have carried out watermark embedding with optimization and without optimization. The embedding factor provides the value of mixing the watermark with the selected frame. The watermark embedding factor value is taken as 0.02. The researcher's primary concern is that embedding of watermark should not impact the output watermarked frame's quality. Peak Signal to Noise Ratio (PSNR) is the quality metric used in this research. The calculation of results is done using the combined approach of Graph-Based-Transform and Singular Value Decomposition. However, this is a static process, and updating the value of embedding factor one after another will be time-consuming. To counter these issues, we have applied an optimization algorithm on embedding factors to target high values of PSNR. The hybrid approach of Grey Wolf Optimization and Genetic algorithm is used for this purpose. The optimization algorithm generates a set of solutions, checks the value of PSNR at every stage, and chooses the keys with high PSNR. There is a list of iterations defined in Grey Wolf Optimizer at that start. After applying the procedure of GWO, the value of the embedding factor is updated after every iteration. After every iteration, the value of the embedding factor is checked. Suppose the value is improved, then updation of the value of the embedding factor in the next iteration by taking the best value as a reference else;. In that case, we apply the genetic algorithm's cross-over operation by various exiting populations to form a new set of values. The hybrid optimization algorithm yield high values of PSNR compared to the static technique (GBT-SVD).There are four performance parameters used in this research: Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Normalized

Correlation(NC), and Bit Error Rate (BER). The robustness of the proposed technique is tested by applying various signal processing attacks. The attacks with different variance values are applied on the watermarked frame produced by Graph-Based-Transform and Singular Value Decomposition (GBT-SVD) and Graph-Based-Transform, Singular Value Decomposition, Grey Wolf Optimization and Genetic Algorithm(GBT-SVD-GWO-GA). The attacks used in this research are: Gaussian Noise attack, Sharpening attack, Rotation attack, Blurring attack, and JPEG Compression attack. A total of 6 videos have been taken in this research. The comparison analysis of both GBT-SVD and GBT-SVD-GWO-GA is done against all attacks. The scope of this research is the area of copyright protection, broadcasting, and ownership identification. The contribution made in the study is to propose a frame selection procedure to select the optimal number of frames from the video to be watermarked. A hybrid optimized watermarking technique is proposed. The effectiveness of the proposed technique is evaluated against many practical video processing attack scenarios. The literature survey demonstrates the use of many algorithms proposed in this area to address quality loss of data after embedding a watermark. The comparison analysis of the proposed method with existing methods is done on a similar set of videos to check its efficiency.

ACKNOWLEDGEMENT

I wish to express my sincere thanks to my supervisor Dr. Amandeep, Associate Professor, School of Computer Application, and my co-supervisor, Dr. Rajeev Sobti, Professor and Dean, School of Computer Science and Engineering, Lovely Professional University, with immense pleasure and a deep sense of gratitude. Both of my supervisors have given me the liberty to follow my passion for research work. The guidance, counseling, and suggestions were beneficial in completing work. It was a great privilege and honor to work and study under their guidance. Without their support, I would not have done this work with dedication. Both were my pillars of strength throughout this journey.

I would like to thank my friend Dr. Aman Singh for all the continuous support and confidence to carry my research correctly. I express my sincere thanks to my colleagues who have encouraged me always to complete this work on time.

I express my gratitude towards my student scholars (Roshan, Aman) for working very hard with me in image processing. Special thanks go to the panel and reviewers of the journals who vetted my submissions and gave valuable comments to improve the work further.

Finally, I wish to express my thanks to my mother, father for their sacrifice and tremendous support and my wife (Tanya Nagpal) for encouraging and inspiring me to do my best.

Date: 16/04/2021 **Chirag Sharma**

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ABC: Artificial Bee Colony

ACO: Ant Colony Optimization

AES: Advanced Encryption Standard

ANN: Artificial Neural Network

AVC: Audio Video Codec

AVI: Audio Video Interleaved

BPNN: Back Propagation Neural Network

BELM: Bi-directional Extreme Learning Machine

BER: Bit Error Rate

BFO: Bacterial Foraging Optimization

CA: Cuckoo Search

DCT: Discrete Cosine Transform

DES: Data Encryption Standard

DFT: Discrete Fourier Transform

DWT: Discrete wavelet transform

FFT: Fast Fourier Transform

FL: Fuzzy Logic

EA: Evolutionary Algorithm

GA: Genetic Algorithm

GA-BPN: Genetic Algorithm Back Propagation Neural Network

GBT: Graph-Based Transform

GBT-SVD: Graph-Based Transform Singular Value Decomposition

GBT-SVD-GWO-GA: Graph-Based Transform Singular Value Decomposition Grey Wolf Optimization Genetic Algorithm

GWO: Grey Wolf Optimization

JPEG: Joint Photographic Expert Group

LSB: Least Significant Bit Modification

MPEG: Moving Photographic Expert Group

NC: Normalized Correlation

OS-ELM: Online Sequential Extreme Learning Machine

PSO: Particle Swarm Optimization

PSNR: Peak Signal to Noise Ratio

SVD: Singular Value Decomposition

CHAPTER 1

INTRODUCTION

1.1 Overview

The internet provides a vast information source that gives unauthorized access and copy-enclosed information in audio, images, and videos to all end-users, allowing various techniques to be proposed and developed that provide digital data legal ownership. Watermarking, Steganography, and Encryption offer the solution to these problems. Encryption systems can shield the information during transmission from sender to receiver; however, accepting the data, there is no assurance whether the data received is correct or not. Watermarking provides the solution to these kinds of problems; the primary aim is to provide a method to embed unnoticeable signal known as watermark into multimedia data in the form of audio, video, text. The most common form of multimedia data that suffers from illegal distribution is videos of many formats. Thus, many researchers are developing various video watermarking techniques to ensure copyright protection. Embedding the watermark in the video visibly and invisibly is required as the attacks such as cropping and resizing attacks can temper the data. Thus, a technique is needed to achieve a robust algorithm for video watermarking to achieve copyright protection. Digital watermarking is a process to embed an invisible watermark into a host/cover digital content in such a way that the spread of watermark bits is scattered in the host evenly. Also, it must be infeasible to alter the watermark bits and could be extracted through some computation. The main applications of digital watermarking are copyright protection, ownership identification. The illegal distributors can readily temper the watermark in place of the original watermark or altogether remove the watermark visually allows the researchers to work on invisible watermarking so that it is challenging for intruders to detect and remove the watermark from the multimedia data. Figure 1.1 represents the visual tempering of data. Quality is an essential aspect of any video; embedding a watermark provides imperceptibility and robustness and makes the video vulnerable.

Researchers are proposing some embedding algorithms to ensure less quality loss after inserting a watermark, leading to an efficient watermarking technique. The videos available nowadays are not raw videos that were captured from satellite and captured cards. Most videos are in compressed form like- .flv,.avi,.mp4.The containers like WMV, H.264, XVID produce these formats. Most of these videos have the good quality, from the compression algorithm to raw videos, and the embedding of the watermark in the compressed video reduces quality. There are further challenges addressed in this research. One of the challenges is to embed a watermark in different formats of video. The most common attack on digital media is the cropping attack that many intruders find success in implementing. The example of a cropping attack is explained in Figure 1.1.

Figure1.1: Visual Tampering of Information[55]

Figure1.1 represents a cropping attack on signed video. An intruder or unidentified person has manipulated the watermark from EUROSPORT HD to TENNISHAVEN HD, or an intruder has wholly removed the watermark on the right-hand side of the video [56]. There are many watermarking techniques proposed. The illegal distribution of videos is gaining a lot of importance as videos from the theatre are directly transmitted to the Internet. The unauthorized users are gaining a lot of money by sharing the videos; hence a watermarking technique is required to counter these issues. Figure 1.2 represents the illegal distribution of data. Watermarking is the solution to this problem. Watermarking is done by adding the hidden signal (watermark) in the multimedia data and a secret key to get the watermarked image. Figure 1.3 represents the illegal distribution of multimedia data. The videos are available in raw and encoded formats. The encoded formats are accessible in mp4 and avi format. The codec used in the videos is x264. The encoded videos have been taken as reference videos as data sets and are available in mp4 format.

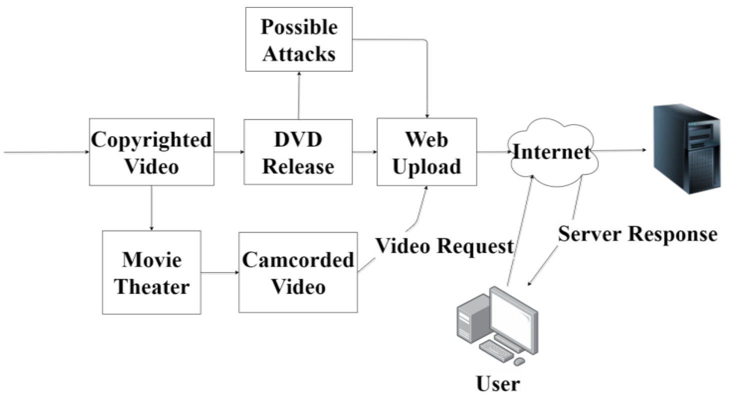


Figure 1.2: Illegal Distribution of Multimedia Data[76]

The watermarking done in the proposed work is based on invisible watermarking. Watermarked image contains confidential information from the intruder-the process of watermarking starts by inserting the watermark into the host image. Encryption of watermark before embedding to the multimedia is gaining a lot of popularity nowadays. Figure 1.3 represents the process of insertion, extraction, and detection of watermarks. The ciphers like plain text, transposition ciphers can be used for encryption purposes. Researchers nowadays aim to reduce embedding time and extraction time and take care of additional watermarking technique security. The proposed technique in this research also deals with the embedding of the encrypted watermark into a video.

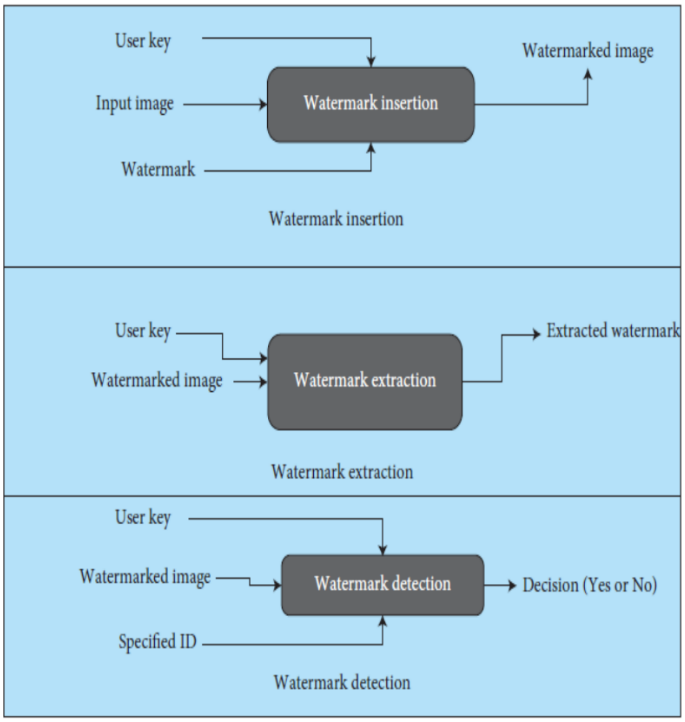


Figure 1.3: Process of Watermarking [90]

1.2 Various Watermarking Techniques

The watermarking techniques are categorized based on Domain, Document, Perception, and Application. Figure 1.4 represents all watermarking techniques.

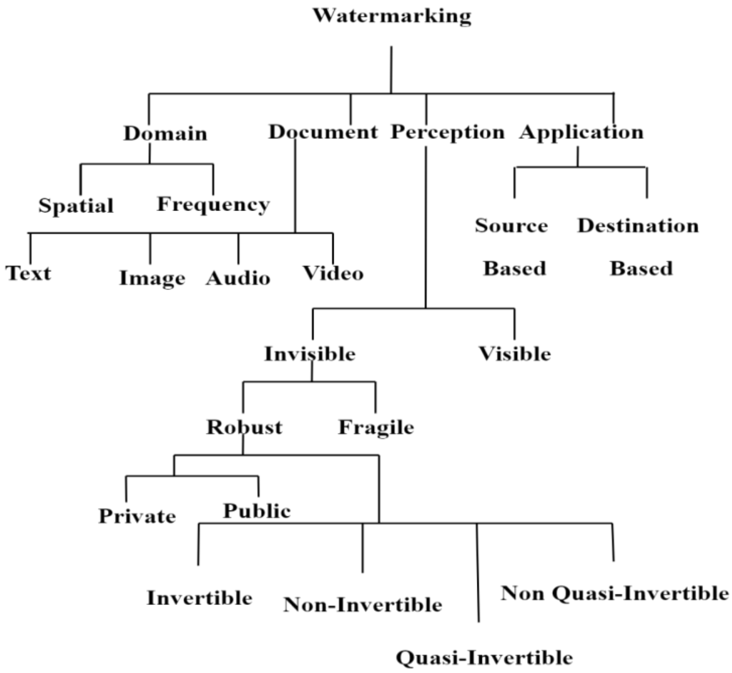


Figure 1.4: Watermarking techniques [76]

A. According to Domain

I. Spatial Domain Watermarking: The primary technique under this category is Least Significant Bit modification (LSB). It is a straightforward technique that uses an entire image to embed a watermark many times. An intruder can destroy the data; there is significantly less possibility for any watermark embedded inside the image to survive. These techniques have low computational complexities but suffer from de-synchronization attacks and multiple frame collusion. It becomes difficult to implement optimization techniques in LSB. Insertion of watermark directly into pixels directly impacts the quality of output watermark image.

a. Frequency Domain Watermarking: The primary techniques in the Frequency domain watermarking are- DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), and DFT (Discrete Fourier Transform) . Embedding of the watermark is done in overall domain of host data. The original data (image, video, audio) gets converted into frequency domain coefficients manipulated to store data in text, image, etc after that, the inverse transformation is carried to obtain original data. Throughout the watermarking process, the coefficients of transformation are altered by the watermark's insertion, followed by inverse transformation.

b. **Singular Value Decomposition (SVD):** SVD is a technique that converts a matrix into three matrices to reduce calculations. It is known as orthogonal transformation, widely used in applications of compression, denoising.

c. **Discrete Fourier Transforms (DFT):** It is widely used transform in applications of image processing. The image signal is represented as function and is converted into transform to carry out the embedding process.

d. **Discrete Cosine Transformation (DCT):** DCT enables an image to be divided into unique reoccur groups, making it a bit difficult to embed watermarking details to an image's prominent reoccur organizations. The primary function objective of DCT techniques will be performing against easy photo preparing modifications, for example, Low pass sifting, brilliance, distinctions shift, and obscure. Just the same, the defect with these kinds of solutions is security against alterations, turn, for instance, scaling and trimming.

e. **Discrete Wavelet Transform (DWT):**. Discrete Wavelet Transform that a type of wavelet transform that decomposes an image signal into corresponding frequency bands. Most researchers target high frequency and low-frequency bands to embed the watermark.

f. **Graph-Based Transform:** It is a newly formed transform that transforms the graph to a signal, G= {V, E, s} where V and E are the vertices and edges of the graph, and s represents the frame signal.

B. **According to Document:** Document represents text, audio, image, and video. There are many designed techniques for all documents.

C. **According to Human Perception**: 2 Methods are mentioned below

   a. **Visible Watermarking**: This is watermarking technique where the watermark is directly visible to the human eye.

   b. **Invisible Watermarking**: This is a type of watermarking technique where the watermark is embedded in a discreet manner.

D. **According to Application**: According to the application, Watermarking is categorized into 2 types.

   a. **Source-Based**: It is used to check whether manipulation of received data.

   b. **Destination Based**: It is used for tracing the source of illegal Copies.

1.3 Attacks on Watermarks

The performance of watermarking is evaluated by applying noise to the watermarked data. Noise represents any distortion to the output watermarked data.

a. **Distortive Attack**: This is an attack where an intruder tries to apply distortion techniques to manipulate the watermark. It can't be extracted properly, thus making the watermark unidentifiable for further use.
b. **Subtractive Attack**: This is an attack where the malicious user tries to extract the location and presence of a watermark to manipulate it.
c. **Filtering**: This is an attack where Low-pass filtering directly impacts the performance of watermarked images, videos especially when it is applied to high-frequency spectral contents
d. **Cropping**: The most common where an intruder removes a specific part of the video or images to make sure owner identification is missing from the digital content is known as cropping attack. An example of this attack is mentioned in figure1.1.
e. **Compression**: It is a form of unintentional attack where videos and images are mostly distributed in compressed form, and insertion in compressed videos poses a good deal of quality to the watermarked video.

1.4 Application of Watermarking

The applications for Watermarking are illustrated in table 1.1

Table 1.1: Applications of Watermarking

SNO	Applications	Function
1	**Broadcasting**	Real-Time embedding of a watermark in various platforms is gaining a lot of popularity in the field of broadcasting
2	**Video Authentication**	Visible and Invisible Watermarks are used in videos of many streaming sites in the application of video authentication.
3	**Copy control**	The addition of copy does it prohibit bit to multimedia data to avoid it from getting copied anywhere.

1.5 Basic terminology to design Watermarking system

The design of the watermarking system is dependent on the following aspects:

a) **Imperceptibility:** The process calculates the degree of invisibility of hidden signals to the user. The main aim is to embed the watermark in inconspicuous areas to avoid any detection of the watermark.

b) **Robustness:** This property verifies watermark ability to survive attacks such as cropping, resizing, and additional noise.

c) **Capacity:** It checks the amount of data(image, text) to be masked inside videos.

d) **Security:** It provides an encryption mechanism to multimedia data.

1.6 Frame Selection and Optimization

Videos are the most attacked multimedia data. The video is a collection of several frames. The watermark can't be embedded on every frame because it increases the possibility of identifying the video's watermark presence. The frame Selection mechanism is fundamental in the proposed work. The watermark embedding process follows after the frame selection process. A secured video watermarking technique must be embedded on selected frames only as embedding in all frames will be a time-consuming task and not a secured method. The frame selection is crucial in finding the correct number of frames in which the watermark will be embedded. Frame selection can be made using fuzzy logic and scene change detection. The proposed frame selection mechanism is implemented using a scene change detection mechanism. Adding a watermark to the multimedia introduces the challenge of quality loss. The watermark embedding can be done directly but may not result in good quality of watermarked data, and there are many optimal algorithms proposed that optimize the embedding factor. The optimization algorithms take quality parameters into the count and further optimizes the embedding factor using certain fitness functions. Table1.2 represents existing frame selection and optimization techniques for frame selection and watermark embedding. The optimization algorithms help in improving the performance of the watermark embedding factor. The embedding factor helps in mixing the watermark with an image. Most of the researchers are using metaheuristic approaches, machine learning concepts to optimize the data. Optimization algorithms also provide the criteria to select the optimal number of frames from the video. Most of these optimization algorithms and artificial intelligence algorithms include Particle Swarm Optimization, Genetic Algorithm, Ant Colony Optimization, Cuckoo Search, Grey Wolf Optimization, Artificial Neural Network, Back Propagation Neural Network, etc.

Table1.2:Frame Selection and optimization techniques

Name	Characteristics	Advantages	Disadvantages
Genetic Algorithm	It optimizes the performance of the predictive model.	Can manage data sets with many features; Can be easily used in parallel systems.	Expensive in computational terms; Take more extended time to converge.
Particle Swarm Optimization	It is a metaheuristic technique that makes assumptions about the problem and optimizes the solution by updating the particle's position.	Parallel Computation; Robust; Easy to implement; Few parameters to adjust; Shorter computation time; Accurate mathematical model.	Initial design pattern challenging to design; Problem of scattering.
Fuzzy Logic Control	Analyze analog input value in terms of logic variables ranges from 0 to 1; Use human expertise to design a controller.	Cheaper; Robust; Efficient; Reliable; Emulate deductive thinking.	Large data sets are required; Needs high human expertise; Regular updating of rules are required.
Artificial Neural Networks	Based on a biological neural network where information flow affects the network.	Vital information about the entire network; Ability to work with the incomplete network; Parallel processing capability.	Hardware dependence; Unexplained behavior; Unknown duration.
BAT	Metaheuristic algorithm on	Handle multi-model problems efficiently; Swift convergence	Lack of good exploration ability; Require improvement

	echolocation behavior of bats	rate; Ability to use as a global and local optimizer; To form diversity of solution in difficulties.	in the technique to allow acceleration of convergence rate
Grey Wolf Optimization	The population-based meta-heuristic technique that simulates leadership hierarchy for decision making among wolves.	Simpler Structure; Low computational requirements; Fewer Decision variables.	Low solving accuracy; Bad local searching ability.
Cuckoo Search	Finding the best solution amongst the possible solution and carry forward that in further steps.	Easy to implement; One Single parameter; Speed up convergence Simplicity.	Bad Accuracy; Easiness to fall into the optimal local value.
Back Propagation Neural Network	Supervised learning algorithm used to train ANN.	Fast; Accurate; No parameters to tune except input; No prior knowledge is required.	Dependency on input data; Sensitivity to noisy data.
Bi Direction Extreme Learning Machine	The two-layer neural network is based on two layers where one is random and the second is trained.	Fast learning Algorithm; Good generalization.	Accuracy of results; Performance incompatibility with other neural networks.

1.7 Various encryption standards applied on watermarking videos

There are many encryption standards proposed along with various techniques like DCT, DWT, and DFT. Some of the standards have been listed and used in previous work. Encryption is a crucial step towards the security of the watermarking scheme. The encryption algorithms are not applied on selected frames directly, as using the encryption algorithm increases the time complexity of the algorithm. Table 1.3 represents a brief description of different types of encryption algorithms used over the years.

Table 1.3: Various Encryption and Security Techniques used in Watermarking

SNO	Name	Functionality
1.	**Transposition Cipher**	This type of cipher comes in the category of simple encryption, where the shifting of plain texts is done in some regular pattern to form the ciphertext.
2.	**Rail-Fence Cipher**	It is a form of transposition cipher where plain text is scrambled more straightforwardly, and alphabets are written in a zig-zag manner where individual rows are combined to form the ciphertext.
3.	**AES**	It is termed as Advanced Encryption Standard. It is a cipher used to protect classified data and is used on both hardware and software to encrypt sensitive data.
4.	**DES**	It is known as Data Encryption Standard. It is a cipher that is used to encrypt data in blocks of size 64 bits each.
5.	**RSA**	It is known as Rivest–Shamir–Adleman. It is used for specific security services that enable public-key encryption to secure sensitive data.
6.	**Triple DES**	3DES is an enhancement of DES; it is 64-bit block size with 192 bits key size. It is the same as DES, like DES but is applied three times more to get more encryption.
7.	**Hyperchaotic Encryption**	The Hyper Chaotic Encryption is a modified encryption standard applied to images. It works on predefined values.

1.8 Motivation

The motivation behind conducting the research work is to find a secured technique that can solve the existing problems faced by users nowadays as the issues related to copyright protection and ownership identification are prevalent. Secrecy and Integrity of data are very hard to maintain. Videos are the most manipulated multimedia data across the internet. The intruders are finding various ways to exploit the use of videos without the information of the owner. Unauthorized people have formulated many mechanisms to misuse the data. Invisible watermarking is a technique to hide data inside multimedia without the information of intruder. The addition of a watermark inside the multimedia poses the challenge of quality loss of data. The proposed work aims to solve those problems. There is a requirement for a secured technique that ensures confidentiality and robustness. Literature survey demonstrates many watermarking techniques developed with challenges either related to security or robustness. Figure 1.5 represents the challenges researchers face to design a secured method to counter illegal distribution and quality loss in watermarked data after embedding is done.

Figure 1.5: Challenges in Watermarking

1.9 Problem Formulation

There are many problems existing researchers face while embedding the watermark on videos. This thesis aims to address and solve problems. The research work involves the insertion of a watermark on selected frames of video. The selection of frames is one of the issues discussed in this thesis. The insertion of watermark inside selected frames also poses the challenge of quality loss of watermarked frames. This issue is also addressed in the research. The watermarked content is subjected to specific signal processing attacks to test the property of robustness. So many signal processing attacks are applied deliberately to check the effectiveness of the proposed technique. Thus, this thesis will address some of the following research questions.

RQ1: Why is frame selection an essential step in video watermarking?

- Discussed in section 3.1(Chapter 3)

RQ2: Will the addition of an encryption mechanism increase complexity of the code?

- Discussed in section 4.2 (Chapter 4)

RQ3: What is the impact of the addition of a watermark on the quality of watermarked data?

- Discussed in section 4.3 (Chapter 4)

RQ4: How robustness of the watermarking technique is tested?

- Discussed in section 4.4(Chapter 4)

1.10 Objectives of the Proposed Work

The objectives of the proposed work are as follows:

I. To implement the preprocessing of video to extract frames and find suitable frames for embedding the watermark.

II. To develop an encrypted watermarking technique on the selected frames of video.

III. To apply the proposed technique on selected frames, then compare, analyze, and validate the performance against different attack scenarios based on quality metrics.

1.11 Thesis Contribution

The significant contribution of this thesis is summarized below:

(a) A frame selection procedure is proposed to select the optimal number of frames from the video to be watermarked.

(b) A hybrid watermarking technique is proposed that involved Graph-Based Transform, Singular Value Decomposition, Hyperchaotic Encryption.
(c) The technique is further optimized with Grey Wolf Optimization and Genetic Algorithm to obtain high-quality metrics.
(d) The performance of the proposed technique is evaluated against various signal processing attacks.

1.12 Organization of the thesis

Chapter 1 explains the introduction to the thesis, Problem formulation, Objtives of research ; the rest of the work is structured as follows

Chapter 2 discusses the existing watermarking techniques of multimedia data along with frame selection and optimization techniques. This chapter explains the importance of selecting the frames and the optimization algorithm's role in embedding factor. The research gaps are also addressed in this chapter.

Chapter 3 discusses the methods and materials used in the proposed work. This chapter explains the frame selection procedure used in the research, watermark embedding technique, optimization criteria used in the study, and quality metrics used in the thesis.

Chapter 4 describes the results and discussion along with comparative analysis with existing techniques.

Chapter 5 describes the summary and conclusion of the research

CHAPTER 2

REVIEW OF LITERATURE

This chapter outlines the existing watermarking methods used by researchers in previous years, followed by identifying research gaps.

2.1 Review on existing watermarking Techniques

This section explains the summary of previously conducted work by researchers in past years.

Hartung F.H et al. (1996) [1] presented a robust scheme applied on encoded video, watermark embedding, and detection using the MPEG bitstream. The primary focus is to avoid drift problems. The proposed scheme can be applied on both original and encoded bitstreams that can be used to ensure the transmission of arbitrary binary information of several bytes/second. The proposed research demonstrates the use of a robust watermark embedded in MPEG encoded video that transmits arbitrary binary information at a speed of a few bytes/seconds.

Swanson M. D. et al. (1996) [2] proposed a scheme where major focus is to conceal copyright data in a picture. The plan utilizes visual covering to ensure that the inserted watermark is undetectable and amplifies the hidden part's robustness. The watermark is developed for discretionary picture hinders by sifting a pseudo-commotion succession (creator id) with a channel that approximates the visual framework's recurrence veiling attributes. The commotion like the watermark is factually imperceptible to stop the unapproved evacuation. Exploratory outcomes demonstrate that the watermark is hearty to a few bends, including white and shaded clamors, JPEG coding at various characteristics, and editing.

Cox I. J et al. (1997) [3] proposed a scheme based on multimedia data i.e audio, images, video. The identical distribution of the watermark is presented. It allows use of Gaussian random vectors to be inserted like spread spectrum into most important spectral components. The proposed scheme's major motive allows the watermark to be robust to various geometric attacks like cropping, scaling, and rotation. Watermark detection is done to identify the owner of the video.

Su J.K et al. (1998) [4] proposed a scheme that focuses on developing the methods for watermarking applied to multimedia data to ensure embedding of the watermark is done on original and compressed documents. The degree of performance is measured on the scales of imperceptibility of the watermark. This research also considered many factors that lead to the complexity of embedding and detection of watermarks.

Mohanty S.P et al. (1999) [5] proposed a dual watermarking scheme that focuses on visible and invisible watermarking to achieve copyright protection and ownership identification. Various attacks are applied to test the efficiency of the watermarking scheme.

Zhang J et al. (2001) [6] proposed a watermarking scheme that works on motion vectors to hide copyright information in MPEG videos. Watermark Embedding is done in higher value motion vectors A less angle changed component and modification of motion vectors are done into bitstream where watermark can be retrieved without any problems. Simulation results suggest less degradation in video quality after embedding of watermark and almost no impact on MPEG decoding speed. Results are formed on both compressed and uncompressed video sequences.

Barni et al. (2003) [7] proposed a scheme that allows security mechanisms to overcome real-life problems. The proposed system is robust to all possible attacks. The research is evolved by the Diffie-Helmann's paradigm keeping cryptographic security in mind.

Shieh C.S et al. (2004) [8] proposed a scheme based on a genetic algorithm and various attacks applied to test the system's robustness. Genetic Algorithms are used to optimize certain features. The fitness function in GA is used in parts related to robustness and invisibility. The proposed scheme shows improvement using GA by applying specific attacks and improving image quality by applying GA.

Huang G et al. (2004) [9] proposed another learning calculation called extreme learning machine (ELM) for Single Layer Feed Forward Neural Systems, which haphazardly picks the information loads and systematically decides the yield loads of SLFNs. In principle, this calculation will in general, give the best speculation execution at a very extreme learning speed.

Shen R.M et al. (2005) [10] proposed a scheme that is based on standard support vector regression-based color image watermarking. The proposed method ensures training of support vector regression in embedding and watermark embedding is done into blue channel of host image keeping human visualization system in mind. Watermark extraction is done by applying specific attacks. The proposed method achieves high-quality results in terms of PSNR in comparison with Kutter_s method and Yu_s method against different attacks.

Barni. M et al. (2005) [11] proposed an algorithm that embeds a watermark in each video's frames by analyzing the relationship between some predefined pairs of DCT coefficients in pseudo-randomly macroblocks(MB_s). Equal embedding of the watermark is applied on inter and intra MBS.

Piao C.R et al. (2006) [12] proposed a scheme that is focused on embedding watermark into original image using BPNN and subsequently training the data to obtain characteristic of image. The picture is isolated into 8*8 squares and the average pixel estimation of each square is utilized as the ideal yield estimation of the BPN. The quantized DC coefficient of Discrete Cosine Transform (DCT) space of each square is being used as an information estimation of the BPN to be prepared. After the BPN is prepared utilizing those info/yield esteems, watermark is inserted into the spatial area using the prepared BPN. The prepared BPN additionally utilized in watermark extraction process. The results show high rate of performance measured in robustness and imperceptibility.

Bhattacharya S et al.(2006) [13] performed a survey on available video watermarking techniques by performing comparative analysis on different techniques.

Piao C.R et al. (2006) [14] proposed a scheme that focuses on the embedding of watermark in DWT domain using HVS model and radial basis neural network. Performance of embedding of the watermark is calculated using HVS model. Watermark insertion is done randomly and secret key determines beginning position where embedding of the watermark is done. Any intruder can't remove the watermark. The proposed scheme shows improvement in results after applying various geometric attacks.

Ye.D et al. (2007) [15] proposed a scheme for real-time application applied to MPEG Videos. The major focus was to best watermarking positions where watermarking is supposed to be done, and watermarking was applied using EQSP(equal quantization step position) . The results show vast improvement than previous methods considering various factors- complexity, robustness, and visual quality.

Li. Q et al. (2007) [16] proposed a scheme that is based on hybrid DWT-SVD that decomposes the image into 4 sub-bands, and SVD is applied to each sub-band. Embedding strength is measure in the scheme proposed and improved in previous papers. The proposed method poses advantages in robustness and imperceptibility.

Huang G.B et al. (2007) [17] proposed a technique based on a convex optimization method that improves I-ELM's convergence rate by recalculating the output weights of the existing nodes when a new hidden node is randomly added. The proposed method works on the parameters of SLFNs which will be determined by ELM instead of backpropagation.

Wang. P et al. (2008) [18] proposed a novel digital video watermarking scheme that allows the application of motion vectors of P frame from the video. The proposed scheme's major focus is to resist the rotating attack that allows only half of the points in the frame to be search effectively. Copyright information is hidden using the motion vectors scheme. Every macroblock searches the best match block in special region by a watermark in the encoding process and every motion vector carries the decoding process. The results are calculated using PSNR and do not impact video bit rate and quality after embedding the watermark.

Choi D et al. (2010) [19] proposed a novel watermarking scheme given the perception that low-recurrence DCT coefficients of a picture are less influenced by geometric processing. Another visually impaired MPEG-2 video watermarking is presented to address the quality loss of data.

Mehta. R et al. (2010) [20] proposed a method based on FNSVR used for embedding and extraction of the watermark in 8-bit greyscale cover images. Embedding is done in a shorter duration using the proposed method. Results indicate higher values of PSNR of signed images, and results show the proposed plan will have less computation time.

Wu.C et al. (2011) [21] proposed a flexible particle swarm optimization (PSO) technique imposed on compressed video with codec H.264/AVC. A variety of attacks have been employed on this technique to check robustness. The primary focus was on the video's imperceptibility and ensuring that PSO was applied on certain requirements and improved the proposed scheme's robustness.

Jiang M et al.(2011) [22] proposed a practical video watermarking scheme by using a compressed video stream to embed a watermark inside it using DC coefficients of block image. Synchronization code is used to solve the synchronization problem. Practical results indicate better performance of proposed scheme considering low rate of MPEG compression and variety of attacks.

Su. P et al.(2011)[23] proposed a scheme on H.264/AVC compressed videos. Watermark is embedded into nonzero quantization indices of frames to achieve good data size. The major focus is to calculate distortion resilient hash that addresses the synchronized watermark issues that will help in watermark sequence. The proposed scheme is aimed to solve encoding process attacks.

Cheung et al. (2011)[24] proposed a hybrid technique based on Graph-Based Transform and Transform Domain Sparsification to detect prominent edges and identify sparse depth signal in the DCT domain. The main aim of the research is to depth map errors. GBT is used for detecting edges and avoiding filtering attacks. The results indicate that the proposed technique outperforms other individual methods.

Wang Y.R et al. (2011) [25] proposed robust watermarking by embedding PSO technique in the wavelet domain to ensure robustness and imperceptibility of watermarking. PSO is fused with the method proposed to avoid potential insecurity in previous research in the proposed method. Here the fixed block size in one sub-band is used, and the permutation is unable to guess which coefficients constitute a block. The proposed work allows the coefficients to be selected randomly from different sub-bands to hide the block. The proposed algorithm gives a better result than SDWCQ, where PSO is not used.

Sharma C et al.(2012) [26] proposed an efficient DWT watermarking scheme applied on images for quality loss. Embedding of watermark poses the challenge of quality loss.

Lee M.J et al. (2012) [27] proposed a scheme focused on designing a robust watermarking system against many attacks and is applicable on a compressed domain. Videos are viewed in lower resolution and in an encoded form that makes watermarking embedding easy but hampers the quality of the obtained video. Other algorithms can't survive the encoding attacks. Still, the proposed work survives by extracting low-frequency coefficients of frames by partly decoding videos and proper quantization index modulation scheme to embed and detect the watermark. The simulation results justify real-time requirements and robustness to ensure copyright protection.

T. Tabassum et al. (2012)[28] proposed a method of extraction of frames from the host video. Then from each video shot one video, frame selection is carried out identically. The identical frame's decomposition is done into 3-level DWT, followed by selecting higher sub-band coefficients to embed the watermark to coefficients to ensure the watermark's perceptual invisibility. NC between the original video and watermarked video is calculated and compared with a threshold value from the embedded watermark signal. The results indicate that the proposed scheme has strong PSNR values against image processing attacks like cropping, salt and pepper, frame dropping etc.

Yang Y et al. (2012) [29] proposed a work based on Bidirectional ELM where hidden nodes are not randomly selected. A relationship is found out between network output error and network output weights. The simulation results measure bidirectional ELM performance and conclude it works about 100 times better than incremental ELM Algorithms.

Huang G.-B et al. (2012) [30] proposed a technique based on least square support vector machine and proximal support vector machine that has broadly utilized parallel characterization applications. Results indicate that ELM has more versatility and quick learning technique compared to the other methods.

Chaudhary V et al. (2012) [31] proposed a scheme that is based on the Least squares support vector method and the proposed method is applied on grey-scale images using DCT Domain. The proposed method intends to solve Quadratic Programming (QP), which makes the problem costly. The major focus is to solve linear equations that make the system perform at faster rate. Embedding of the watermark is done in 3 different grayscale images in less period and good values of PSNR values.

Ramamurthy N et al. (2012) [32] proposed a robust digital image watermarking technique based on BPNN in DWT domain. The host image is divided into 4-levels using DWT. The bitmap of size 64x64 is selected as a watermark. BPN optimizes in a way to achieve fast convergence and high accuracy. The proposed watermarking algorithm is robust to all image processing attacks.

He Y et al. (2012) [33] proposed a scheme that focuses on a real-time dual algorithm applied on H.264/AVC for Video On Demand Service. Watermarking is embedding is done into the first non zero coefficients of Intra 4*4 coded blocks. It uses error code mechanism at the same step only to avoid distortion caused by quantization and watermarking embedding.

Faragallah O.S et al. (2013) [34] proposed a scheme that presents an efficient, robust, intangible video watermarking method dependent on singular value decomposition (SVD) performed in DWT domain. Transformation with DWT of video frames is done in 2 levels. HH band and Middle-frequency bands LH and HL are transformed using SVD. 2 Improvements are highlighted compared to previous work- DWT-based SVD using additive method results in cascade of 2 powerful transforms together. Error correction code is applied and embeds the watermark in temporal redundancy and the proposed technique is robust to various processing attacks.

Singh T.M et al. (2013) [35] proposed a scheme using SLFN right now known as Extreme Learning Machine by calculating its motion vectors in the uncompressed domain. Raw Video is split up into frames and extraction of frames is done of blue component. Maximum motion frames are determined by the block chaining method. Transformation of every frame is done using DCT and these coefficients, which will train ELM. The ELM after training, will produce a normalized output vector to be used as an embedded watermark in the low-frequency DCT coefficients of the frame. Testing of embedding frames is done by calculating PSNR. The resultant video exhibits good visual quality. It results higher value of BSNR and a lower value of BER.

Agarwal C et al. (2013) [36] proposed a scheme that embeds the watermark in binary form into grayscale images by applying the GA-BPN network. The sequence of weighting factor is used by HVC characteristics of the DCT domain and used to embed and extract watermark in the DWT domain. Major focus of the scheme is to consider edge sensitivity, luminance sensitivity, contrast sensitivity. Visual Quality of images is obtained before and after application of attacks and PSNR is obtained accordingly.

Mansoor et al. (2013) [37] proposed a low-complexity symmetric cryptographic algorithm, denoted as Secure Force (SF) to enhance security mechanism.

Mishra A et al. (2014) [38] proposed a scheme that combines functionalities of DWT and SVD. Embedding of the watermark is done in singular values of the LL3 sub-band coefficients of the host image using MSF's(Multiple Scaling factors). Firefly Algorithm is used for optimization by making use of an objective function that linearly combines imperceptibility and robustness. Quality of signed and attacked images yield good quality that ensures a higher value of PSNR .

Mishra A et al. (2014) [39] proposed a work based on raw video watermarking scheme by applying ELM to train the data by computing its motion vectors in uncompressed domain. At First, Video is split up into frames followed by extraction of frames.. Frames having maximum motion vectors get selected. Next, every video frame chosen is transformed using DCT coefficients. The normalized output vector produced by trained ELM will serve as watermarks to be embedded in the low-frequency DCT coefficients of the frame. PSNR is tested with a normal and watermarked frame. High values of PSNR suggest good video quality. High values of NC and low values of BER indicate the effectiveness of machine. The results indicate proposed technique is robust against many compression attacks.

Masoumi M et al. (2014) [40] proposed a new watermarking approach where motion vector is detected and wavelet transformation is applied to obtain 10 sub-bands of wavelet coefficients. Embedding is done by selecting 3rd level of 3D coeffients of HL,LH,HH sub-bands. This technique uses the spread spectrum technique to embed watermark in selected wavelet coefficients. The experimental results show good performance in robustness and transparency where an intruder can't detect watermark. The proposed method is tested against Median Filtering, Gaussian Noise and frame drooping and averaging attacks to measure PSNR.

Agarwal C et al. (2014) [41] proposed a fast and accurate watermarking scheme for three different standard videos using XVID codec in DWT domain by applying Extreme Learning Machine (ELM). The embedding of the watermark is done by using scene detection. The LL4 sub-band coefficients of frames act as a dataset to train the ELM in less amount of time. The output layer of the ELM then embeds a binary watermark in the selected frame of the video. Good quality of output video is produced with good values of PSNR, BER.

Patel B et al. (2014) [42] presented an overview of encryption standards that can be incorporated with various watermarking techniques in the field of speech.

Gange S et al. (2014) [43] presented a set of security and copyright protection techniques that can be applied on digital media to provide advanced security mechanisms.

Ali M et al. (2014) [44] proposed an innovative watermarking scheme based on the transform domain. Using SVD-DWT- embedding and extraction is done. Embedding into host image is done and then transformed into sub-bands of separated frequencies by third-level DWT and then SVD is applied on the low pass and high pass (HH) sub-bands at level third. Scaling of different the Watermark image is done using multiple scaling factors and are imparted into the Singular value matrix of Low pass and high pass sub-bands of the host image to achieve robustness and invisibility. An arbitrary watermark is applied in a lossless manner.

Venugopala P et al. (2014) [45] proposed a scene based detection scheme where blind method is proposed for the extraction of watermark keeping in mind that digital content i.e, images, videos, audios are the most vulnerable content readily available. The proposed watermarking method is used to embed 8 bit plane images using grayscale into different video scenes. It allows the selection of some luminous values applied in various scenes and are divided into groups. The watermark retrieval is done in the extraction stage after processing certain manipulation and signal processing attacks.

Mirjalili et al. (2014) [46] proposed a metaheuristic approach named Grey Wolf Optimization that works with the hierarchy of wolves attacking the prey in different passes. Different types of Wolves are represented in the form of alpha, beta delta and omega. The leadership strategy is implemented by attacking, encircling, and searching the prey. This fitness function is calculated and updated according to the position of prey. The proposed metaheuristic algorithm's performance is testes against existing algorithms such as Particle Swarm Optimization, Evolutionary Programming, Differential Evolution. The proposed algorithm is applied to overcome challenges in real time applications of optical engineering.

Yen C.T et al. (2015) [47] proposed a technique based on the inverse discrete cosine transform technique was utilized to adjust the recurrence of the spatial domain, permitting the host picture to be unmistakable to the human eye. After the decimation procedure, the watermark was most recognizable in a somewhat harmed state, however hard to distinguish in a genuinely harmed state after utilizing the DCT watermarking plan. BPNN algorithm is applied along with DCT watermarking technique on obtained data set from selected frames. The simulation results indicated that most properties of the original image is retained after using certain attacks.

Rajpal A et al. (2015) [48] presented a watermarking scheme using online sequential machine learning is proposed where transformation is done using DWT. A fixed number of training data is used to tune OS-ELM and training data to OS-ELM is constructed by a combination of quantized LL4 sub-band. Embedding is done randomly where 2 binary images are used for the watermark . Results show the similarity between extracted and attacked watermarks and significantly less time is consumed for the embedding process.

Kulkarani Shylesh et al. (2015) [49] presented a hybrid technique that embeds the watermark by using SVD, DWT, Rail-fence and 10's complement. DWT decomposes the image into certain sub-bands and LL1 was chosen. Various attacks have been applied to check the robustness of scheme.

Thind D et al. (2015) [50] proposed a scheme that combines DWT and SVD in high-frequency subbands and various attacks are applied to test the technique's efficiency. The reason for using SVD is to discover similar information throughout transform. The proposed technique outperforms individual methods.

Agarwal C et al. (2015) [51] proposed a scheme is modeled using hybrid Fuzzy-BPN to embed a binary watermark in grayscale images. High values of PSNR and SSIM are obtained. High normalized values of extracted watermarks lead to successful watermark recovery. The proposed scheme obtains high computed values of normalized correlation for attacked images that suggest high robustness and imperceptibility.

B. Sridhar et al. (2016) [52] proposed a wavelet-based enhanced approach robust to certain processing attacks where selected frames are grouped into pixel shares using wavelet that achieve good quality of watermarked image.

Rasti P et al. (2016) [53] proposed a robust watermarking scheme that uses scaling and embedding factors in the wavelet domain to obtain good values of PSNR .

Su Po-Chyi et al. (2016) [54] proposed a watermarking scheme for streaming services where a watermark is embedded into the video stream, which contains video frames, and many attacks are suggested to check the efficiency of the same.

Sharma C et al. (2016) [55] proposed an efficient hybrid watermarking technique based on DWT, SVD and Rail Fence methods that are applied on digital multimedia such as videos, images and various attacks have been used to test the scheme's efficiency.

Rajpal A et al. (2016) [56] presented a multiple Scaling factor-based Semi blind watermarking scheme using online sequential machine learning for grayscale images is proposed where transformation is done using 4 Level DWT. Defined training data is used to tune OS-ELM and training data to OS-ELM is constructed by the combination of quantized LL4 sub-band. Output is a sequence of predicted coefficients that is divided into 3 equal parts. MSF Scheme is used to embed a watermark in a semi-blind manner. Embedding is done randomly where 2 binary images are used for the watermark. Results show very little difference between extracted and attacked watermarks and significantly less time is consumed for the embedding process.

Hou et al. (2016) [57] proposed a graph-based transformer technique to explore two types of correlation: intercorrelation and spatial correlation of set of images. The correlation of images is done to explore human motion data by exploiting Graph-Based Transform. This transform uses an orthogonal matrix for implementation. There is no loss of information after correlation is applied and decorrelation provides better results than other transform domain techniques such as DCT.

Mittal et al. (2016) [58] proposed a modified Grey Wolf Optimization algorithm that overcomes the shortcomings in the previously existing algorithm. The metaheuristic algorithms are analyzed by taking key features like exploitation, exploration and attacking. The comparative analysis is done accordingly and the modified algorithm considered several iterations and provided the right balance amongst them to calculate the global optimum. The proposed mechanism is useful in solving benchmark problems and clustering problems in wireless sensor networks.

Sadi K. et al. (2016) [59] proposed a technique based on frequency domain method discrete cosine transform to embed a watermark in motion vectors to ensure best features are selected for this process. The group of pictures are chosen based on selection criteria, and an additional security mechanism is applied to the scheme to make it robust against various attacks

Mishra A.et al. (2017)[60] presented a scheme that optimizes the MSFs by applying an optimization technique called cuckoo search (CS). The objective function is implemented as a linear combination of visual quality determined by PSNR and robustness determined by NC . Results of PSNR show good values to enhance visual quality. The proposed technique is applied against various processing attacks. Meta Heuristic techniques provide better results than already used methods.

Li et al. (2017)[61] proposed an image encryption algorithm based on multiple chaos that overcomes the problem of low dimensional chaotic map that suffers from the pain of plain text attack. The proposed algorithm works on pixel level and bit-level permutation to provide additional security. The decryption process follows the encryption process. This algorithm is gaining importance in the field of watermarking with the strong cryptosystem it possesses. The analysis shows the proposed technique to be robust and reliable.

Tawhid et al. (2017)[62] proposed the hybrid algorithm involving Grey Wolf Optimization and Genetic Algorithm that employs certain features such as exploration and exploitation, dimensionality reduction, and population partitioning. The proposed algorithm tends to operate faster compared to individual algorithms used. The comparative analysis is done on 8 algorithms to evaluate the performance.

Farri et al. (2018) [63] proposed a video watermarking technique based on integer wavelet transform and chaotic sine map. The proposed scheme embeds watermark in key frames and robustness of the proposed scheme is tested by applying processing attacks to aim high values of quality metrics.

Nouioua et al. (2018) [64] proposed a fast motion frame selection technique and singular value decomposition technique in the multiresolution domain. The proposed method solves the problem of embedding a watermark in every frame. QIM is used for embedding purposes. The validity of the proposed scheme is tested against signal processing attacks. The proposed scheme presents good results against various attack scenarios like filtering, collision, noising, and compression.

Rajpal A. et al. (2018) [65] applied new watermarking technique on MPEG Videos using Bi-directional Extreme Learning Machine. Good Frames to be watermarked by using Fuzzy Inference System. A binary watermark, encrypted by transposition cipher, is used to ensure enhanced security. The proposed Scheme achieves good results against certain attacks.

Sharma C. et al. (2018) [66] applied a hybrid combination of DWT, SVD and Rail Fence on videos. 3 level DWT is applied on frames of the video. The proposed technique is robust against signal processing attacks but suffers from frame selection which is covered in future work.

Gu et al. (2019)[67] proposed a hybrid technique based on Grey Wolf Optimization and Genetic Algorithm that solves the problem of dimensionality reduction by using the opposition-based learning method. The cross-over operation is applied to reduce dimensionality reduction. The problem of local optima is diminished. The comparative analysis is done with existing approaches and this algorithm outperforms the existing methods.

Egilmez et al. (2019)[68] proposed a new class of transform named Graph-Based Transform for video compression that formulates optimization problems and proposed adaptive edge transform and removes signals with sharp edges.

Cao et al. (2019)[69] proposed a secured watermarking technique based on hyperchaotic encryption. Non-motion frames are extracted from the video and the discrete wavelet transform is applied on those frames to get appropriate sub-bands. The proposed technique's performance is calculated using Peak Signal to Noise Ratio, Structural Similarity Index Measure, and Normalized Correlation. The various attacks are applied to test robustness and imperceptibility.

Li et al. (2019)[70] proposed a new color image algorithm on encryption based on the principle of hyperchaotic sequence and scrambling. It involves the conversion of pixel values of a color image into grey code. The sorting of the hyperchaotic sequence is done into the one-dimensional matrix. The ciphertext is also produced by scrambling and matrix transformation.

Wang et al. (2019)[71] proposed an incremental version of Grey Wolf Optimization that uses a faster convergence rate and higher optimal accuracy to calculate fitness function. The proposed algorithm uses the design strategy to solve the problem of local optimum. The Survival of Fittest technique updates wolf pack nature by eliminating R wolfs with very few fitness values. The proposed algorithm is compared with existing algorithms such as differential evolution, Particle Swarm Optimization, Artificial Bee Colony, Cuckoo Search Algorithm and provides faster convergence rate compared to all.

Hammami et al. (2019)[72] proposed a Hybrid watermarking technique based on DWT, SVD in mid-frequency bands. The proposed method is found to be robust against many signal processing attacks.

Hu et al. (2020)[73] proposed the Binary Grey Wolf Optimization technique to optimize binary problems. The proposed technique aims to improve the solution quality by considering time consumption and convergence speed.

Heba Al Nasour et al. (2020)[74] improved Grey Wolf Optimization's searching capability to determine optimized values of Probabilistic Neural Network. This study's main objective was to improve classification precision and provide the solution by maintaining the balance between exploitation and exploration.

Yue et al. (2020) [75] proposed a hybrid algorithm based on the Fireworks algorithm and Grey Wolf Optimization to solve the problem of local optima. The algorithm combines the exploration ability of both algorithms to optimize solutions by setting a balance coefficient. The performance is compared against nine algorithms.

Sharma et al. (2020)[76] conducted a comparative analysis of frequency-domain techniques and optimization algorithms so as to develop novel watermarking techniques. Various frequency domain techniques such as DWT, DCT and DFT are analyzed along with various optimization algorithms such as Ant Colony Optimization, Genetic Algorithm, Grey Wolf Optimization, Firefly Algorithm.

Sang et al. (2020)[77] proposed a robust video watermarking technique combining DCT and DWT and scrambling of video frames using the Arnold algorithm. Embedding of the binary watermark is done using LL sub-bands. Various attacks like Gaussian noise and sharpening attacks have been applied to test the performance of the algorithm.

Begum et al. (2020)[78] reviewed all the existing proposed watermarking technique and provided analysis by considering the performance against various attacks.

Mehta et al. (2020)[79] proposed a novel greyscale image watermarking technique based on Lifting wavelet transform using fuzzy logic rules. The training of input features is done using Lagrangian twin support vector regression. The solution is optimized using a genetic algorithm to improve the robustness of the scheme.

Houby et al. (2020)[80] proposed a hybrid watermarking technique based on Discrete Wavelet Transform and Hadamard Transform. The performance of the technique is optimized using a Genetic Algorithm and Decision Tree. The proposed technique is tested against many signal processing attacks such as blurring, scaling, cropping, and better results in terms of imperceptibility.

Xu et al. (2020)[81] proposed image encryption algorithm based on random walk and hyper chaotic sequence. Permutation operations increase the scrambling effect. The performance analysis is done by comparing the algorithm with existing algorithms.

Yadav et al. (2020)[82] proposed an optimized watermarking technique based on combined transform involving DCT and DWT. The performance of the technique is optimized using Particle Swarm Optimization. The performance of the technique is improved using an optimization mechanism.

Zhu et al. (2020)[83] proposed image encryption technique based on hyperchaotic system from dynamic DNA encoding and scrambling mechanism. The proposed algorithm has certain advantages comparative to other existing algorithms in terms of sensitivity to plaintext.

Shankar et al. (2021)[84] reviewed image security performance by using various watermarking techniques such as DWT, DCT and SVD by taking factors of robustness and imperceptibility.

Kahlessenane et al. (2021)[85] proposed a watermarking approach to protect data in medical images. The frequency-domain techniques have been used in this research to provide security. The proposed technique performs better in terms of imperceptibility and robustness.

Seyyedabbasi et al. (2021)[86] introduced two metaheuristic algorithms to solve the problem of local optima. The proposed algorithm is based on incremental and expanded Grey Wolf Optimization to find solutions faster than normal Grey Wolf Optimization by focusing on algorithm exploration and exploitation abilities.

Qu et al. (2021)[87] proposed an improved visible image watermarking technique based on Gradient Weighted class activation and Just Noticeable Difference. The selection strategy is used to locate parts of image to be watermarked. The greyscale images and colored images are used as data sets separately.

Khare et al. (2021)[88] proposed image watermarking technique based on Discrete Wavelet Transform and Homomorphic Transform and Singular Valued Decomposition. Encryption is done using Arnold Transform and Watermark is embedded into singular values. The proposed technique is tested against various attacks like rotation and sharpening to test the technique's performance.

Negi et al. (2021)[89] presented Grey Wolves' social behavior and its application in complex real time problems by taking exploration and exploitation into consideration.

Sharma et al. (2021)[90] proposed a novel frame selection-based video watermarking technique by combining Graph-Based Transform, Singular Valued Decomposition. The watermark is encrypted by using hyperchaotic encryption before being embedded into selected frames. The frame selection algorithm is proposed in this research based on scene change detection. The proposed embedding technique provides good results in terms of robustness and imperceptibility. The proposed technique's performance is tested by applying certain signal processing attacks such as Gaussian Noise, Sharpening attack Rotation attack. The performance can be improved by applying any optimization algorithm on the embedding factor.

2.2 Comparative analysis of different watermarking techniques

Table 2.1 explains the comparative analysis of various watermarking techniques used so far. Findings from existing research include techniques used; Methodology applied, analysis from that research, and future research scope that leads to researchers to solve existing problems.

Table 2.1: Findings from Techniques, Methodology, Analysis and Future Scope of Existing Research Techniques

Reference	Techniques used	Methodology	Analysis	Future Scope or any Research gaps
[1]	DCT Transformation Technique is used	Watermarking Scheme on MPEG compressed video is produced.	Used Compressed videos instead of uncompressed because it transmits faster	Only H.261 standard was used
[6]	Select inter frames(B or P) to embed watermark by using intra watermark decision scheme. No wavelet is used, Decoding and Encoding process only	A large Motion vector is used to embed the watermark. It is modified to the bitstream, where information can be easily retrieved.	Good Decoding speed, Good Inter frame selection.	No Security
[8]	DCT with GA	Image is transformed to 8*8 Blocks after DCT is applied, Training of Frequency bands is done by Genetic Algorithm; Embedding is done along with the secured feature of the pseudo-random cipher.	Use frequency bands for insertion; good results against different attacks	Vulnerable to Cropping attack, which is addressed in future research
[10]	LSB with SVR	Permute the watermark using random position	Watermark is embedded into the	LSB can never give good results

		selection followed by training using SVR for reference position to Embed watermark and extract it	blue channel based on SVR Training.	
[12]	DCT with BPNN	Image converted to 8*8 block then DCT is applied followed by quantization followed by BPNN then watermark insertion and extraction is done	QIM is applied on DCT (dc) coefficient; Neural Network Applied on DCT Domain3	Security is missing
[13]	DCT,DWT,DFT and FFT	DCT, Spread Spectrum, JAWS, CDMA, Region-based energy Modification	Good analysis of the techniques is done against various attack scenarios.	Analysis on results
[14]	DWT with RBF	DWT is applied after that selection of the beginning position of watermark embedding is done, then Quantization of DWT followed by using RBF Extraction.	Good quality watermarked image is produced	Time-Consuming to embed the watermark
[15]	Watermark embedded in Spatial DCT Coefficients in the macroblock.	Block Classification-High-Level Texture blocks have an excellent visual making impact to Human eyes. They are identified as they are	Motion Vectors are considered as reference parameters. Original MPEG video is converted into	Improved video watermarking with proper Feature selection can be the best option

		divided into flat and texture blocks classified into edge and detailed blocks. Detailed Block will give better results. Embedding is done via Redundancy Style: Local and Global Redundancy	bitstreams. Chosen blocks of frames combined with a watermark to form watermarked streams. Classifying the detailed texture block is the critical factor. Random Extraction of Frames is implemented. A highly Detailed texture block for embedding watermark gives high values of PSNR than other blocks. Exclusion of edge texture block-Edge effects are removed. Achieve Less BER than LU Method.	
[16]	Embedding is done using DWT-SVD and optimal matrix decomposition technique	DWT-SVD image is taken	Robustness	Security

[18]	Region Information of Motion Vector	The best Possible macroblock was chosen to embed a watermark Embedding, the scrambling of the watermark is done Fast search algorithm was chosen to find the best possible macroblock	Bit rates are increased slightly after adding watermark	Video quality affects slightly
[19]	DCT	Applies DCT to embed watermark by limiting embedding capacity To avoid both drift and extra complexity, we embed a watermark in B Frames. U Domain is chosen from YUV. B Frame is determined to retain higher energy. The synchronization pattern is retained after every 400 frames.	Increase in Bit Rate from 1-5 %; An advantage over other methods	Can further reduce complexity in b frame
[20]	DCT with FNSVR	Image is decomposed to 8*8 Blocks, DCT is applied to get Zig Zag Scan after that Data Set is trained using FN-SVR to get output vector and Embedding of the watermark, Inverse DCT	Good Insertion and Extraction	Security is missing

		is done to get the watermarked image.		
[21]	PSO Based watermarking scheme with dither modulation	Frames divided into macroblocks(Inter and Intra Frames) DCT is applied, followed by Scanning of coefficients using a zigzag manner. Selection of Coefficient using PSO. A pseudo-Random key is used. Embedding using Dither Modulation followed by the extraction process	Good values of PSNR; Better than GA; Applicable to H.263	Keys must be placed in a secured location H.264 can be applied
[22]	Watermarking embedding is done using DCT and PCM	The watermark embedding is done directly on DPCM to generate DCT DC Coefficients after that; frames are processed in macroblocks followed by DCT, Quantization, Entropy coding, motion compensation, and Extraction.	Watermark Extraction can be done in random duration; insertion is done after 8 seconds(setting up the time frame); Good Robustness; Synchronization code added as a security feature	Additional Security can be imposed
[27]	DCT	Employ QIM technique on Low-frequency coefficients. Encoding is done to create	Analysis of both compressed and uncompressed videos is performed.	Modifying Low-Frequency coefficients in uncompressed domain poses a

		watermarked videos. The quantization step is applied in DCT to check the robustness		challenge of Flickering and Robustness against Rotation.
[28]	3 Level DWT is applied	Frames Divided into shots Identical frames are targeted, Intensity is calculated as I=0.299R+0.587G+0.114B Blue channel has characteristics of High-Frequency range and Embedding is done to achieve high imperceptibility.	Strong robustness against cropping, Gaussian Noise	Time Complexity is an issue
[33]	Selection using CDMA, Embedding using DCT	CDMA for Preprocessing DCT For Embedding AC Coefficients are used. The proposed technique used P Frames to Embed information and Check the Number of Non-Zero Coefficients and P has less non zero coefficients	Randomly extract frames before and after watermarking and evaluate the performance	Full decoding is not possible and low computational complexity
[34]	Hybrid DWT-SVD was applied.	Video is converted to frames after that conversion of Frame is	Robustness is calculated by applying attacks;	The security feature is missing

		done from RGB to YC_bC_r; Luminance is transformed to Level2 DWT SVD is applied. Bit Error Correction Mechanism is applied. Embed watermark Extract it. The binary image was used as a watermark; 2D DWT-SVD was applied ; High and Middle-Frequency bands were tested, Watermark embedded in diogonal Matrix	Computationally less demanding; Different parts of the single watermark is applied to different scenes; Good performance against scaling.	
[36]	DWT, GA, and BPNN Of grey images	The watermark is embedded into a greyscale image using hybrid GA-BPNN. The weight factor is used to embed and extract the watermark. Training done with 27 inference rules.	Luminance, Edge and Contrast Sensitivity are considered. The similarity between original, watermarked image is viewed; Outperforms GA and BPNN both	Security feature
[39]	Watermark is embedded on the low frequency of DCT	Uncompressed video is taken. SLFN is known as ELM in Motioned vectors of the uncompressed	High Normalization correlation and Low Bit Error Rate. Time taken for scanning is	No Security is considered; adding security could also

	Coefficients, Training of data is done using ELM	domain using Block Matching, Extraction of Frames from the blue component. Maximum motion is determined by the block matching method. The selected frame is transformed using DCT, which used to train ELM .	milliseconds to seconds for entire video	affect results in the computation
[40]	Frame Selection Technique is proposed, followed by frequency-domain technique.	Frame Extraction is done by considering motioned part as motionless are not imperceptible; scene Change Detection is avoided as it is not suitable for rapid change of scene. It demands different algorithms for embedding and extracting. Detection of Motion part is done using Green Channel. HVS is less sensitive to motioned part.	Good Security; Better results; Robust against compression	Complexity is increased by encrypting the watermark
[44]	3 Level DWT and SVD is applied.	Watermark Embedding followed by Finding Optimal Scaling factors by DE(genetic algorithm)	To overcome false-positive algorithm binary watermark is applied using lossless manner	Large Computation time makes it nonfeasible

[45]	DCT using Scene Change detection	Luminous value is selected to embed watermark inside it ; greyscale watermark is used by converting into 8-bit plane images into one scene and other for different scenes; decided channel is divided into 8*8 Blocks	Multiple watermarks in locations ensure most of the watermarks getting protected	Robustness can be improved using Audio watermarks.
[47]	DCT with BPNN	3 layer BPNN has been used for watermarking and selected Image is firstly converted to DCT then watermark embedding is done using BPNN	Salt and Pepper Noise, Gaussian noise Random testing is done using NN	Can Work better in Gaussian and Salt &Pepper Noise
[48]	OS ELM with DWT based on SLFN on Colored	The proposed method targets the Blue Channel, followed by applying 4 level DWT; then, Quantization is performed, followed by training data set using OS ELM.	Can fulfill real-time constraints. OSELM is better than soft computing techniques because they don’t satisfy time complexity constraints	Security
[51]	DWT with Fuzzy BPNN	An input image is divided into 8*8 DCT blocks to get edge Sensitivity, Brightness sensitivity, and luminance sensitivity.	Applied on Grey Scale Images; High Values of PSNR and SSIM; High Computed value of NC	Security

		Train using Fuzzy rules, Apply NN with it and apply permuted watermark, apply 3 level DWTand Embed permuted watermark to get the watermarked image		
[56]	OS ELM with DWT based on SLFN on Gray Scale	Blue Channel of the frame is targetted after that 4 level DWT is applied, followed by Quantization, Training data set using OS ELM. Selection of starting location is done using a secret key.	Can fulfill real-time constraints. OSELM is better than soft computing techniques because they don't satisfy time complexity constraints	Security
[63]	Integer Wavelet Transform, Singular Value Decomposition and General chaotic sine map	Embedding is done using IWT, SVD into low frequency components on selected key frames.	High PSNR values against signal processing attacks.	Additional Security feature is missing.
[64]	Fast Motion Frame Selection Technique along with SVD and MR SVD	Frame Selection is made by rapid motion detection of frames, and embedding is done using QIM and SVD.	Lesser number of frames getting selected; embedding scheme is fast and good results against various signal processing attacks.	High values of quality metrics can be produced.

[65]	Bi-Directional ELM, Fuzzy Selection, DWT, transposition cipher	Video is converted to frames; Fuzzy frame selection procedure is followed then train using bi-directional ELM then embed using DWT and transposition cipher	Less Complexity in time	More security can be addressed And Low values of PSNR
[69]	DWT, Hyperchaotic sequence.	Frame Selection is applied using Shot boundary detection, which further finds nonmotion frames to be watermarked. Discrete Wavelet Transform is used for Embedding purpose.	Fast Approach and provides good results against signal processing attacks	An optimization algorithm is missing.
[77]	Hybrid Combination of DCT-DWT is applied on the Selected frame of video	The Video watermarking is done using hybrid DCT-DWT Transform. Performance is tested against various attacks	Fast Approach and good results against attacks.	Optimization algorithms can be added to increase the performance of embedding factor
[79]	Lifting Wavelet Transform is applied with the Genetic Algorithm.	LWT is applied to selected portions on image and performance of embedding factor's image and performance are optimized using genetic algorithm and training of data is obtained using LTSVR.	Provides good results in robustness and imperceptibility	Embedding factor can be optimized with other algorithms apart from genetic algorithm to increase the proposed scheme's performance.

[82]	Hybrid Combination of DCT, DWT, PSO is applied	The image watermarking technique is proposed using DCT-DWT and PSO.	The embedding factor is optimized using PSO	Can produce better results in colored images.
[90]	GBT-SVD-HyperChaotic Encryption	The frame selection approach is done using scene change detection followed by encrypted watermark embedding using Graph-Based Transform, Singular Valued Decomposition, and Hyper Chaotic Encryption.	Fast Approach and Good Results in terms of Time Complexity	Optimization can be added to the embedding factor to improve the quality of the watermarked frame.

Table 2.2 explains the comparison of existing transform domain techniques such as Spatial and Frequency Domain Techniques. It is studied that spatial domain techniques are vulnerable to attacks and not imperceptible. That is why most of the researchers are using Frequency-domain techniques for watermark embedding.

Table 2.2: Comparison Analysis of Existing Transform Techniques

Domain Transform Techniques	Robustness	Complexity	Transient Signal changes	Edge adaptive transform	Real-Time Application
LSB	×	×	×	×	×
DWT	✓	✓	✓	×	✓
DCT	✓	✓	✓	×	✓
DFT	✓	✓	✓	×	✓
SVD	✓	✓	✓	×	✓
GBT	✓	✓	✓	✓	✓

From table 2.2, the time complexity is defined as the amount of time for a watermark to be embedded on a selected frame. Spatial domain techniques such as LSB has very little time complexity but they are not robust as the quality is impacted after the insertion of a watermark but frequency domain techniques such as DCT, DWT, and GBT have high robustness after the embedding of the watermark.

2.3 Research Gaps

I. Rajpal's work [65] is focused on fuzzy inference systems and bi-directional ELM. After testing with all the possible neural networks and various feature selection features. It cannot generate high values of quality metrics with an uncompressed video that impacts imperceptibility and robustness. Our work will solve that problem by proposing a technique that takes care of quality loss after embedding.

II. Most researchers use transposition ciphers to encrypt the watermark as perfect encryption algorithms such as AES and DES increase the code's complexity. Even transposition ciphers used in various research do not offer the good security of watermarked data. This problem has been solved in this research.

III. The frame Selection procedure used by various researchers [14,22,28,34,45,56,65] is time-consuming; this research will solve the time complexity of frame selection.

IV. Most research is conducted on wavelet transforms such as DCT, DWT, DFT for watermark embedding. These are good techniques but not as effective as edge adaptive transforms adopted in the international standard of videos.

V. Optimization of embedding factor is done using various methods such as Back Propagation Neural Network, Bi-directional Extreme Learning Machine, Particle Swarm Optimization, Grey Wolf Optimization, Genetic Algorithm, etc. Some researchers have used combined optimization algorithms to get high-value quality metrics that can be time-consuming. This thesis's significant gap is to utilize the optimization of embedding factor by taking only essential features of a hybrid algorithm.

CHAPTER 3

MATERIALS AND METHODS

This chapter explains the proposed methodology used for this research. The process of frame selection, followed by the embedding of encrypted watermark and various quality metrics, are discussed in this chapter

3.1 Frame Extraction and Selection

The First phase in the proposed work is to perform the preprocessing of video to extract the number of frames and find the suitable number of frames from extracted frames. The process of finding suitable frames in real-time is done using scene change detection. The proposed work has applied frame selection techniques on compressed domain video. The watermark can't be embedded in all extracted frames because adding a watermark will significantly increase the video's bit rate, affecting the processing time and increasing the video's size. So, frame selection is crucial to decide which optimal frames are selected. Frame selection will depend upon motioned and motionless frames; the selection criteria for a frame depending on the video's variations. More significant changes in the video will have a higher number of frames getting selected. Frame selection using a key has been conducted in most studies, but it does not serve as the best frame selection method. The comparison of adjacent frames is made to find frame difference which is calculated in equation 1. RGB to the grey color conversion of adjacent frames is done and the absolute difference amongst the frames is calculated using the histogram method. The different groups of similar images are made. The frame difference's value will decide whether the frame will be considered the part of the same group or a different group. If the difference is large, then it will be regarded as part of a diverse group. The decision parameter will be taken as a threshold calculated in equation 2; if the frame difference is higher than the threshold, the next frame will be the next group. This technique is fast and provides better results than research done by Sharma [66] where random frame selection was done

$$F_k=\sum_{K=1}^{T} H_k(m)-H_k(m+1) \qquad (1)$$

F_k represents frame difference, and H_k is the histogram value of a k^{th} frame of level m, and T denoting the number of histogram levels. The proposed work focuses on the importance of histogram difference;

the selection of frames is made based on the difference represented in equation 1. The frames with less difference than the value of threshold can't be chosen, but the frames representing the large histograms difference value are selected in the next group. The Threshold is maintained to detect intensity histogram difference to calculate sudden transition amongst frames (to find more considerable frame difference). This Scenario is expressed as:

$$M_b = \sigma + \alpha\mu \tag{2}$$

M_b= Threshold Value

σ and μ represent the standard deviation and mean values of selected frame intensity histogram differences. α factor varies from 1 to 6; in our research, we have taken this value as 1.8. The process is carried by applying a timer on the given video to select frames that run until the video. The criteria of frame selection depend upon the comparison of F_k with M_b. Algorithm1 for frame selection is given below:

Algorithm 1: Frame Selection Algorithm

Input: T← No of Frames, M←Mean(T), S←Std Deviation(T)
M_b←M+ αS(Equation-2)
F_k← Frame Difference (Equation -1)
Output: Selected(T)
Begin
(1) for i← 1 to T
(2) {
(3) Read (T) and Store in variables
(4) Compute the difference amongst Frames and Store in F_k
(5) if (F_k>M_b)
(6) {
(7) Select and group them
(8) Apply random key amongst frames from different groups
(9) Write Frames to the Disk
(10) }
(11) }
End

The frame selection procedure is represented in Figure 3.1, where several frames get extracted from the video. The grouping is done based on frame difference. Single Frame is selected from a group; after that, a watermark embedding process is carried out. The number of similar images are shown in figure 3.1; different groups of similar images are represented, selection of similar images is made as per threshold comparison with frame difference.

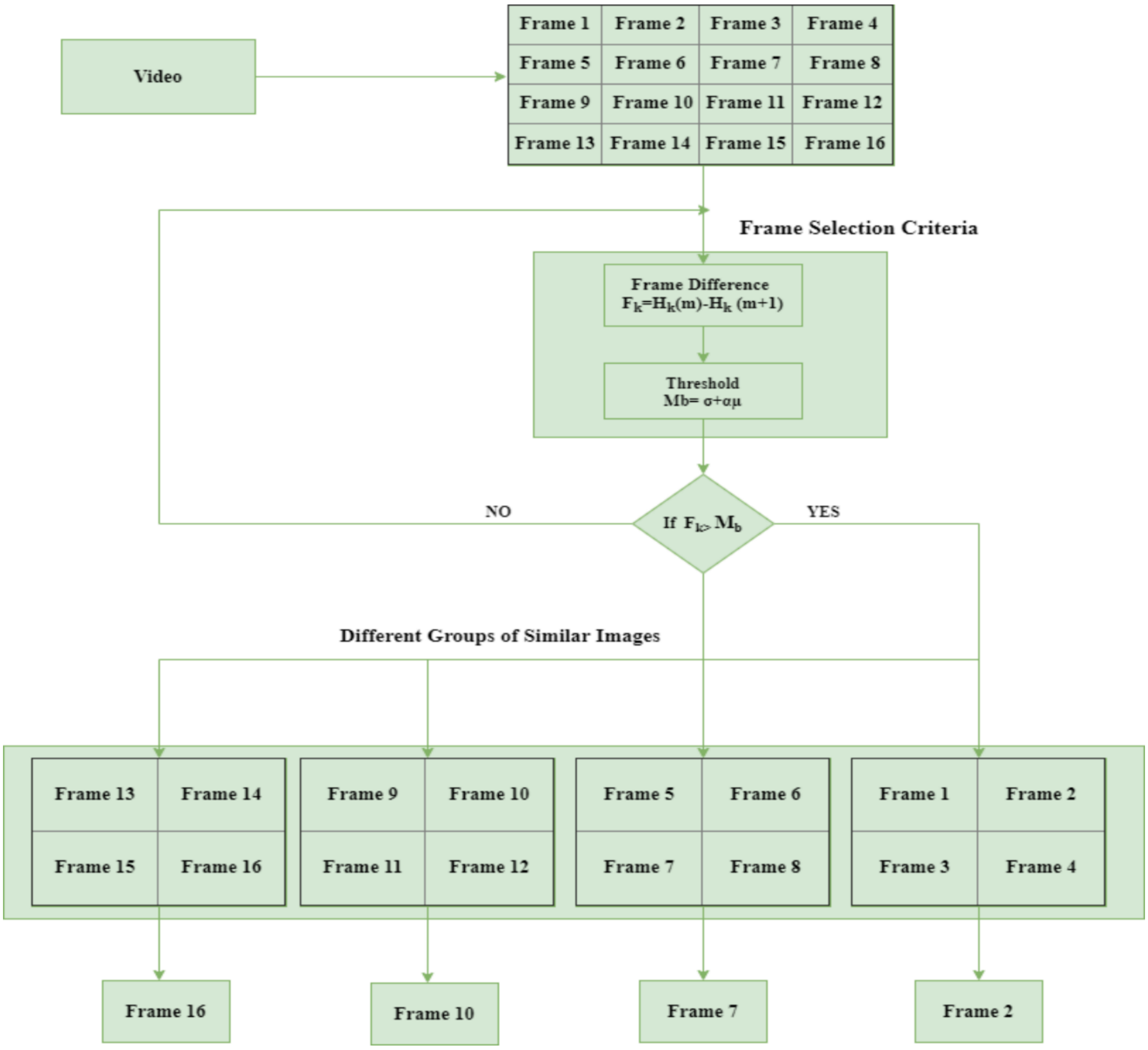


Figure 3.1: Frame Selection Procedure

3.2 Embedding of Watermark

The next step after the selection of frames is to embed the watermark on those frames. Watermark is not applied directly to the frame; the frame's transformation is done before embedding. Most research is done on frequency domain methods such as DWT, DCT for transforming the frame; the techniques are not good enough to handle adaptive edge transformations. Every frame chosen has its property, so the target is to embed a watermark to obtain high-quality metrics values. That is why the proposed technique in this thesis focuses on transforming the frame into a Graph-based transform followed by SVD. Singular Value Decomposition is used as it provides good results against compression attacks.

The embedding factor offers the value to mix the watermark with the selected frame. The combined approach of GBT-SVD does provide good values of quality metrics where value is chosen randomly. The optimization algorithms improve the performance of embedding factors using various steps. The performance of the proposed technique is evaluated after signal processing attacks to the watermarked frame. Most of the research on the watermark's embedding is done using Discrete Wavelet Transform and Discrete Cosine Transform. But the proposed method presented in this thesis is a hybrid combination of Graph-Based Transform, Singular Value Decomposition, and hybrid optimization technique involving Grey Wolf Optimization and Genetic Algorithm. Watermark will not be applied directly; it will be encrypted before embedding.

The embedding technique is explained in the following sections. The proposed work applies Graph-Based Transform followed by Singular Value Decomposition on selected frames. Graph-Based Transform (GBT) transforms the image signal into a graph signal and adapts the image's signal structure. SVD is used for the decomposition of the matrix. This section introduces a novel embedding technique based on the combination of GBT and SVD, further optimized by the hybrid algorithm of Grey Wolf Optimization and Genetic Algorithm. The additional security feature is given in section 3.2.4, based on hyperchaotic encryption, which adds to the proposed technique's functionality. The embedding of the encrypted watermark is presented in further sub-sections.

3.2.1 Graph-Based Transform

There are three steps in Graph-Based Transform while processing the image: the first step involves edge detection on a block. The second step is to generate a graph from pixels from the edge map. The third step is to construct a transformation matrix from the generated graph. In the first step, detection of edges is done in residual block based on the difference with neighboring blocks using threshold technique. Generation of binary edge map is done for the construction of transformation matrix. In the second step, the graph node represents each pixel position; the neighboring node is connected by 8-connectivity, and the adjacency matrix is formed, presented in equation 3. Adjacency matrix computes degree matrix given in equation 4. In the third step, the Laplacian matrix is computed as T and K's difference calculated in equation 3,4. Graph G is projected on eigenvectors of L to perform spectral decomposition and the transformation matrix can be constructed from eigenvectors of the Laplacian matrix. Graph-Based Transform is a transform represented by G={V,E,s} where V and E are the vertices and edges of the graph, and *s* represents the frame signal for graph G

$$T(m,n) = \begin{Bmatrix} \sum T_{m,n} \ if \ \mathrm{m} = n \\ 0 \ otherwise \end{Bmatrix} \tag{3}$$

Where $T_{m,n}$ represents the weight of the edge. The degree matrix $D\epsilon N\times N$ is a diagonal matrix

$$K(m,n)=\begin{cases}\sum T_{m,n} \ if \ \mathrm{m}=n \\ 0 \ otherwise\end{cases} \tag{4}$$

Then, the Laplacian-Graph Matrix L would be defined as,

$$L = T - K \tag{5}$$

Where the operator L is also known as Kirchhoff operator and T is the adjacency matrix. Eigen Value decomposition is represented by eigenvalues $\boldsymbol{\Lambda}=\{\boldsymbol{\lambda}1,\boldsymbol{\lambda}2,\ldots.\boldsymbol{\lambda N}\}$, orthogonal eigenvectors are represented by $\mathbf{V}=\{v1\ldots.vN\}$, derived as,

$$L = V\Lambda V^T \tag{6}$$

Decorrelation of the signal defined on the graph is done using eigenvectors.

$$C = V^T s \tag{7}$$

3.2.2 Singular Value Decomposition

Singular Value Decomposition is a transform in which a matrix is decomposed into three matrices having the same size as the original matrix. GBT Matrix will be transformed into 3 matrices given in equation 3 (E, S,R) where S value will be picked for combining with watermark S value as it will be resit many changes and signal processing attacks. SVD will be applied to the watermark as well. S value is picked because it is a diagonal matrix and it is unaffected after watermark embedding is done using S value of the watermark.

$$A = E_A * S_A * (R_A)^T = \sum_{i=1}^{r} E_i * S_i * (R_i)^T \tag{8}$$

$E_A = [e_1, e_2, e_3 \ldots . e_N]$

$R_A = [r_1, r_2 \ldots \ldots . r_N]$

$$S_y = \begin{pmatrix} S_1 & \cdots & N \\ \vdots & \ddots & \vdots \\ 0 & \cdots & S_N \end{pmatrix} \tag{9}$$

$$A = ESR^T \tag{10}$$

$$K'(i,j) = K(i,j) + \alpha W(i,j) \tag{11}$$

3.2.3 Optimizing Embedding Factor

The combined transform of Graph-Based Transform and Singular Value Decomposition will aim at high-quality metrics, but it may not be sufficient to outperform some existing techniques. Optimization algorithms target quality metrics like PSNR(Peak Signal to Noise Ratio) as a fitness function and provide the dynamic process of updating the fitness function's values after every iteration. In this thesis, we have taken a hybrid optimization algorithm using Grey Wolf Optimization and Genetic Algorithm. The explanation of these algorithms is given below

3.2.3.1 Grey Wolf Optimization

The Grey Wolf Optimization model optimizes the factor by finding the fitness value from three wolves α,β, and δ, which provides the best solution, the 2nd best solution, and the 3rd best solution. The approach is to find a prey referred to as a fitness function (Quality Metric) in the watermarking scheme to get the fittest answer. The whole process is the search of prey, gradually updating the position to capture the prey faster. α is the leader of the pack, and rest all the wolves follow it. The role of grey wolves is updated by using the formula given in equation:12,13

$$\vec{M}=|\vec{L}*\vec{S}p(t)-\vec{S}(t)| \quad (12)$$

$$\vec{S}(t+1)=\vec{S}p(t)-\vec{F}*\vec{M} \quad (13)$$

Whereas $\vec{M}$ = distance between grey wolf and a prey, $\vec{L}$ =coefficient vector, t = number of iterations, $\vec{S}p$ = position vector of prey, $\vec{S}$ =position vector of the wolf, $\vec{F}$ =balance convergence coefficient between prey and wolf, The calculation of coefficient vectors $\vec{F},\vec{L}$ is done by equation 14,15.

$$\vec{F}=2\vec{a}*\vec{r}-\vec{a} \quad (14)$$

$$\vec{L}=2*\vec{q} \quad (15)$$

$\vec{a}$ =linearly decreases from 2 to 0, $\vec{r}$ and $\vec{q}$ are random vectors, $\vec{F}$ decreases with reduction in value $\vec{a}$. It means the wolf is nearer to prey. The grey wolves will update the positions by moving within search space to find the optimal solution. The location updating is done by following equations (16-22)

$$\vec{M}_\alpha=|\vec{L}1*\vec{S}_\alpha-\vec{S}| \quad (16)$$

$$\vec{M}_\beta=|\vec{L}2*\vec{S}_\beta-\vec{S}| \quad (17)$$

$$\vec{M}_\delta=|\vec{L}3*\vec{S}_\delta-\vec{S}| \quad (18)$$

$$\vec{S}1=\vec{S}_{\alpha}-\vec{F}_1*\vec{M}_{\alpha} \tag{19}$$

$$\vec{S}2=\vec{S}_{\beta}-\vec{F}2*\vec{M}_{\beta} \tag{20}$$

$$\vec{S}3=\vec{S}_{\delta}-\vec{F}3*\vec{M}_{\delta} \tag{21}$$

$$\vec{S}(t+1)=\frac{\vec{S}1+\vec{S}2+\vec{S}3}{3} \tag{22}$$

$\vec{M}_{\alpha},\vec{M}_{\beta},\vec{M}_{\delta}$ = distance amongst wolves α, β, and δ and the prey.

$\vec{S}1,\vec{S}2,\vec{S}3$ represents parameters that determine position w.r. t to α, β, and δ wolves. $\vec{S}(t+1)$ represents the positional vector after updating the grey wolf.

Steps of GWO Model of Optimization

a. The initial step is to generate an initial set of the population randomly, initialize parameters $\vec{a},\vec{F},\vec{L}$.

b. The next step is to calculate the fitness value of the grey wolf individual, save the highest individual with the highest fitness values $\vec{S}_{\alpha},\vec{S}_{\beta},\vec{S}_{\delta}$.

c. Next is to update the position parameter value as per equations (16) to (22) to obtain the next generation population and further update the value $\vec{a},\vec{F},\vec{L}$.

d. Calculate the fitness value of each individual of grey wolf and update $\vec{S}_{\alpha},\vec{S}_{\beta},\vec{S}_{\delta}$.

e. Repeat Steps b–e until maximum iterations are completed and the optimal solution is obtained.

Improved algorithm of global exploration improves convergence speed. The value of a improves efficiency of the algorithm. The value of a does not impact any local convergence; thus, solving large-scale multi-model problems will be hard to solve. So the improvement in the value of a will impact the optimal solution

$$a=a_{max}+(a_{min}-a_{max})\left(\frac{1}{1+e^{\frac{i}{i_{max}}}}\right)^{g} \tag{23}$$

a_{max}= initial value of parameter a, a_{min}=end value of parameter a, i=iteration index, i_{max}=maximum iterations, g= nonlinear adjustment coefficient

The value of F from equation 13 entirely depends upon the value of a, where a higher value of M expands searching criteria of a better way. If |F|<1, then the range is limited to a certain extent. F_i

represents current population fitness. The highest fitness values make the selection of individuals. K represents total fitness, and P_i represents the selected individual's probability given in equation 24,25, respectively.

$$K=\sum_{i=1}^{M-1} F_i \quad (24)$$

$$P_i = \frac{F_i}{\sum_{i=1}^{M-1} F_i} \quad (25)$$

Cumulative fitness value Ki is calculated till children are consistent like a parent illustrated in equation 26.

$$K_i = \frac{\sum_{i=0}^{i} F_i}{K} \quad (26)$$

3.2.3.2 Genetic Algorithm

A genetic algorithm is a heuristic approach where a set of random solutions is generated, followed by calculating fitness values, selection criteria, cross-over, and mutation. The advantages of using genetic algorithms are: easier to use, suitable for noisy environments, and good results when hybridization is done with other algorithms. The representation of the Genetic Algorithm is done using Figure 3.2.

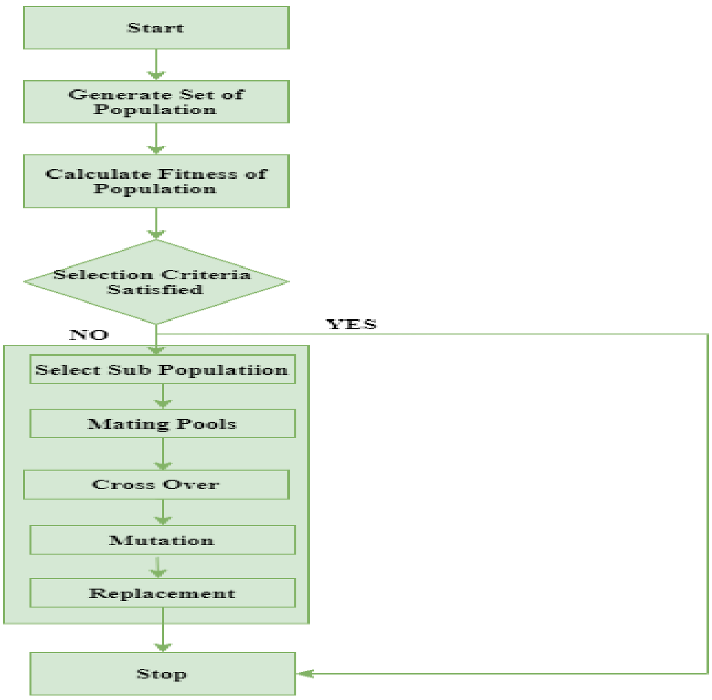


Figure 3.2: Process of Genetic Algorithm

3.2.3.3 Updated Model of Optimization

The genetic algorithm only applies when GWO does not update the value of quality metric(PSNR) after its iteration. The algorithm used in research [67] applied all operations of the Genetic Algorithm in case Grey Wolf Optimization does not update the value of PSNR. The representation of the hybrid model in research [67] is given in Figure 3.3. The hybrid model presented in research [67] solves the problem of local optima. More time will be consumed in each iteration if all operations of the genetic algorithm are performed. The proposed work will focus on the only cross-over operation of the Genetic Algorithm after Grey Wolf Optimization fails to update values of PSNR. The representation of the model used in this work is given in Figure 3.4. To solve significant scale problems, the Grey Wolf Optimization Algorithm is combined with the Genetic Algorithm where the entire population P is divided into t × d subpopulations $P_{i,j}$ (i = 1…..t; j = 1……..d). The random number is generated for each xi for cross overpopulation. The cross-over probability is represented by Pc, c11, c21 represent children generated from parents p11, p22 where z represents the random number that ranges from 0 to 1. The cross-over operation is illustrated from equations 27, 28.

$$c_i^1 = z\, p_i^1 + (1-z)\, p_i^2 \quad (i=1,2\text{------} M) \tag{27}$$

$$c_i^2 = z\, p_i^2 + (1-z)\, p_i^1 \quad (i=1,2\text{------} M) \tag{28}$$

$$\begin{pmatrix} x_{1,1} x_{1,2} & \cdots & x_{1,d} \\ \vdots & \ddots & \vdots \\ x_{p,1}\ x_{p,2} & \cdots & x_{p,d} \end{pmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\begin{pmatrix} x_{1,1} & \cdots & x_{1,5} \\ \vdots & \ddots & \vdots \\ x_{5,1} & \cdots & x_{5,5} \end{pmatrix} \qquad \begin{pmatrix} x_{1,(d-4)} & \cdots & x_{1,d} \\ \vdots & \ddots & \vdots \\ x_{5,(d-4)} & \cdots & x_{5,5} \end{pmatrix}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\begin{pmatrix} x_{(p-4),1} & \cdots & x_{(p-4),5} \\ \vdots & \ddots & \vdots \\ x_{p,1} & \cdots & x_{p,5} \end{pmatrix} \qquad \begin{pmatrix} x_{(p-4),(d-4)} & \cdots & x_{(p-4),d} \\ \vdots & \ddots & \vdots \\ x_{p,(d-4)} & \cdots & x_{p,d} \end{pmatrix} \tag{29}$$

The mutation operator is applied to elite individuals in the population. The individuals are taken as x_i with mutation probability P_m. It is represented in equation 29

$$x_i^1 = \begin{cases} l+z*(u-l) & ; \quad i=g \\ x_i & ; \quad i>g, i<g \end{cases} \tag{30}$$

l and u are lower and upper bounds to generate new individuals; z is a random number between 0 to 1. Optimization using hybrid optimization algorithm is given by:

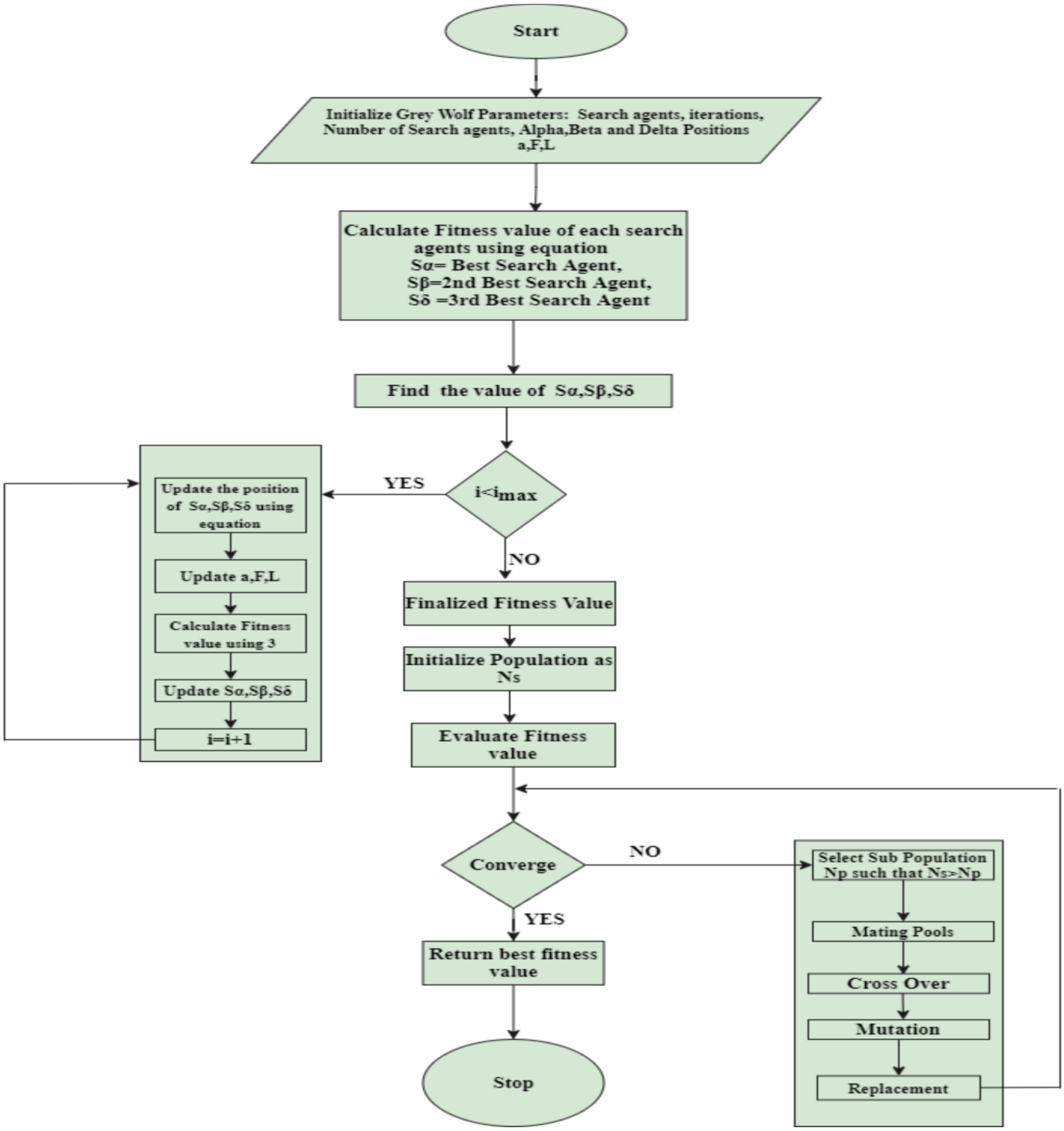


Figure 3.3: Optimizing Embedding factor using Hybrid GWO-GA [67]

The central part of embedding is to find the value of the embedding factor, which provides high values of quality metrics. The updated model in the research is given in Figure 3.4.

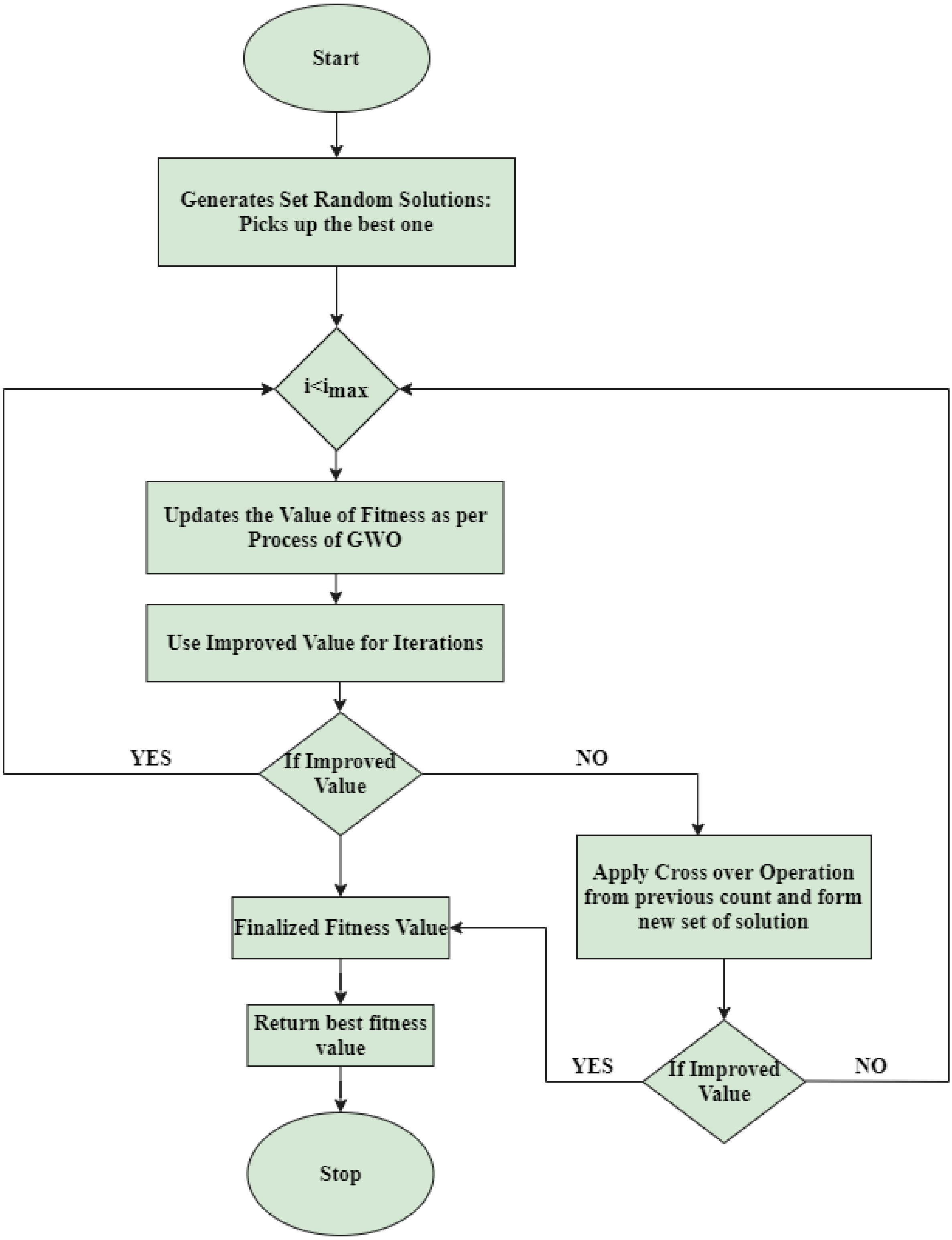


Figure 3.4: Optimizing Embedding factor using Hybrid GWO-GA in proposed work

3.2.3.4 Steps in Updated Optimization Algorithm in proposed work

Following steps are performed in the optimization of embedding factor value using the proposed model:

a. The watermark embedding on selected frames requires the good value of embedding factor to aim at high values of quality metrics (PSNR).
b. The embedding factor decides how much watermark has to be mixed with the selected frame value. Our thesis evaluated results of embedding factor with and without optimization algorithm, and the importance of optimization algorithm is realized in various attack scenarios.
c. We used the static process to embed the watermark by putting different values of embedding factor and found out at a 0.02 embedding factor value in equation 11; we got good results of quality metrics(PSNR) using Graph-Based Transform and Singular Value Decomposition listed in published work[90].
d. There is a possibility that results can be improved by using an optimization algorithm. For that purpose, we used a hybrid algorithm involving Grey Wolf Optimization and Genetic Algorithm. PSNR is taken as a quality parameter.
e. The optimization algorithm generates a set of solutions, checks the value of PSNR at every iteration, and chooses the keys with high PSNR.
f. There is a list of iterations defined in Grey Wolf Optimizer at that start, and after applying the procedure of GWO, the value of the embedding factor is updated after every iteration.
g. After every iteration, the value of the embedding factor is checked. If the value is improved, we update the value of the embedding factor in the next iteration by taking the best value as a reference else; we apply the genetic algorithm's cross-over operation by various existing populations to form a new set of values. The selection and mutation operations in genetic algorithms are skipped. Only a cross-over function was applied, as it will check from solutions generated by GWO and update the values as per its procedure.
h. Using cross-over operation instead of making new solutions proposed in research [67] , shuffling of another set generated by GWO, might give better values of PSNR in the same iteration.
i. If values still do not improve, we will go with the last reference value in GWO.

It has been discussed in chapter 4 that the technique proposed (GBT-SVD-GWO-GA) by optimizing embedding factor gives better results than static methods (GBT-SVD). The values of Quality

Metric(PSNR) are higher in GBT-SVD-GWO-GA is higher than GBT-SVD. The comparative analysis for every situation is represented in chapter 4 (Results and Discussions). Various attacks have been performed on the proposed technique to check the efficiency and the proposed optimized approach gives a higher value of quality metrics considering attack scenarios. The algorithm of optimization of embedding factor is shown below :

Algorithm 2 Hybrid GWO-GA Approach for Embedding Factor

Input: Embedding Factor
Output: Optimized Embedding Factor for Watermark Embedding on alpha value
Begin
(1) Initialize parameters a, F, L, population size N, P_c and P_m
(2) Initialize current population *P*
(3) i=0
(4) While $i<i_{max}$
(5) {
(6) Find the fitness value of all search agents
(7) S_α= Best Search agent for embedding factor
S_β= 2nd Best Search agent for embedding factor
S_δ= 3rd Best Search agent for embedding factor
(8) for i = 1 to N
(9) {
(10) Update search agent positions given in equation (21).
(11) }
(12) Assign P1←P except the $S\alpha$
(13) for i = 1to N-1
(14) {
(15) Get new value of P2 by the selection on new value of P1.
(16) }
(17) Assign P←newP2, S_α
(18) Find the fitness value of all search agents.
(19) Find updated search values $S_{\alpha us}$, $S_{\beta us}$,$S_{\delta us}$.
(20) if ($S_{\alpha us}$, $S_{\beta us}$,$S_{\delta us}$)> (S_α, S_β, S_δ)
(21) return S_α
(22) else
(23) {
(24) Select the individuals using crossover probability P_c.
(25) for i = 1 to $N*P_c$
(26) {
(27) Perform Crossover on each search agent by equations (27) and (28).
(28) }
(29) Return S_α.
(30) }
End

The approach starts with the Grey Wolf Optimization application to find the best search agents; if the best search agents are not found, then the Genetic Algorithm's crossover operation is applied to get higher values of PSNR as a target function. The optimization of embedding factor is done using Grey Wolf Optimization followed Genetic Algorithm. The areas to find the best fitness parameter(PSNR) are done by calculating each search agent's fitness, updating the fitness value after every iteration. The algorithm works better than the research [67] as there is no selection and mutation operation done, which increases the time complexity of the optimization algorithm. The watermark's embedding is done using Graph-Based Transform (GBT) and Singular Valued Decomposition (SVD) followed by optimization of embedding factor by using an updated optimization algorithm.

3.2.4 Encryption of Watermark Before Embedding

The encryption of the watermark is a significant feature of providing security to the technique. The watermark image taken in the proposed work is encrypted before the watermark is embedded. Most research conducted using a transposition cipher [65], although it is not increasing the code's complexity, security is compromised in this aspect. Our proposed technique will apply Hyper Chaotic Encryption for encrypting the watermark that is inspired by research [69].

The watermark is encrypted using Hyper Chaotic Encryption to add a security feature to the proposed technique. Watermark is not required to be transformed using GBT transform—the reason why it is not changed because encryption is supposed to be applied to the watermark. Watermark is scrambled using hyperchaotic encryption, and after that S value of the watermark is taken using Singular Value Decomposition.

$$\left\{\begin{array}{l} x=a(y-x)+w \\ y=cx-y-xz \\ z=xy-bz \\ w=-yz+rw \end{array}\right\} \tag{31}$$

The value of x,y,z, and w calculated from the above equation will be used to encrypt the watermark image. The standard values of a,b,c were taken as per [69]. The second step is rows and columns conversion into x,y for column and row of the encrypted watermark image.

$$X=\mathrm{mod}\left(\mathrm{floor}\left(R+100\right)*105,i\right)+1$$

$$Y=\mathrm{mod}\left(\mathrm{floor}\left(S+100\right)*105,j\right)+1 \tag{32}$$

The third step is to interchange the coefficients of m^{th} row and $x(m)^{th}$ row of image W m=1,2………..i , N=1,2………j

$$W(m,:)=W(x(m),:) \tag{33}$$

$$W1=W \tag{34}$$

$$W1(:,n)=W1(:,y(n)) \tag{35}$$

W1 is an encrypted watermark image to be embedded.

The encryption of a watermark image is represented as W(i,j) where the image size is defined as m*n. The first step is generating the sequence of R, S using the Lorenz system. The security feature added here adds to the security feature by encrypting watermark before being embedded, thus making the technique more secure. Hyperchaotic encryption is a mechanism that uses predefined values and a higher number of Lyapunov exponents [65], thus making it a secured method of encryption. The watermark embedding procedure is defined in algorithm3 and represented in Figure 3.5.

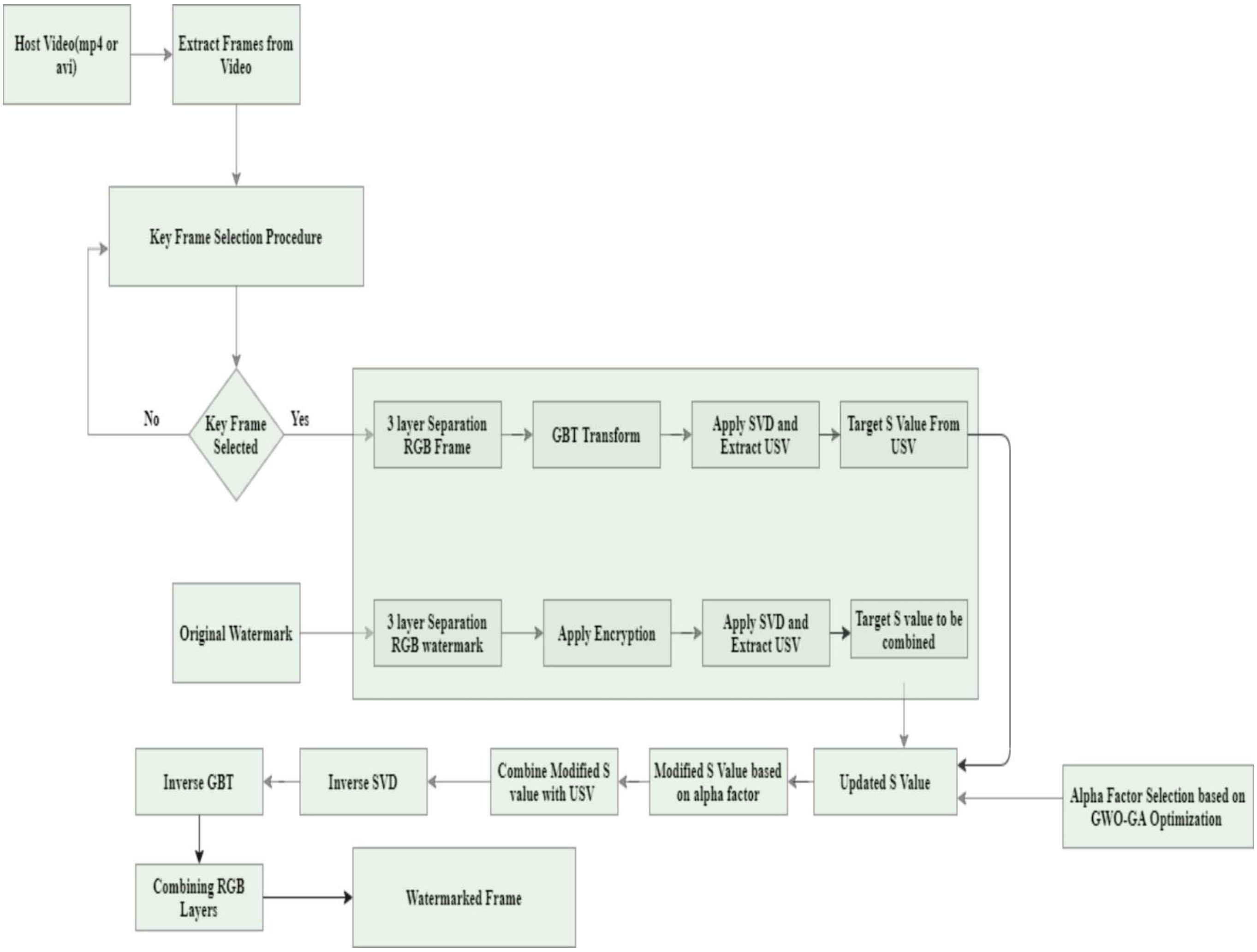


Figure 3.5: Watermark Embedding Procedure

Algorithm 3: Watermark Embedding Algorithm

Input: Selected Frames from Algorithm 1
Output: Watermarked Video
Begin
(1) for selected frames ←1 to k.
(2) {
(3) Take a The image watermark W(i,j).
(4) Use Layer separation on selected RGB frame K(i,j) and watermarked image W(i,j).
(5) Apply Hyper Chaotic Encryption on the watermark.
(6) Apply GBT Transform on each layer of K(i,j).
(7) Apply SVD and extract USV feature of each layer of K(i,j) and W(i,j).
(8) Take S value of the frame and watermarked image.
(9) Optimize the value of embedding factor α mentioned in equation 6 using hybrid GWO-GA.
(10) Embed watermark W(i,j) to K(i,j) using the optimized value of α calculated in equation 6.
(11) Combine both S values of Selected frame and Watermarked image to get modified S from
(12) Target the best PSNR from the alpha value calculated from equation
(13) Repeat steps from 2 to 12 till all the selected frames are processed.
(14) }
(15) for frames 1 to m in the directory of extracted frames.
(16) {
(17) Combine watermarked frames and replace them with frames in extracted frame directory.
(18) Process all selected frames and frames in the given directory to form watermarked video.
(19) }

End

3.3 Watermark Extraction Procedure

The next section in the proposed work describes the watermark extraction procedure to recover watermark from watermarked video. The watermarked extraction from the watermarked video was a reverse process . The extraction of frames is followed by applying GBT and SVD. The extraction is calculated as per equation 36, followed by inverse GBT and inverse SVD. Then decryption is done using a key then the watermark is recovered. Figure 3.5 represents watermarking embedding procedure, and Figure 3.6 illustrates the watermark extraction procedure. The method of watermark extraction is discussed in algorithm 4.

$$W(i,j)=\left(K'(i,j\ )-K(i,j)\right)/\alpha \tag{36}$$

W(i,j)=Extracted watermark

K'(i,j)=Watermarked Frame

K(i,j)=Selected Frame

Algorithm 4: Watermark Extraction Algorithm

Input: Watermarked Video
Output: Recovered Watermark
Begin
(1) Take Watermarked Video
(2) for frames from 1 to k
(3) {
(4) Perform layer separation on RGB Frame
(5) Apply GBT Transform on each layer of K'(i,j).
(6) Apply SVD and extract USV feature of each layer of K'(i,j).
(7) Extract watermark W(i,j) from K'(i,j) using formula W(i,j)=(K'(i,j)-K(i,j))/α
(8) Extract S value.
(9) Perform Inverse SVD to combine S value with USV of each layer
(10) Perform Inverse GBT Transform
(11) Decrypt watermark using Key
(12) Repeat steps from 4 to 12 till all the watermarks on selected frames are extracted.
(13) }
End

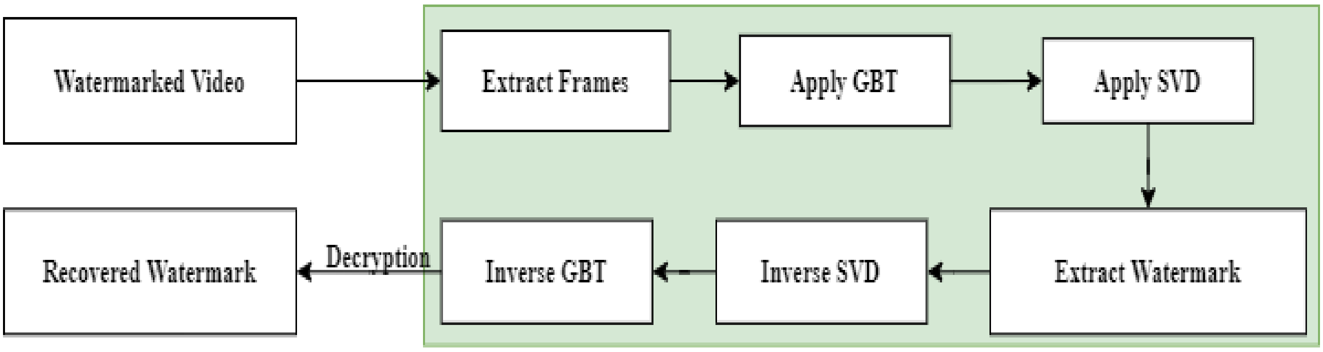


Figure 3.6: Watermark Extraction Procedure

3.4 Performance Evaluation

The watermarking technique's performance evaluation is calculated in terms of the video's quality parameters and robustness against various attack scenarios. The parameters are given below:

a. **PSNR (Peak Signal to Noise Ratio):** PSNR is a significant quality parameter that differentiates original and watermark frames based on Mean Square Error. PSNR is a performance parameter also along with that it is the quality metric used in this research as the optimization algorithms (GWO and GA) are taking PSNR as a fitness function, and PSNR is passed as a parameter to calculate the fitness function after every iteration. PSNR is inversely proportional to Mean Square Error (MSE). MSE is calculated in equation 37. The average PSNR is the sum of PSNR of all selected frames divided by several frames. Average PSNR is calculated by equation 39. The proposed technique's objective is to obtain high values of PSNR as the embedding of watermark causes quality loss. Higher values of PSNR indicate the efficiency of the method.

$$MSE=\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{1}{M*N}\left([A(i,j)-E(i,j)]\right)^2 \quad (37)$$

where M, N represents rows and columns

$$PSNR=\frac{10\log_{10}(255)^2}{MSE} \quad (38)$$

A(i,j) = Selected Frame

E(i,j)=Watermarked Frame

$$\text{Average PSNR}=\frac{\sum_{i}^{n} PSNR_i}{n} \quad (39)$$

b. **Normalized Correlation (NC):** This performance parameter is used to find a correlation between the watermarked frame and a selected frame. It is calculated using equation 40

$$NC=\frac{\sum_{i=1}^{G}\sum_{j=1}^{H}(A(i,j)-\bar{A})(E(i,j)-\bar{E})}{\sqrt{\sum_{i}^{G}\sum_{j=1}^{H}(A(i,j)-\bar{A})^2\sum_{i=1}^{G}\sum_{j=1}^{H}(E(i,j)-\bar{E})^2}} \quad (40)$$

A(i,j): Selected Frame, E(i,j): Watermarked Frame, $\bar{A}$ is mean of selected frames, $\bar{E}$ is mean of watermarked frames.

c. **Structural Similarity Index Measure:** This performance parameter is used to find structural similarity between the watermarked frame and selected frame. It is calculated from equation 41, where l,c, and s represent luminance, contrast, and structure, m n represents selected and watermarked frames. The structural comparison is done with m and n. C_1, C_2, and C_3 are variables.

$$SSIM(m,n)=[l(m,n)]^{\alpha}[c(m,n)]^{\beta}[s(m,n)]^{\gamma} \tag{41}$$

$$l(m,n)=\frac{2\mu_m\mu_n+C_1}{\mu^2_m+\mu^2_n} \tag{42}$$

$$c(m,n)=\frac{2\sigma_m\sigma_n+C_2}{\sigma^2_m+\sigma^2_n+C_2} \tag{43}$$

$$s(m,n)=\frac{\sigma_{mn}+C_3}{\sigma_m\sigma_n+C_3} \tag{44}$$

where μ_m, μ_n,σ_m, σ_n, σ_{mn} are local means, standard deviation, cross variances of selected frames and watermarked frames. α,β,γ are the weights used. If $\alpha=\beta=\gamma=1$, $C_3=C_2/2$, the index simplifies as:

$$SSIM(m,n)=\frac{(2\mu_m\mu_n+C_1)(2\sigma_m\sigma_n+C_2)}{(\mu^2_m+\mu^2_n+C_1)(\sigma^2_m+\sigma^2_n+C_1)} \tag{45}$$

d. Bit Error Rate: This is a quality parameter. It is an inverse of PSNR. Higher values of PSNR or lower values of BER indicate the effectiveness of the technique. It is calculated in equation 46.

$$BER=\frac{1}{PSNR} \tag{46}$$

The Numerical values of NC, SSIM, and BER lie in the range of [0,1] while SSIM and NC measure the similarity, so high values are preferred. Out of these parameters, we have taken PSNR as a quality metric as taking combined parameters like PSNR and NC as fitness functions would not have made the difference. The value of NC ranges from 0 to 1. This situation would have led to more time complexity in every iteration of the optimization algorithm.

CHAPTER 4

RESULTS AND DISCUSSION

This chapter outlines the results and discussions after the implementation of the proposed technique. Results and Discussion include calculating frame selection time, watermark embedding time, and values of quality metrics. A detailed analysis of watermark embedding techniques is done in this chapter.

4.1 Experimental Results on Input Video Set

This section explains the input data set and the number of frames selected from the given videos. The results were calculated in MATLAB 2018b using an i5 processor. The frame selection and embedding time are dependent on the type of processor used. The compiled results are dependent upon watermark embedding, frame selection. A total of 6 cif encoded videos have been taken, and the frame selection mechanism depends on scene change detection. Algorithm 1 discusses the selection of frames. The video named Akiyo didn't have sufficient scene change detection so, as a result of this, no frames got fixed, and the watermarking technique couldn't be applied. The reseason was that the value of F_k(Frame difference) was not greater than M_b (threshold), so no significant frames got selected from the video, the rest of the videos have important frames chosen as per the frame selection algorithm.

Table 4.1: Comparison of videos in terms of frame selection

SNO	Video Name	No of Frames Selected
1	Akiyo	0
2	Coastguard	1
3	Foreman	2
4	News	3
5	Bowing	4
6	Pure_Storage	5

Table 4.1 represents the number of frames getting selected from the input video data set. Pure_Storage video has got maximum chosen frames. The video Pure_Storage has more number of significant changes; hence more frames got selected from it. The plots in Figure 4.1 represent the number of frames from the input video data set.

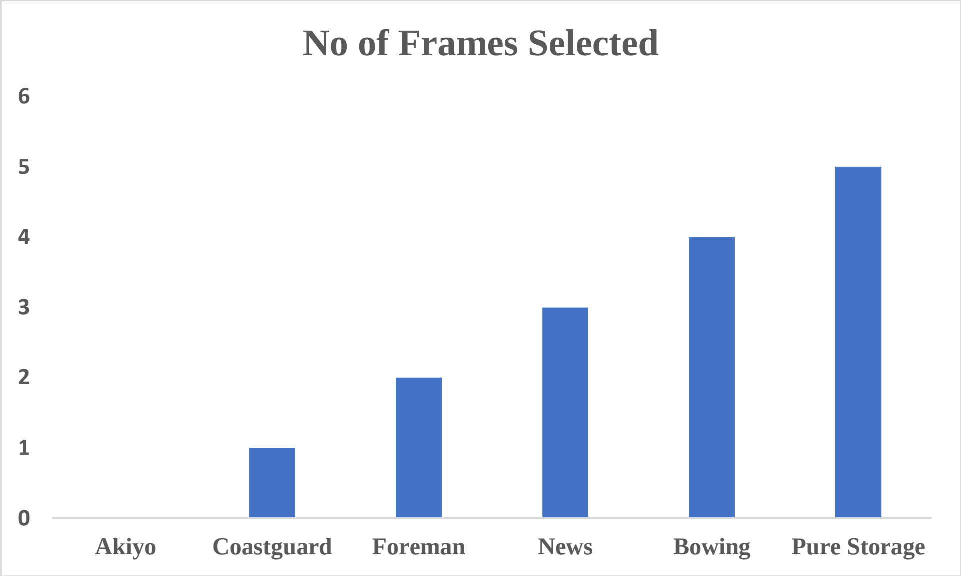


Figure 4.1: Plots of Selected frames from the input data set

Along with these videos, two watermarks and their encrypted versions have been depicted in Figure 4.2. The compressed domain videos are taken in this research. The encrypted watermark not only addresses security issues but also adds to copyright protection to achieve ownership identification. The experimental results are divided into certain phases; frame extraction, frame selection, the embedding of the encrypted watermark, attacks on the watermarked frame. Embedding of the watermark is done using the proposed method, followed by testing the technique's validity by applying specific attacks. Higher values of PSNR and lower BER values implicate the proposed technique to be efficient, leading to less loss of output video quality. Every video will have different properties that mean frame selection in every video will be different. The representation of videos is demonstrated in this research where different videos have the other numbers of frames getting selected. Figure 4.3 represents watermarked frame after watermarking process along with watermark 1. Figure 4.4 illustrates the plot of various videos and their respective quality parameters against no attack. In this research, the calculation of results is done by applying the watermark embedding technique (GBT-SVD-Hyper Chaotic Encryption) on selected frames. This research is justified in published work[90]. However, the results of quality metrics can be improved by applying an optimization algorithm3. The optimization algorithm's importance is realized by comparing the effects of the embedding technique with and without optimization. The comparative analysis is done on both methods, and all attack scenarios are applied to check the efficiency of the proposed method. GBT-SVD represents the watermarking technique without optimization and GBT-SVD-GWO-GA is the proposed technique that optimizes the embedding factor.

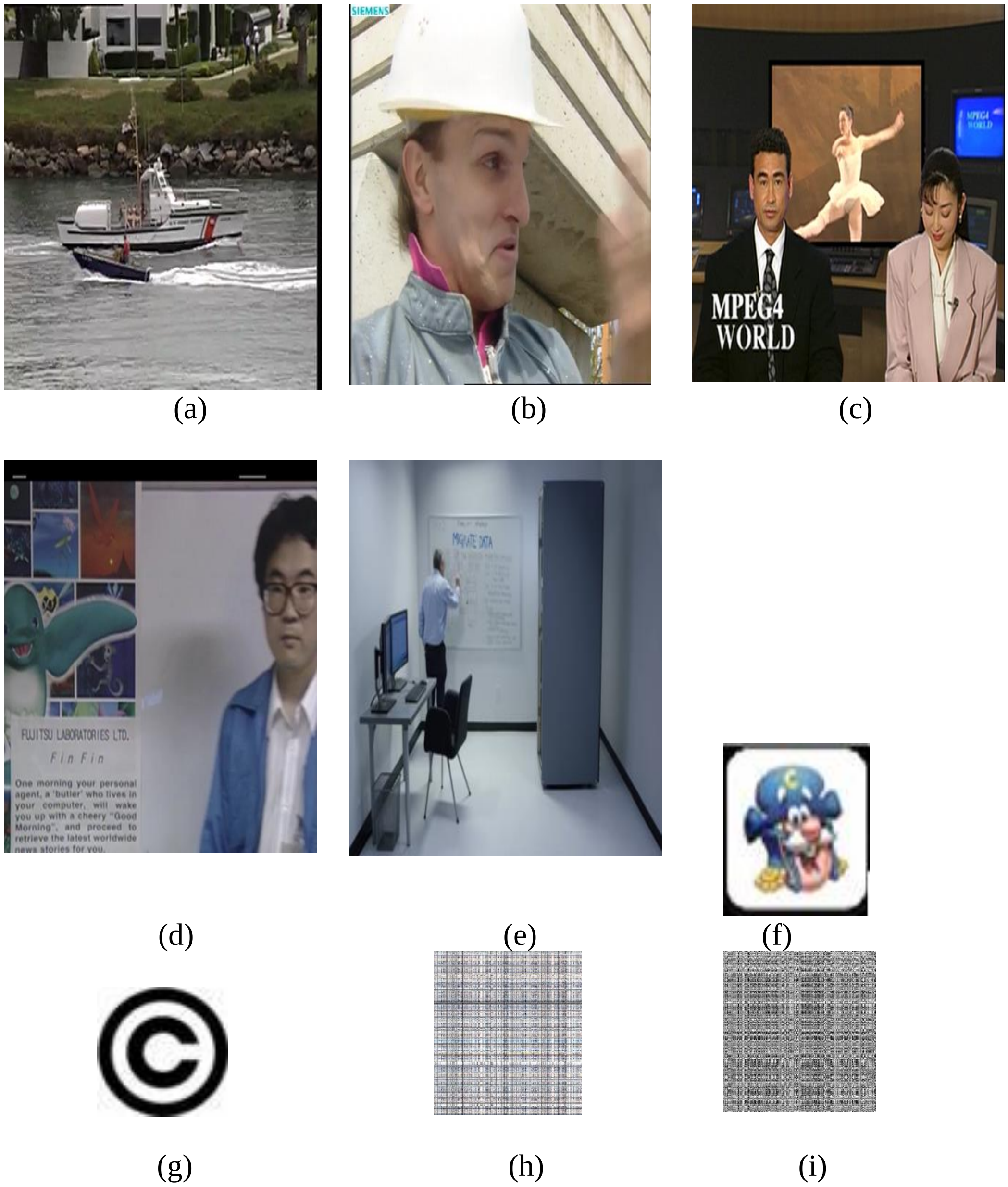
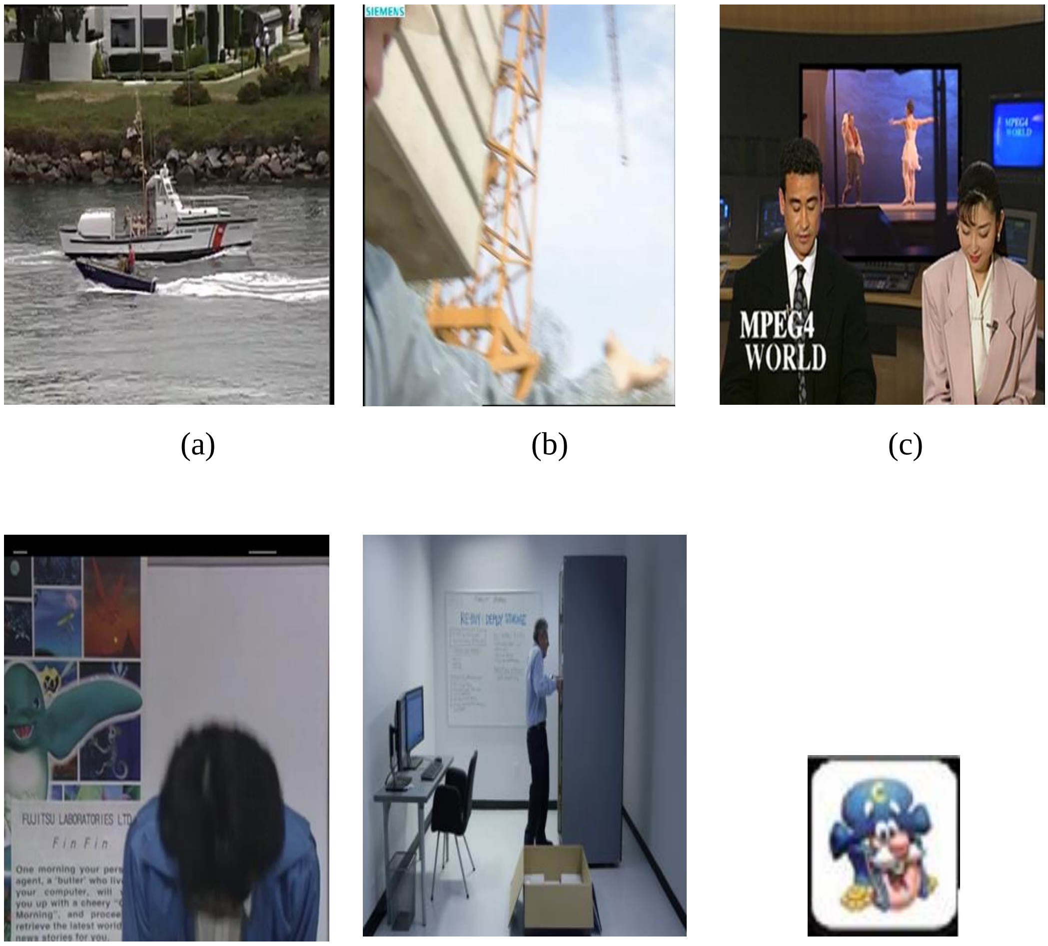


Figure 4.2 (a-i): Selected frames from videos (a) Coastguard (Frame # 64), (b) Foreman (Frame # 134), (c) News (Frame # 78), (d) Bowing (Frame # 48) and (e) Pure_Storage (Frame #57); (f) original watermark1, (g)original watermark2 , (h) encrypted watermark1 ,(i) encrypted watermark

4.2 Experimental Tests for Quality Check

This section discusses the calculation of the results for both GBT-SVD and GBT-SVD-GWO-GA techniques. There are two watermarks used for the proposed watermarking scheme. The comparative analysis is done for both watermarks. The proposed method's performance is measured in terms of PSNR, SSIM, NC, and BER. The validation of implementation is done by applying attacks on watermarked frames. The comparative analysis of the technique with optimization and without optimization is done using watermark 1. The comparison analysis of both watermarks' applications is done to justify no difference if similar watermarks are taken.



(a) (b) (c)

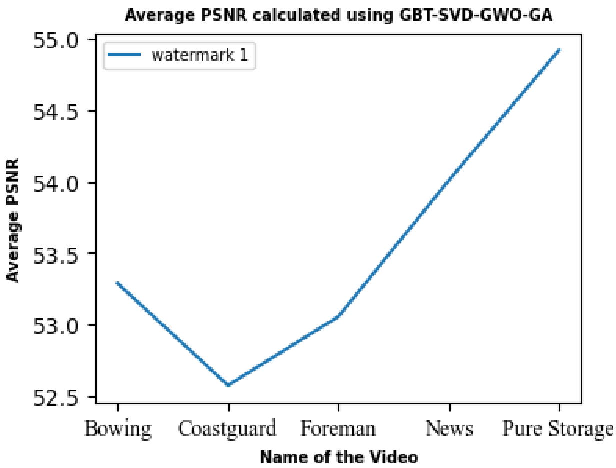
(d) (e) (f)

Figure 4.3 (a-e): Watermarked frames from the video, (f)- Selected Image Watermark

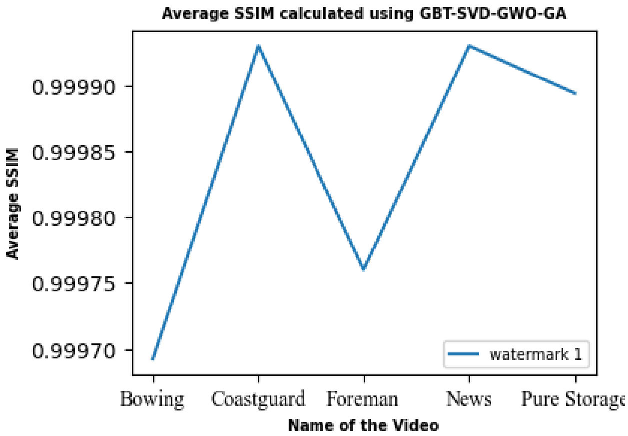
Figure 4.3 represents the watermarked frame after embedding the optimized watermarking technique on the selected frames. Watermark 1 has been used for embedding purposes. Table 4.2 describes the results of the proposed method (GBT-SVD-GWO-GA) after embedding of watermark1. Performance parameters: PSNR, SSIM, NC, and BER are used to calculate results. Plots in Figure 4.4 represent the calculated values of performance parameters using the proposed technique(GBT-SVD-GWO-GA).

Table 4.2: Results after Embedding of Watermark 1 on selected frames

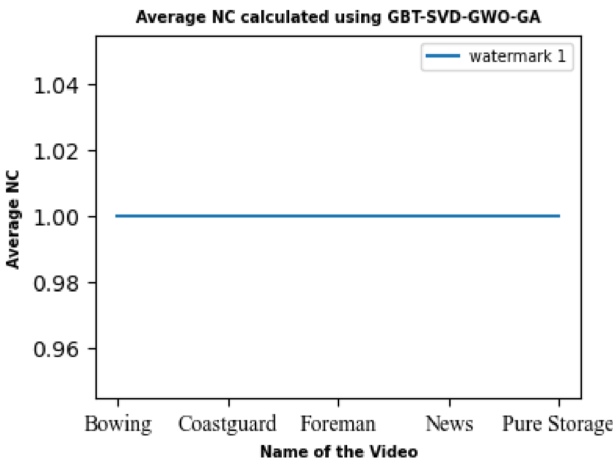
Video	PSNR (dB)	SSIM	NC	BER
Coastguard	52.5768	0.99993	0.9999	0.01902
Foreman	53.05685	0.99976	0.9999	0.01885
News	54.0078	0.99993	0.9999	0.01852
Bowing	53.289375	0.9996925	0.9999	0.01876
Pure_Storage	54.91922	0.999894	0.9999	0.01829



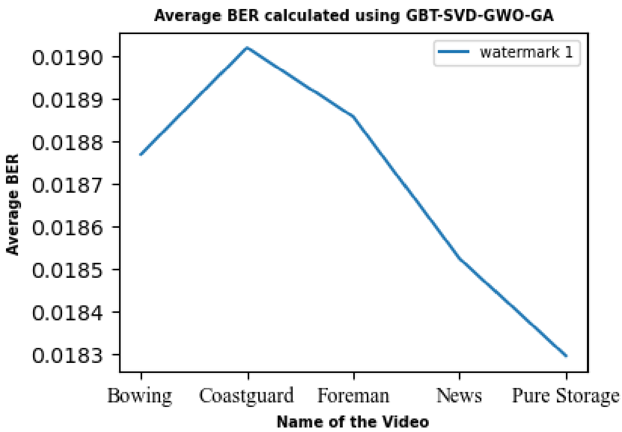
(a)Average PSNR against No attack using Watermark1



(b) Average SSIM against No attack using Watermark1

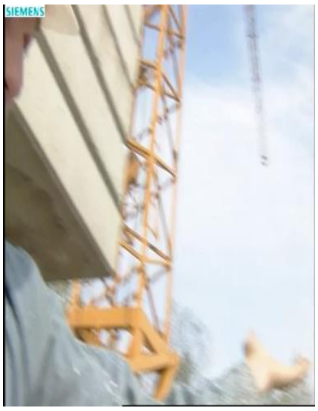


(c)Average NC against No attack using Watermark1

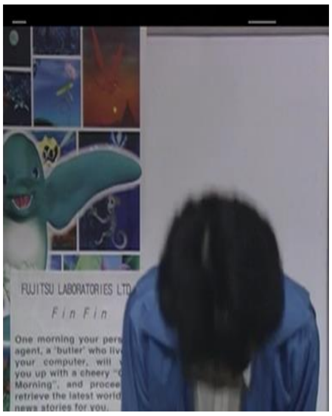


(d)Average BER against No attack using Watermark1

Figure 4.4(a-d): Plot of PSNR, SSIM, NC, BER of GBT-SVD-GWO-GA w.r.t the videos taken in the proposed work for watermark 1 against No attack



(a) (b) (c)



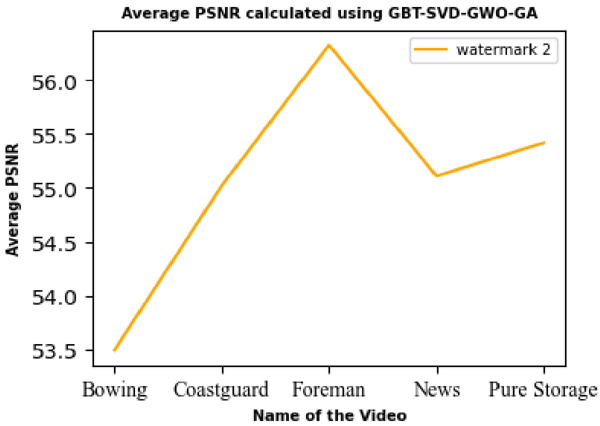

(d) (e) (f)

Figure 4.5 (a-e) : Watermarked frames from the video, (f)- Selected Image Watermark

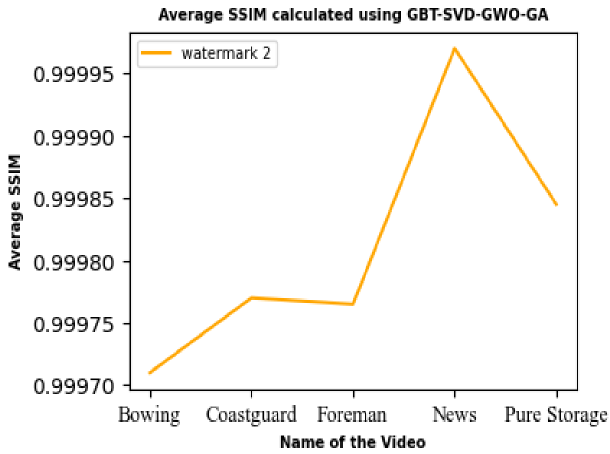
Figure 4.5 represents the watermarked frame after embedding the optimized watermarking technique on the selected frames. Watermark 2 has been used for embedding purposes. Table 4.3 describes the results of the proposed method (GBT-SVD-GWO-GA) after embedding of watermark2. Performance parameters: PSNR, SSIM, NC, and BER are used to calculate results.

Table 4.3: Results after Embedding of Watermark 2 on selected frames

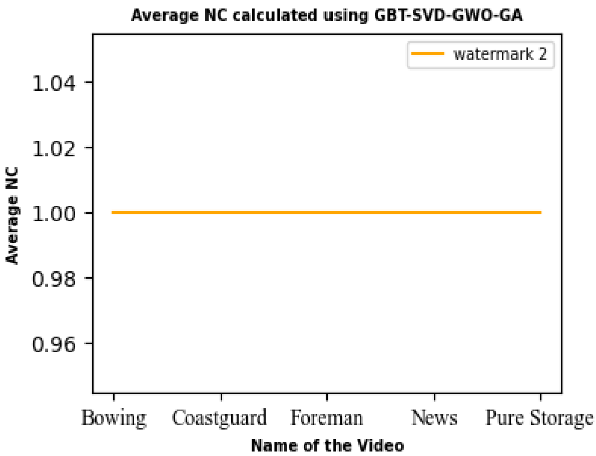
Video	PSNR (dB)	SSIM	NC	BER
Coastguard	55.020	0.99977	0.99998	0.01817
Foreman	56.327	0.99976	0.99998	0.01776
News	55.109	0.99997	0.99999	0.01814
Bowing	53.490	0.99971	0.99997	0.01869
Pure_Storage	55.418	0.99984	0.99998	0.01807



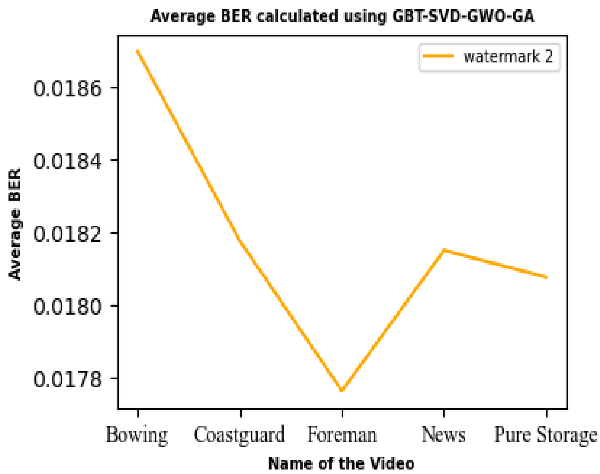
(a)Average PSNR against No attack using Watermark2



(b) Average SSIM against No attack using Watermark2



(c)Average NC against No attack using Watermark2



(d)Average BER against No attack using Watermark2

Figure 4.6 (a-d): Plot of PSNR, SSIM, NC, BER of GBT-SVD-GWO-GA w.r.t the videos taken in the proposed work for watermark 2 against No attack

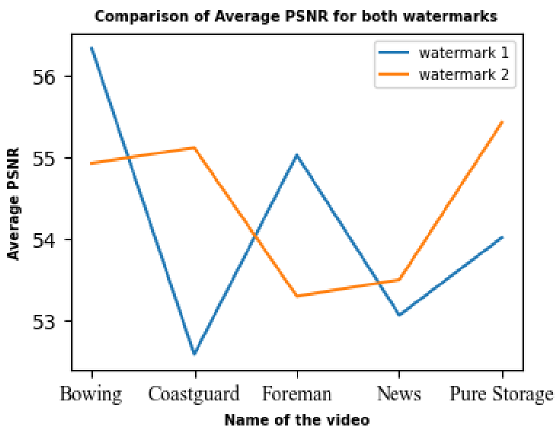
Table 4.2,4.3 represents the calculated values of quality parameters after applying the optimized watermarking technique using watermark 1,2. The PSNR has improved after applying the hybrid model of Grey Wolf Optimization and Genetic Algorithm. The comparative analysis of the proposed method by using watermark 1 (W1) and watermark 2(W2) is represented in Table 4.3. Plots in Figure 4.6 represent the calculated values of performance parameters using the proposed technique(GBT-SVD-GWO-GA).

Table 4.3: Comparative Analysis of GBT-SVD-GWO-GA for Watermark 1 and 2

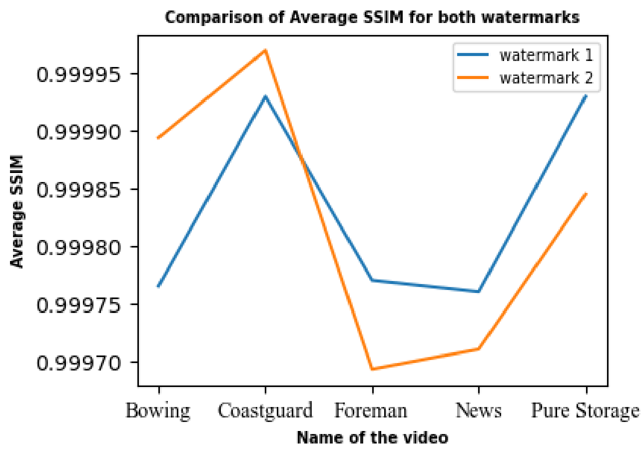
Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	W1	W2	W1	W2	W1	Ws2	W1	W2	W1	W2
PSNR	52.52	55.02	53.05	56.32	54.00	55.10	53.28	53.49	54.91	55.41
SSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
NC	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
BER	0.019	0.018	0.018	0.01	0.018	0.018	0.018	0.018	0.018	0.018

The results in Table 4.3 describe the comparative analysis of two watermarks embedded in input videos; the results signify no significant changes in quality parameters. In the proposed work, many frames are extracted from videos and the other frame selection is done, and the watermark is embedded in every selected frame. To carry out the analysis of these processes with both watermarks will be time-consuming, as both signify similar values. W1 and W2 represent the watermark taken to carry out the embedding process. The results in the other section will also indicate the importance of the optimization mechanism. So, watermark 1 is used for carrying out the embedding process.

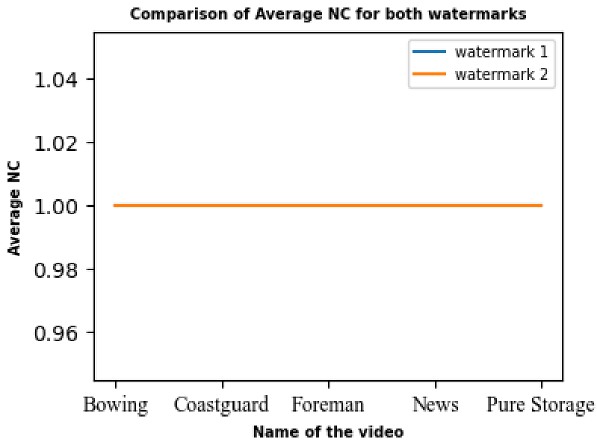
Further analysis has been done on the embedding time of both watermarks. Plots in Figure 4.7 represent the calculated values of quality parameters for both watermarks. The results illustrate that apart from the marginal difference in PSNR and BER for both watermarks, there is no significant difference among both watermarks' quality parameters. Table 4.5 represents the comparative analysis of the proposed optimized technique tested on five videos by applying both watermarks.



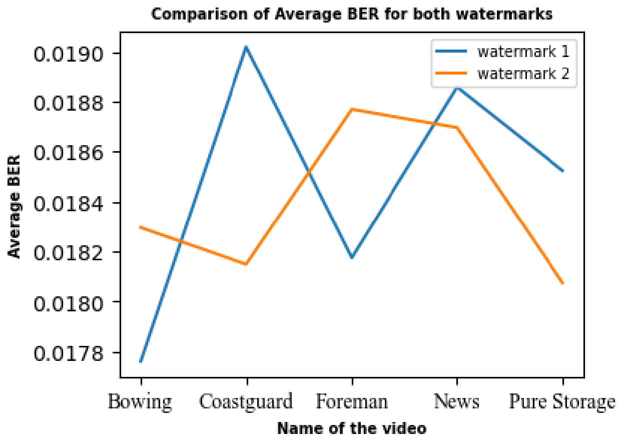
(a) Comparison of Average PSNR of watermark1 and watermark 2



(b) Comparison of Average SSIM of watermark1 and watermark 2



(c) Comparison of Average NC of watermark1 and watermark 2



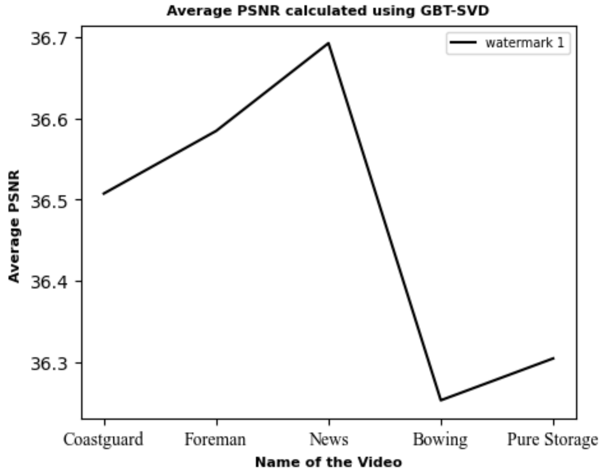
(d) Comparison of Average BER of watermark1 and watermark 2

Figure 4.7(a-d): Plot of Comparison of PSNR, NC, SSIM, BER w.r.t the videos taken in the proposed work for both watermarks

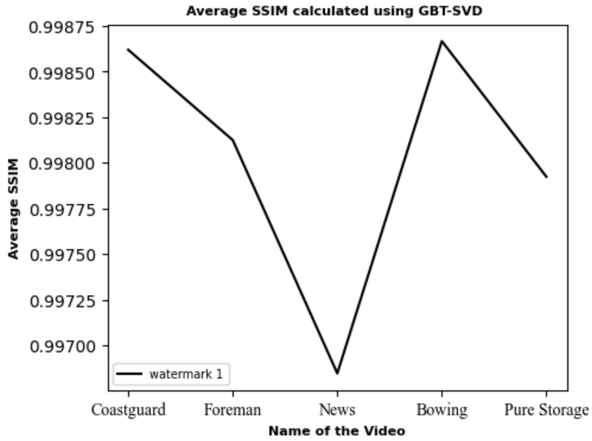
The importance of optimization is realized by taking the number of iterations for the best fitness function. The fitness function targets the high value of PSNR by optimizing the embedding factor. If an optimization algorithm is not used, then the result calculation is done on the GBT-SVD technique. The hyperchaotic mechanism is applied to the watermark before embedding it. Result calculation of GBT-SVD is done for all input videos. The comparative analysis is done on GBT-SVD and GBT-SVD-GWO-GA using watermark 1 to realize the importance of optimization. Plots in Figure 4.8 represent the calculation of quality parameters against no attack. Table 4.4 represents calculated values after the embedding technique (GBT-SVD) is applied using Graph-Based Transform and Singular Valued Decomposition. The embedding factor is taken as 0.02.

Table 4.4: Results of Watermark Embedding Technique GBT-SVD using Watermark 1

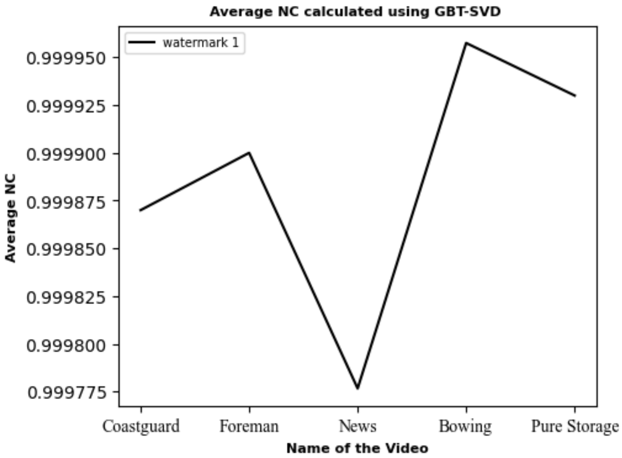
Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.5075	0.99862	0.99987	0.027392
Foreman	36.5845	0.99812	0.99999	0.027335
News	36.6924	0.99684	0.99977	0.027254
Bowing	36.2533	0.99866	0.99995	0.027584
Pure_Storage	36.30476	0.99792	0.99993	0.027545



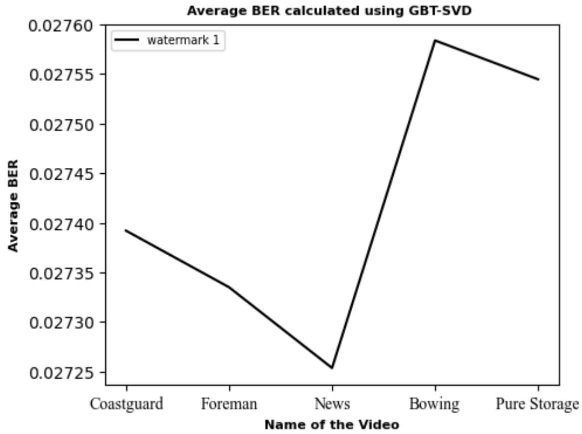
(a)Average PSNR against No attack using Watermark1



(b) Average SSIM against No attack using Watermark1



(c)Average NC against No attack using Watermark1

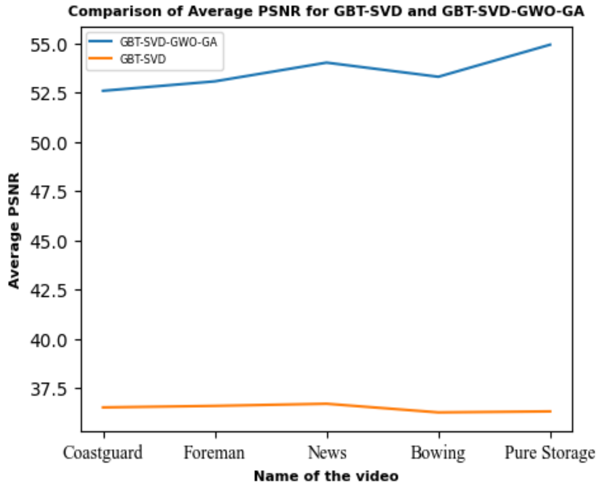


(d)Average BER against No attack using Watermark1

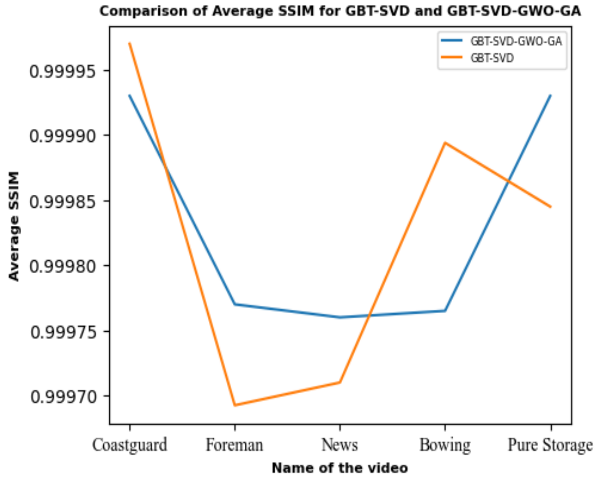
Figure 4.8(a-d): Plot of PSNR, SSIM, NC, BER of GBT-SVD w.r.t the videos taken in the proposed work for watermark1 against No attack

Table 4.5: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1

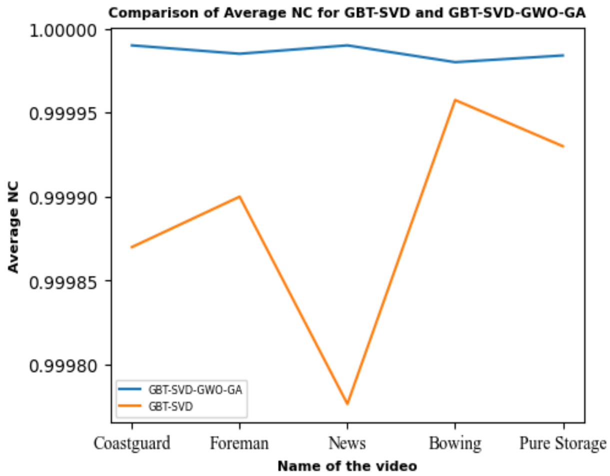
Parameters	**Coastguard**		**Foreman**		**News**		**Bowing**		**Pure_Storage**	
	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2
PSNR	52.57	36.50	53.05	36.58	54.00	36.69	53.28	36.25	54.91	36.30
SSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
NC	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
BER	0.019	0.027	0.018	0.027	0.027	0.018	0.027	0.027	0.018	0.027



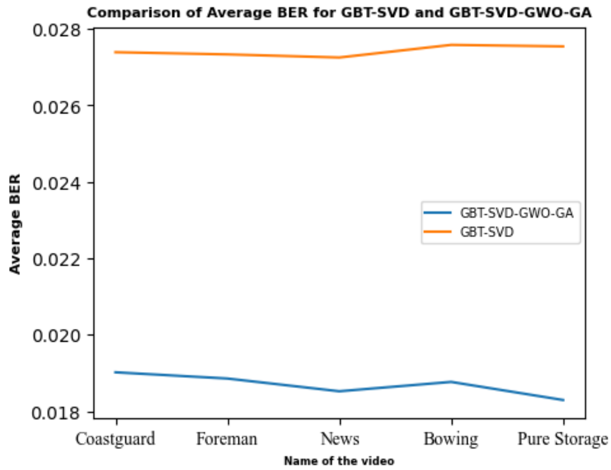
(a)Average PSNR without attack



(b) Average SSIM without attack



(c)Average NC without attack



(d)Average BER without attack

Figure 4.9(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA without attack

The analysis from Table 4.5 indicates that optimizing the embedding factor improves the value of PSNR. The PSNR is taken as a fitness function in optimization that is why it has a higher value using GBT-SVD-GWO-GA. There is no difference in values of NC, SSIM in both techniques(T1 and T2) The optimization is a dynamic process in which grey wolf optimizer is used in the earlier part of the iteration; after the initial iteration, GWO updates the values of PSNR, if the value is improved, then it goes to the next iteration to enhance the value of PSNR else it goes to cross over operation of Genetic algorithm. The results indicate high values of PSNR using the optimized technique (GBT-SVD-GWO-GA) comparative to GBT-SVD. Plots in Figure 4.9 show the comparative analysis of both methods.

4.3 Experimental Tests for Time Complexity

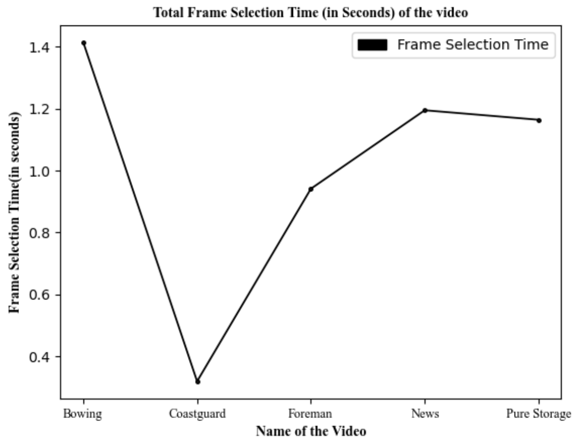
Table 4.6 and Table 4.7 compile the processing time (in seconds) required to carry out frame selection, embedding, and extraction of both watermarks for a given set of videos. Figure 4.10 represents plots for comparison of quality parameters of both watermarks. The time is entirely based on processor requirements. The total time consumed depends upon the selection of frames from the video. Pure_Storage video has got five frames selected and the time for every frame varies from 20 to 35 seconds for every frame. Embedding time is dependent upon the number of selected frames and iterations in which optimization is applied. As a standard, ten iterations have been taken to obtain the high value of fitness i.e. PSNR, more iteration will lead to the higher value of embedding time. The total time consumed for every video is mentioned in Table 4.6 and Table 4.7, and the frame selection plot is represented in Figure 4.10 for GBT-SVD and Figure 4.11. For GBT-SVD-GWO-GA. The value of embedding time is similar for both watermark1 and watermark2. A total of 5 frames got selected from the Pure_Storage video; thus, the total embedding time is the highest for the same video. Plots in Figure 4.12(a-b) represent the embedding time for both watermarks. In plots, there is less difference in the values of quality parameters when both watermarks are compared.

Table 4.6: Processing Time (in seconds) for 5 videos using watermark1

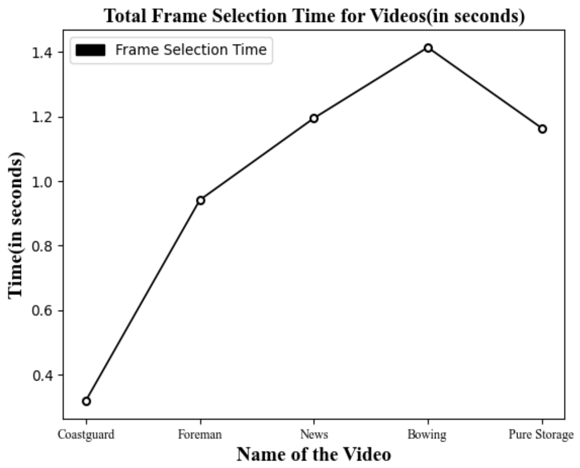
Video	Frame Selection Time	Embedding Time	Extraction Time
Coastguard	0.31845	251.7971	4.34
Foreman	0.94113	474.7267	6.23
News	1.19484	714.3616	7.56
Bowing	1.41451	950.4568	11.56
Pure_Storage	1.16416	1100.3613	13.78

Table 4.7: Processing Time (in seconds) for 5 videos using watermark2

Video	Frame Selection Time	Embedding Time	Extraction Time
Coastguard	0.31845	230.7971	4.14
Foreman	0.94113	460.2656	6.21
News	1.19484	730.3616	8.23
Bowing	1.41451	962.4568	12.12
Pure_Storage	1.16416	1088.2613	13.30

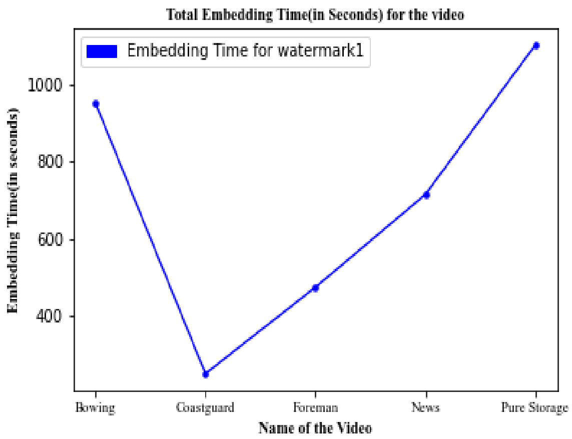


Average Frame Selection Time for GBT-SVD

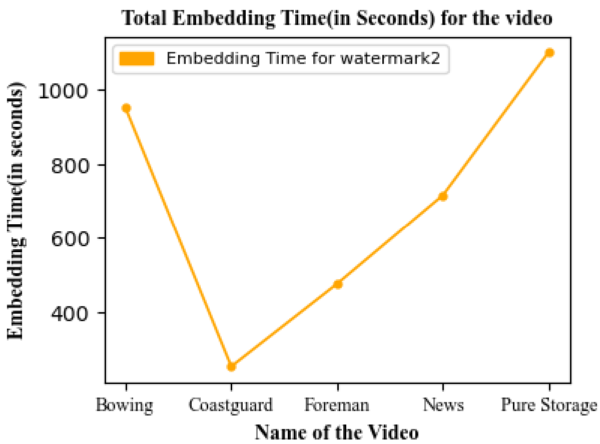


Average Frame Selection Time for GBT-SVD-GWO-GA

Figure 4.10,4.11: Plot of Frame Selection Time w.r.t the videos taken in the study



(a) Average Embedding Time for Watermark1



(b) Average Embedding Time for Watermark2

Figure 4.12(a-b): Plot of Embedding Time taken for Watermark 1 and 2.

Table 4.8: Processing Time (in seconds) for 5 videos using watermark1 for GBT-SVD

Video	Frame Selection Time	Embedding Time
Coastguard	0.31845	1.2614
Foreman	0.94113	2.5288
News	1.19484	4.9685
Bowing	1.41451	5.3493
Pure_Storage	1.16416	5.9485

Table 4.9: Comparison of Processing Time (in seconds) for 5 videos using watermark1

Video	Frame Selection Time	Embedding Time using GBT-SVD-GWO-GA	Embedding Time using GBT-SVD
Coastguard	0.31845	251.7971	1.2614
Foreman	0.94113	474.7267	2.5288
News	1.19484	714.3616	4.9685
Bowing	1.41451	950.4568	5.3493
Pure_Storage	1.16416	1100.3613	5.9485

Table 4.9 signifies the embedding time comparison of both techniques. It can be noted from Figure 4.13 that the embedding time of the optimization technique (GBT-SVD-GWO-GA) is comparatively higher than the simple embedding technique (GBT-SVD) given in Table 4.8. Embedding time is also processor-dependent. The optimization algorithm works on the number of iterations. More iterations help in improving the quality of the watermarked frame but at the cost of time.

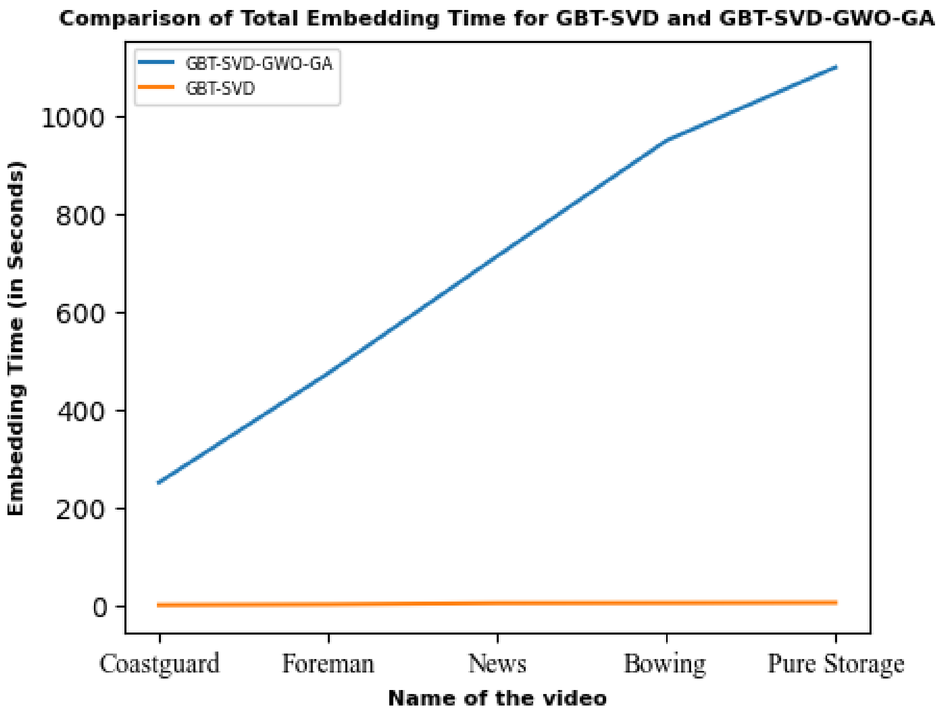


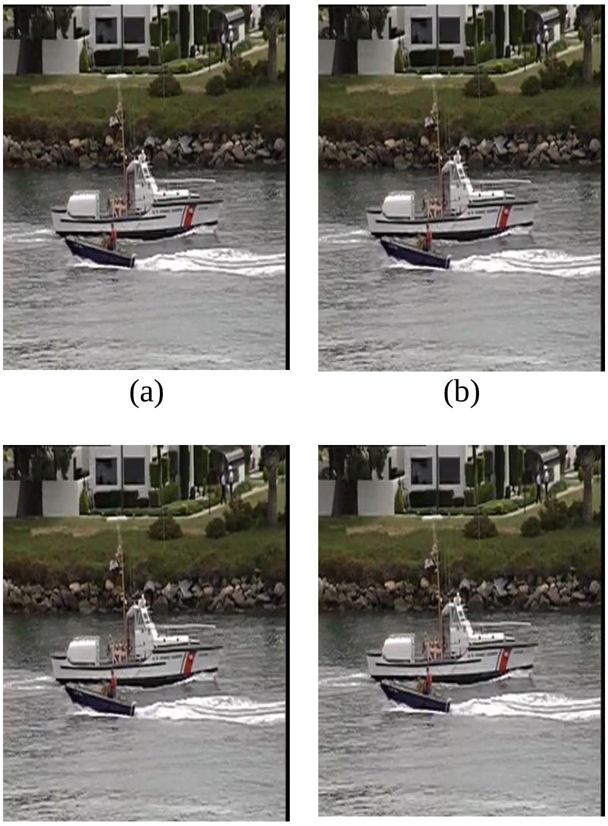
Figure 4.13: Comparison of Average Embedding Time for GBT-SVD and GBT-SVD-GWO-GA

4.4 Processing Attacks

This Section represents various signal processing attacks, and the efficiency of the proposed embedding technique is tested after applying multiple signal processing attacks on the watermarked data. The proposed technique's robustness is tested against multiple attack scenarios such as Gaussian Noise, Sharpening, Rotation, Blurring, and JPEG Compression. Series of experiments have been conducted to attack every watermarked frame to measure quality loss. The robustness of the technique entirely depends on PSNR, SSIM, NC, and BER values. A detailed description is given below:

4.4.1 Gaussian Noise Attack

In the gaussian Noise attack, a random gaussian sequence of real values {0,0.0001, 0.001, 0.01} is added to all frames of the watermarked video using watermark 1. The value NA indicates no attack is applied. The gaussian Noise attack is applied to the input video's watermarked frames to check the proposed technique's robustness. It is used in both GBT-SVD(T2) and GBT-SVD-GWO-GA (T1). The random noise sequence values of 0.0001,0.001 and 0.01 are taken. The comparative analysis is done on all values taken for both techniques.



(a) (b)

(c) (d)

Figure 4.14(a-d): Attacked watermarked frames of Cost guard video (a) No Attack (b) Gaussian Noise attack with 0.0001 Value, (c) Gaussian Noise attack with 0.001 Value and (d) Gaussian Noise attack with 0.01 Value of coastguard video

The proposed technique's performance is realized by applying gaussian attacks to both GBT-SVD and GBT-SVD-GWO-GA techniques with 3 variance values 0.0001,0.001 and 0.01. The results are represented in the following tables, and comparative analysis is done on both methods after the Gaussian noise attack is applied. Figure 4.14 represents attacked watermarked frames after a gaussian noise attack.

Table 4.10 Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using variance 0.0001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	39.7634	0.97748	0.99904	0.025149
Foreman	39.8525	0.97614	0.99904	0.025092
News	39.8598	0.96966	0.99921	0.025088
Bowing	39.8364	0.95935	0.99881	0.025102
Pure_Storage	39.7844	0.96118	0.99869	0.025135

Table 4.11: Results of GBT-SVD using Watermark 1 after Gaussian Noise Variance 0.0001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	34.8989	0.97662	0.99103	0.028654
Foreman	35.1160	0.97355	0.99139	0.028478
News	35.0360	0.96684	0.99239	0.028542
Bowing	34.7400	0.95602	0.98943	0.028786
Pure_Storage	34.7543	0.96857	0.98887	0.028773

Table 4.12: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD against Gaussian Noise Variance 0.0001

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2
PSNR	39.76	34.89	39.85	35.11	39.85	35.03	39.83	34.74	39.78	34.75
SSIM	0.977	0.976	0.976	0.973	0.969	0.966	0.969	0.966	0.961	0.968
NC	0.999	0.991	0.999	0.991	0.99	0.99	0.99	0.99	0.99	0.99
BER	0.025	0.028	0.025	0.028	0.025	0.028	0.025	0.028	0.025	0.028

Table 4.10 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.11 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.12 represents the comparative analysis of both of them against Gaussian noise variance 0.0001.

Table 4.13: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using variance 0.001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	30.0503	0.8373	0.99088	0.033278
Foreman	30.2636	0.8349	0.99111	0.033043
News	30.1124	0.8107	0.99243	0.033208
Bowing	30.0832	0.7498	0.98865	0.033241
Pure_Storage	30.0856	0.7493	0.98768	0.033239

Table 4.14: Results of GBT-SVD using Watermark 1 after Gaussian Noise Variance 0.001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	34.8989	0.97662	0.99103	0.028654
Foreman	35.11605	0.97355	0.991395	0.028478
News	35.03607	0.96684	0.992393	0.028542
Bowing	34.74003	0.95602	0.98943	0.028786
Pure_Storage	34.7543	0.96857	0.988878	0.028773

Table 4.15: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD against Gaussian Noise Variance 0.001

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	30.05	29.18	30.26	29.60	30.11	29.26	39.83	34.74	30.08	29.15
SSIM	0.83	0.83	0.834	0.84	0.81	0.80	0.74	0.73	0.74	0.79
NC	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
BER	0.033	0.034	0.033	0.033	0.033	0.034	0.025	0.028	0.033	0.034

Table 4.13 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.14 describes the estimation of the proposed technique's performance parameters without optimization, and Table 4.15 represents the comparative analysis of both of them against Gaussian noise variance 0.001.

Table 4.16: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using variance 0.01

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	20.2687	0.45548	0.91896	0.049337
Foreman	20.7113	0.43355	0.92450	0.048288
News	20.6704	0.49248	0.93639	0.048378
Bowing	20.2502	0.35278	0.90143	0.049382
Pure_Storage	20.3198	0.31245	0.89568	0.049229

Table 4.17: Results of GBT-SVD using Watermark 1 after Gaussian Noise Variance 0.01

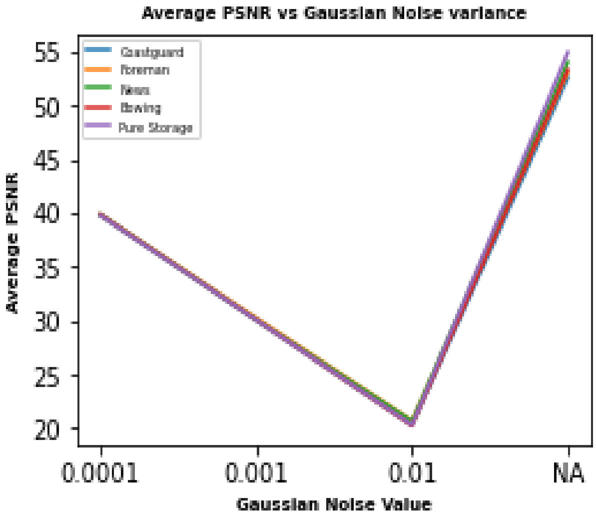
Video	PSNR (dB)	SSIM	NC	BER
Coastguard	20.1843	0.46125	0.92212	0.049543
Foreman	20.8119	0.44313	0.92700	0.048058
News	20.5122	0.49327	0.93742	0.048751
Bowing	20.1141	0.33756	0.90684	0.049716
Pure_Storage	20.2006	0.34762	0.90556	0.049516

Table 4.18: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD against Gaussian Noise Variance 0.01

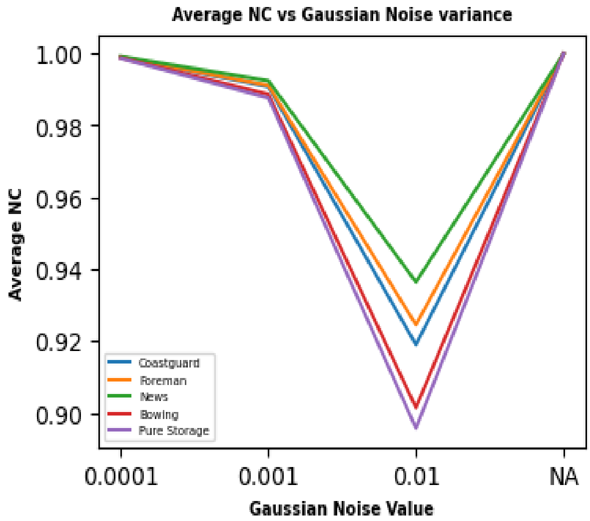
Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2
PSNR	20.26	20.18	20.71	20.81	20.67	20.51	20.25	20.11	20.31	20.20
SSIM	0.45	0.46	0.43	0.44	0.49	0.49	0.35	0.33	0.31	0.34
NC	0.91	0.92	0.92	0.92	0.93	0.93	0.90	0.90	0.89	0.90
BER	0.049	0.049	0.048	0.048	0.048	0.048	0.049	0.049	0.049	0.049

Table 4.16 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.17 represents the calculation of the proposed technique's performance parameters

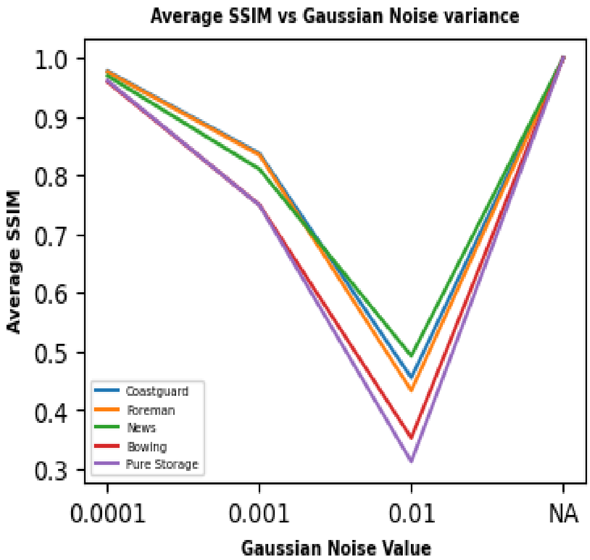
without optimization, and Table 4.18 represents the comparative analysis of both of them against Gaussian noise variance 0.01. Plots in Figure 4.15 describe the calculation of performance parameters against Gaussian noise variance 0.001,0.001,0.01 and 0 for the optimized proposed method.



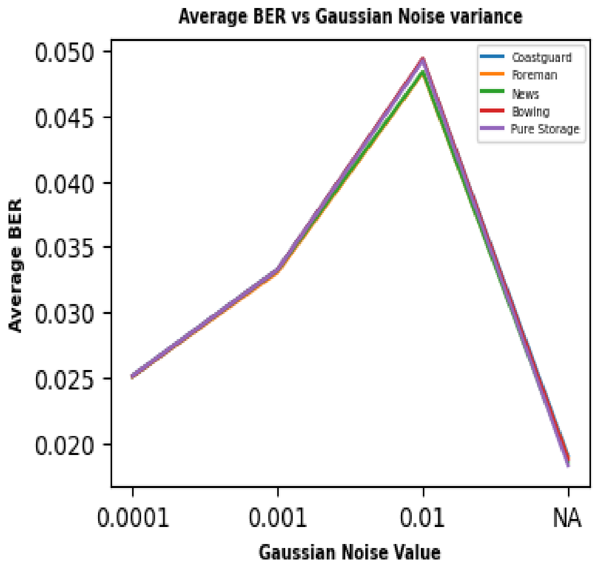
(a) Average comparison of PSNR VS Gaussian Noise Variance



(b) Average comparison of NC VS Gaussian Noise Variance



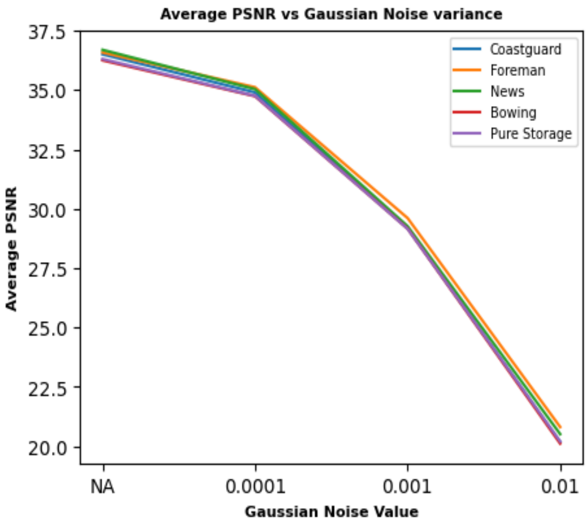
(c) Average comparison of SSIM VS Gaussian Noise Variance



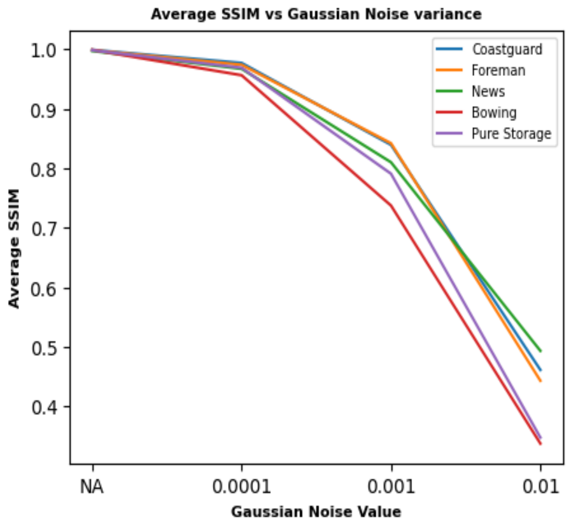
(d) Average comparison of BER VS Gaussian Noise Variance

Figure 4.15(a-d): Plot of PSNR, NC, SSIM and BER w.r.t Gaussian Noise Variance using watermark

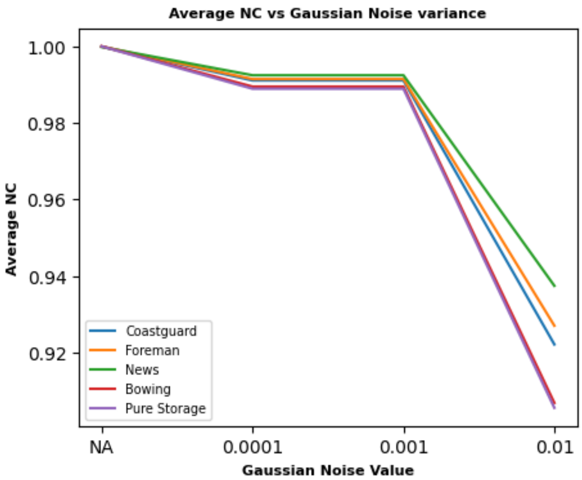
Plots in Figure 4.15 describe the calculation of performance parameters against Gaussian noise variance 0.001,0.001,0.01 and 0 for the proposed optimized technique.



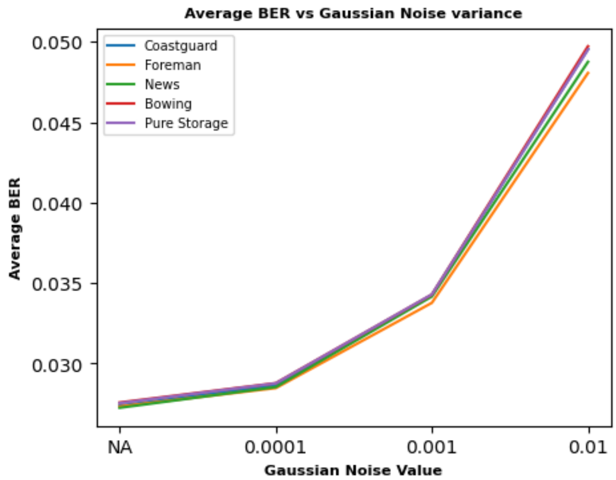
(a)Average PSNR against Gaussian Noise Variance



(b) Average SSIM against Gaussian Noise Variance



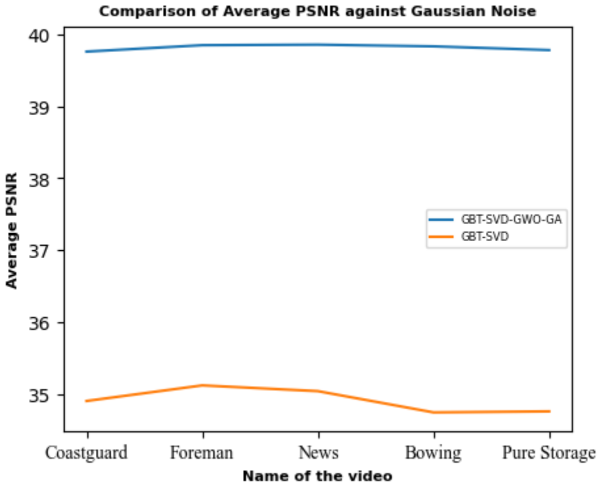
(c)Average NC against Gaussian Noise Variance



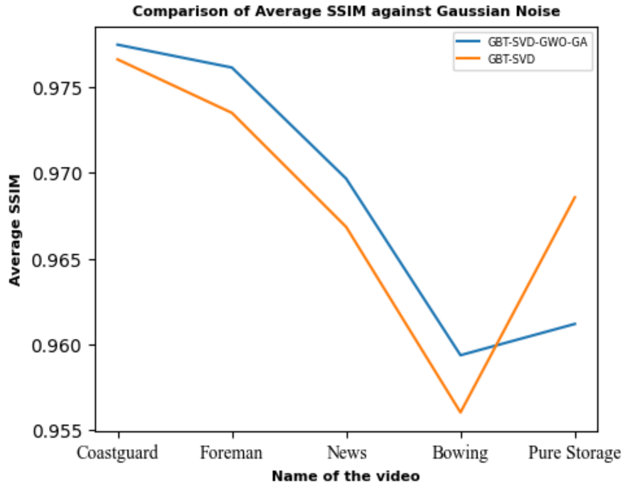
(d)Average BER against Gaussian Noise Variance

Figure 4.16(a-d): Plot of PSNR, SSIM, NC, BER w.r.t the videos taken in the proposed work for GBT-SVD against Gaussian Noise Attack

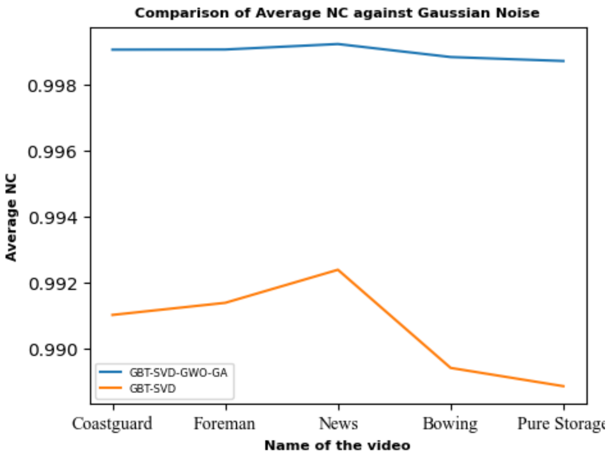
Plots in Figure 4.16 describe the calculation of performance parameters against Gaussian noise variance 0.001,0.001,0.01 and 0 for the proposed technique(GBT-SVD) without optimization.



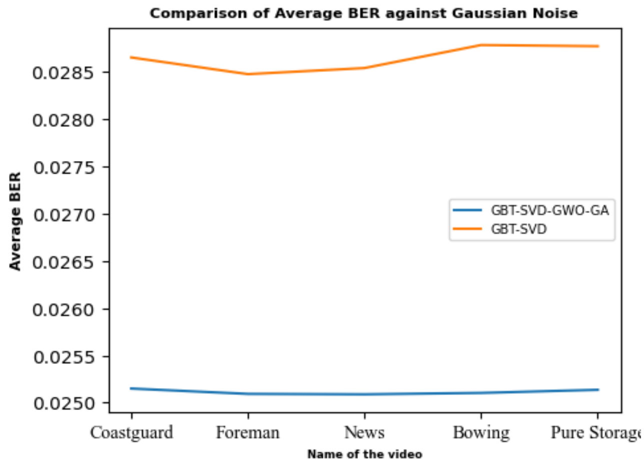
(a)Average PSNR against Gaussian Noise variance 0.0001



(b) Average SSIM against Gaussian Noise variance 0.0001



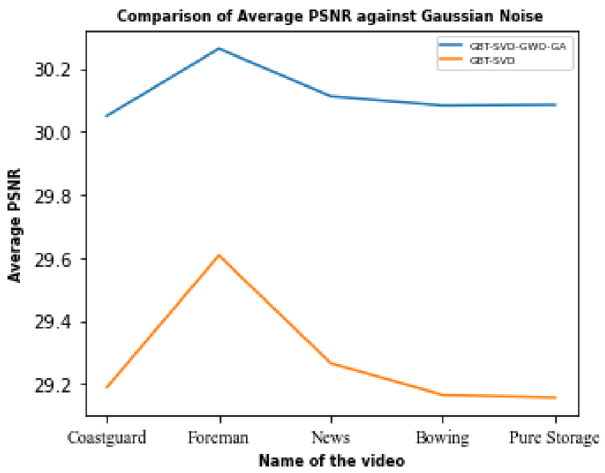
(c)Average NC against Gaussian Noise variance 0.0001



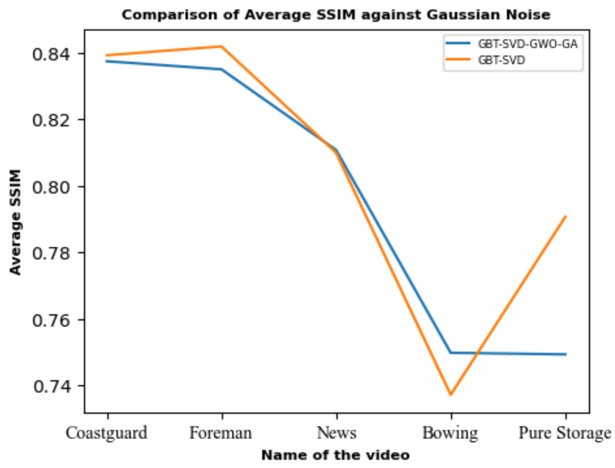
(d)Average BER against Gaussian Noise variance 0.0001

Figure 4.17(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Gaussian Noise Variance 0.0001

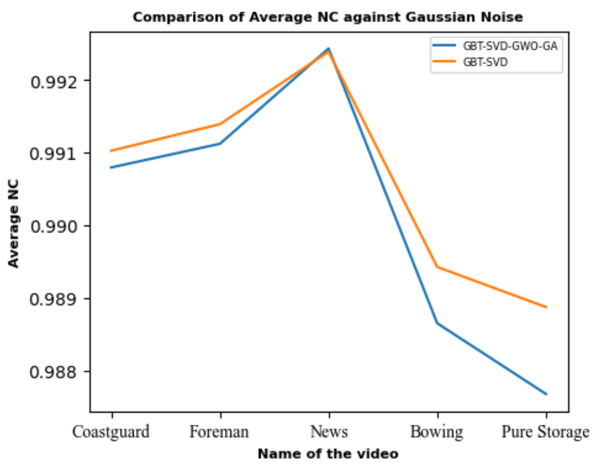
Plots in Figure 4.17 describe the comparative analysis of the proposed method with and without optimization against Gaussian noise variance 0.0001.



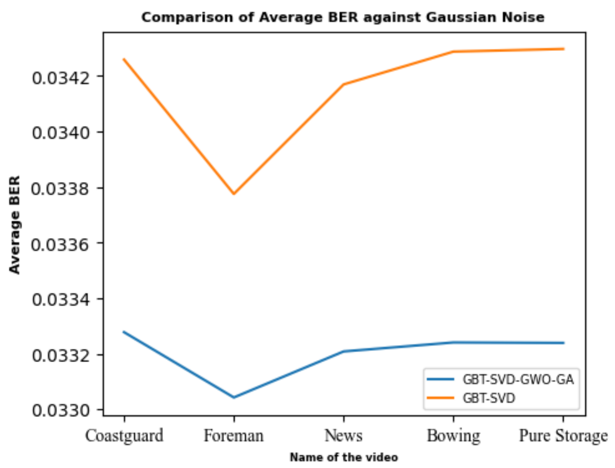
(a)Average PSNR against Gaussian Noise variance 0.001



(b) Average SSIM against Gaussian Noise variance 0.001



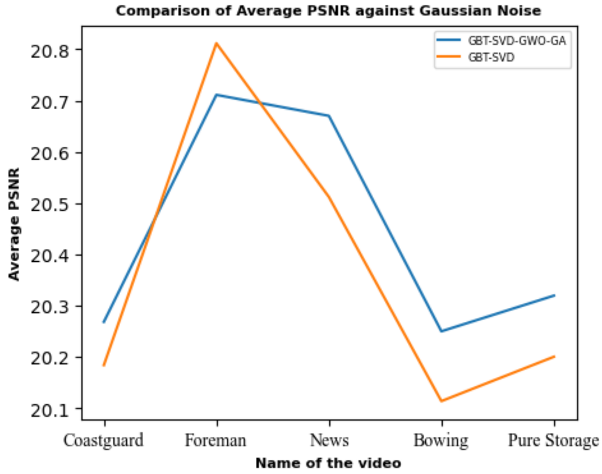
(c)Average NC against Gaussian Noise variance 0.001



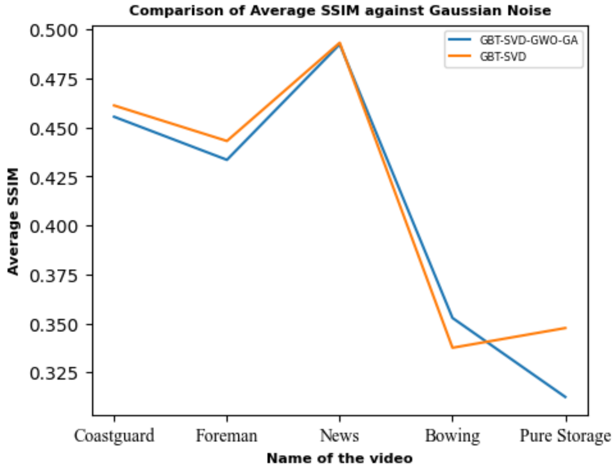
(d)Average BER against Gaussian Noise variance 0.001

Figure 4.18(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Gaussian Noise Variance 0.001

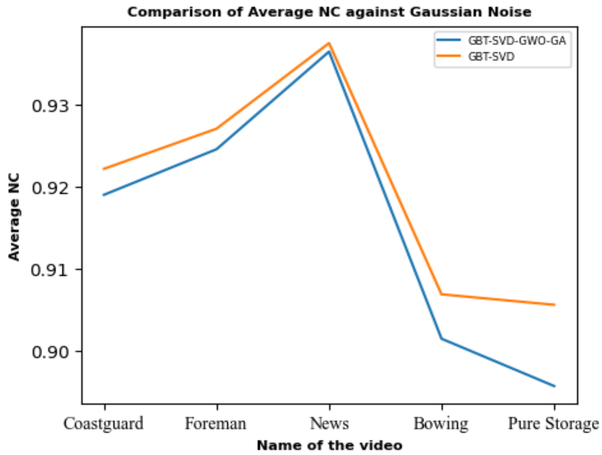
Plots in Figure 4.18 describe the comparative analysis of the proposed method with and without optimization against Gaussian noise variance 0.001.



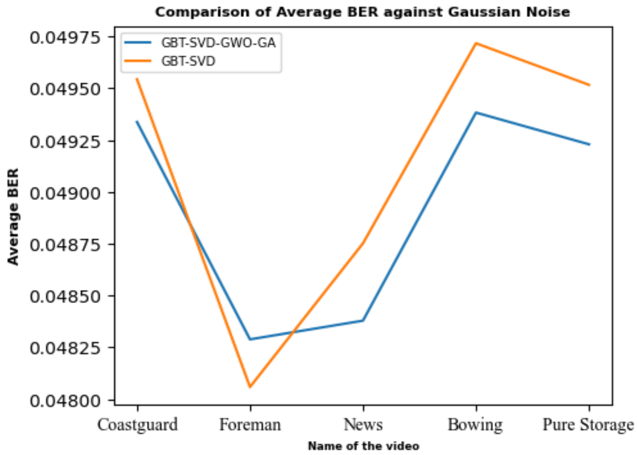
(a)Average PSNR against Gaussian Noise variance 0.01



(b) Average SSIM against Gaussian Noise variance 0.01



(c)Average NC against Gaussian Noise variance 0.01



(d)Average BER against Gaussian Noise variance 0.01

Figure 4.19(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Gaussian Noise Variance 0.01

Plots in Figure 4.19 describe the comparative analysis of the proposed method with and without optimization against Gaussian noise variance 0.01.

4.4.2 Sharpening Attack

In the Sharpening attack, a random sequence of real values {0,0.0001, 0.001, and 0.01} is added to the watermarked video's all frames using watermark 1. It can be noted from plots in Figure 4.21 that the average PSNR, NC, and SSIM decrease with an increase in attack value, and BER increases with an increase in attack value. The higher value of PSNR, NC, SSIM justifies the robustness of the proposed technique against sharpening attack. The value of sharpening attack for 0.0001 and 0.001 is approximately the same. Sharpening attack has a negligible difference on the watermarked frame The higher value of NC indicates the robustness of the proposed technique. Figure 4.21 compiles the Sharpening attack results for all quality parameters using values {0,0.0001, 0.001, and 0.01} for all 5 videos taken in research work. PSNR, SSIM, NC and BER values of all the videos are similar. The value of NA in graphs means no attack is applied, and higher values of PSNR, NC, SSIM will be obtained for NA. Lower values of BER are obtained for NA. The value 0 indicates no attack is applied. The sharpening attack is used to highlight details of the image. Figure 4.20 represents attacked watermarked frames using the different variance of this attack.

Figure 4.20(a-d): Attacked watermarked frames of Foreman video (a) No Attack (b) Sharpening attack with 0.0001 Value, (c) Sharpening attack with 0.001 Value and (d) Sharpening attack with 0.01 Value

Table 4.19: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using Sharpening attack variance 0.0001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	50.054	0.99887	0.99994	0.01999
Foreman	49.694	0.99837	0.99993	0.02012
News	49.470	0.99845	0.99993	0.02021
Bowing	49.912	0.99753	0.99992	0.02003
Pure_Storage	50.078	0.99775	0.99991	0.01997

Table 4.20: Results of GBT-SVD using Watermark 1 after Sharpening Attack Variance 0.0001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.4152	0.997288	0.999822	0.027461
Foreman	36.49322	0.996722	0.999845	0.027403
News	36.55293	0.995473	0.999717	0.027358
Bowing	36.15699	0.996428	0.999898	0.027657
Pure_Storage	36.21914	0.996277	0.999862	0.027611

Table 4.21: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after sharpening attack using variance 0.0001

Parameters	**Coastguard**		**Foreman**		**News**		**Bowing**		**Pure_Storage**	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	50.05	36.41	49.69	36.49	49.47	36.55	49.91	36.15	50.07	36.21
SSIM	0.998	0.997	0.998	0.996	0.998	0.995	0.997	0.996	0.997	0.996
NC	0.999	0.99	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999
BER	0.019	0.027	0.020	0.027	0.020	0.027	0.020	0.027	0.019	0.027

Table 4.19 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.20 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.21 represents the comparative analysis of both of them against sharpening attack variance 0.0001.

Table 4.22: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using Sharpening attack variance 0.001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	50.0544	0.998877	0.99994	0.01999
Foreman	49.6948	0.998375	0.99993	0.02012
News	49.4709	0.998456	0.99993	0.02021
Bowing	49.9124	0.997535	0.99992	0.02003
Pure_Storage	50.0782	0.997752	0.99991	0.01997

Table 4.23: Results of GBT-SVD using Watermark 1 after Sharpening Attack Variance 0.001

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.4152	0.997288	0.999822	0.027461
Foreman	36.4932	0.996722	0.999845	0.027403
News	36.5529	0.995473	0.999717	0.027358
Bowing	36.1569	0.996428	0.999898	0.027657
Pure_Storage	36.2191	0.996277	0.999862	0.027611

Table 4.24: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1

Parameters	**Coastguard**		**Foreman**		**News**		**Bowing**		**Pure_Storage**	
	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2
PSNR	52.57	36.50	53.05	36.58	54.00	36.69	53.28	36.25	54.91	36.30
SSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
NC	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
BER	0.019	0.027	0.018	0.027	0.027	0.018	0.027	0.027	0.018	0.027

Table 4.22 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.23 describes the estimation of the proposed technique's performance parameters without optimization, and Table 4.24 represents the comparative analysis of both of them against sharpening attack variance 0.001.

Table 4.25: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using Sharpening attack variance 0.01

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	50.054	0.99887	0.99994	0.01999
Foreman	49.694	0.99837	0.99993	0.020126
News	49.470	0.99845	0.99993	0.020215
Bowing	49.912	0.99753	0.99992	0.020036
Pure_Storage	50.078	0.99775	0.99991	0.019976

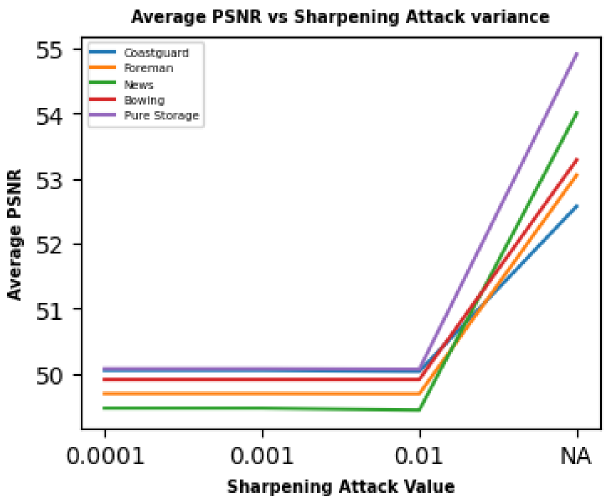
Table 4.26: Results of GBT-SVD using Watermark 1 after Sharpening Attack Variance 0.01

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.4152	0.99728	0.999822	0.027461
Foreman	36.4932	0.99672	0.999845	0.027403
News	36.55293	0.99547	0.999717	0.027358
Bowing	36.15699	0.99642	0.999898	0.027657
Pure_Storage	36.21914	0.99627	0.999862	0.027611

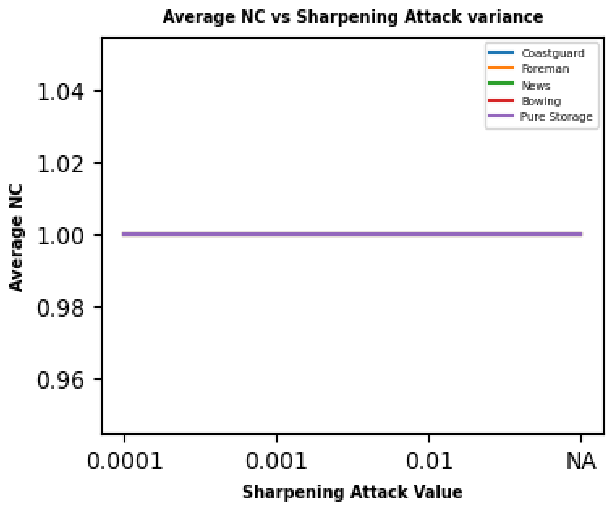
Table 4.27: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after sharpening attack using variance 0.01

Parameters	**Coastguard**		**Foreman**		**News**		**Bowing**		**Pure_Storage**	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	50.03	36.41	49.69	36.49	49.44	36.55	49.91	36.15	50.07	36.21
SSIM	0.998	0.997	0.998	0.996	0.998	0.995	0.997	0.996	0.997	0.996
NC	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999
BER	0.019	0.027	0.018	0.027	0.018	0.027	0.018	0.027	0.018	0.027

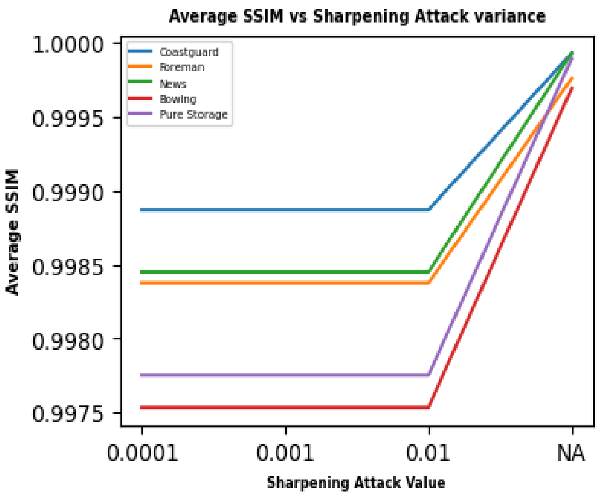
Table 4.25 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.26 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.27 represents the comparative analysis of both of them against sharpening attack variance 0.01.



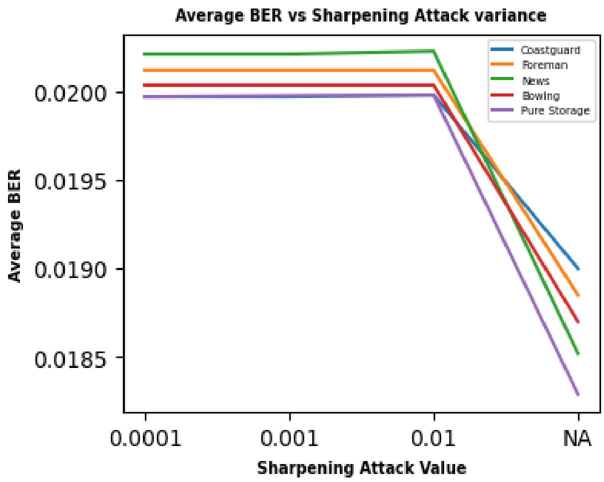
(a) Average comparison of PSNR against Sharpening Attack Variance



(b) Average comparison of NC against Sharpening Attack Variance



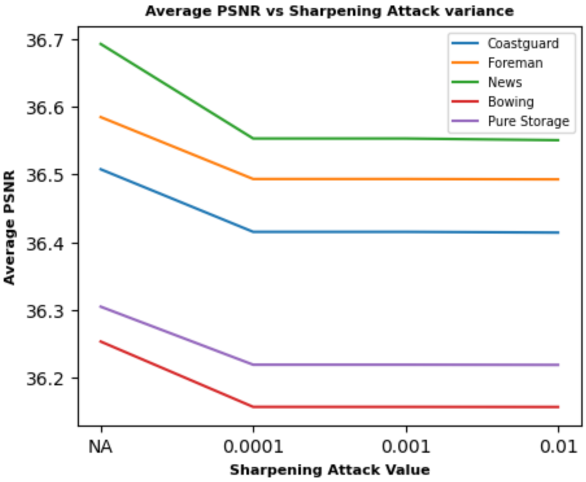
(c) Average comparison of SSIM against Sharpening Attack Variance



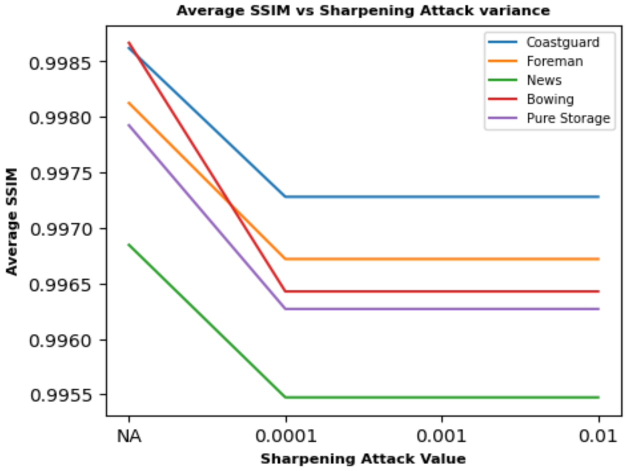
(d) Average comparison of BER against Sharpening Attack Variance

Figure 4.21(a-d): Plot of PSNR, NC ,SSIM, and BER w.r.t Sharpening Attack using watermark1

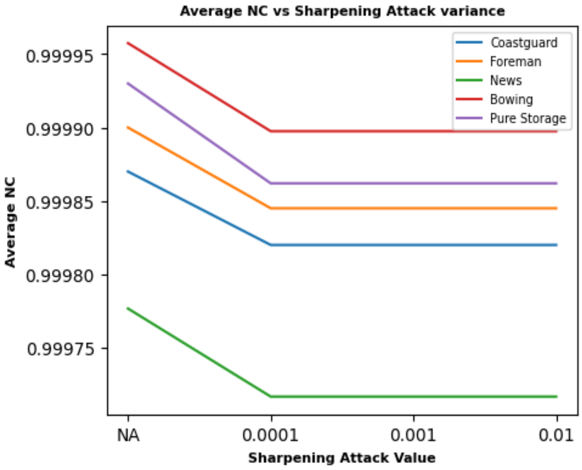
Figure 4.21 represents plots of performance parameters for the GBT-SVD technique against different sharpening attack variance values. The watermarked frames are subjected to sharpening attack variance values, and the calculation of performance parameters is done accordingly. It is estimated that the addition of sharpening noise variance does not impact the quality of the watermarked frame. The proposed optimized technique achieves good values of quality metrics after this attack is applied.



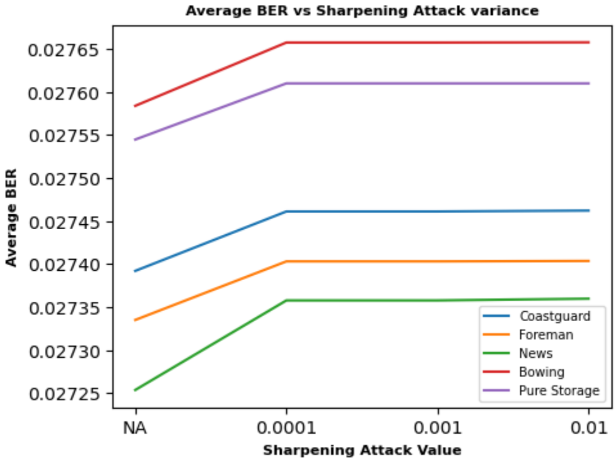
(a)Average PSNR against Sharpening Attack Variance



(b) Average SSIM against Sharpening Attack Variance



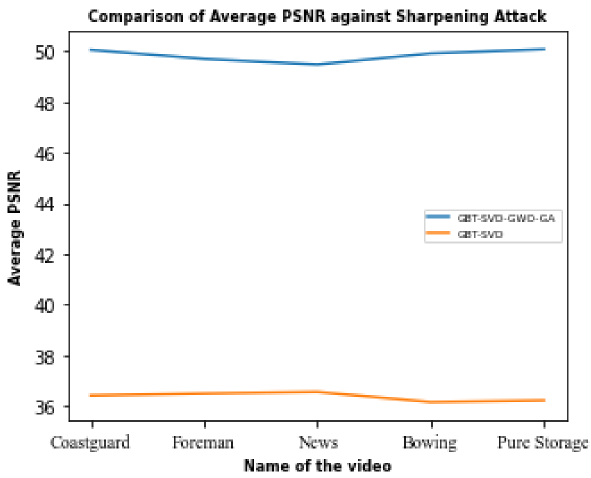
(c)Average NC against Sharpening Attack Variance



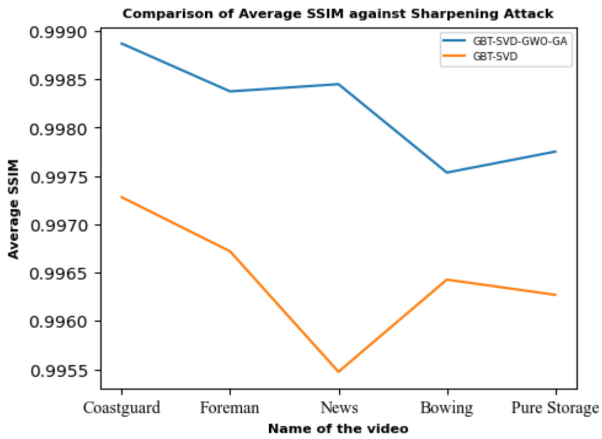
(d)Average BER against Sharpening Attack Variance

Figure 4.22(a-d): Plot of PSNR, SSIM, NC, BER w.r.t the videos taken in the proposed work for GBT-SVD against Sharpening Attack

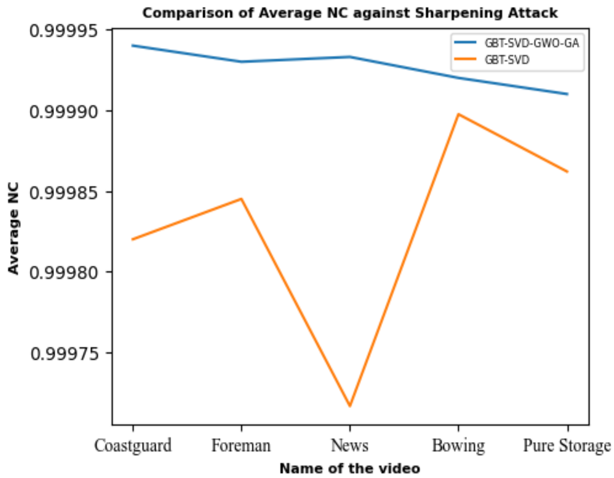
Figure 4.22 represents plots of performance parameters for the GBT-SVD technique against different sharpening attack variance values. The watermarked frames are subjected to sharpening attack variance values, and the calculation of performance parameters is done accordingly.



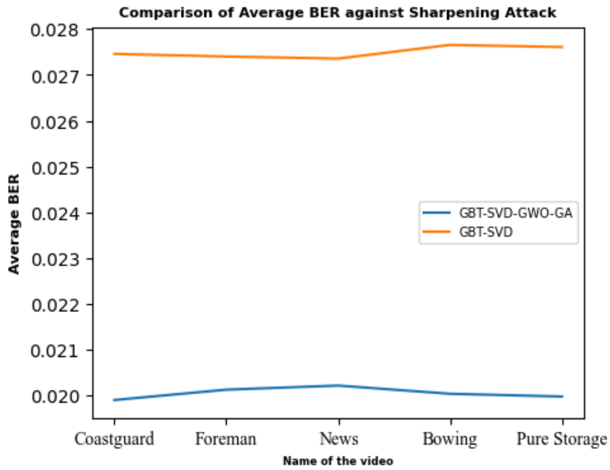
(a)Average PSNR against Sharpening Attack variance 0.0001



(b) Average SSIM against Sharpening Attack variance 0.0001



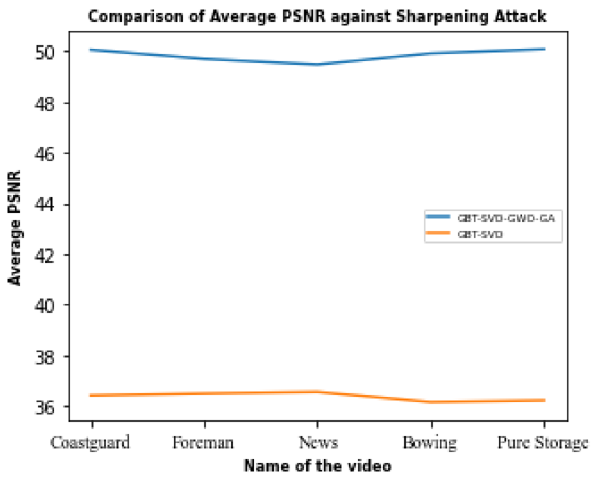
(c)Average NC against Sharpening Attack variance 0.0001



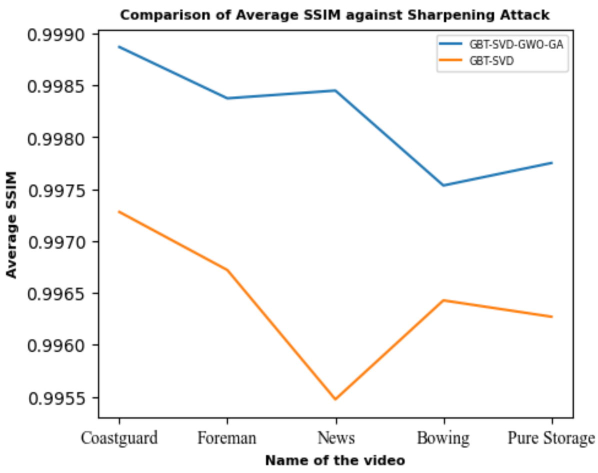
(d)Average BER against Sharpening Attack variance 0.0001

Figure 4.23(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Sharpening Attack Variance 0.0001

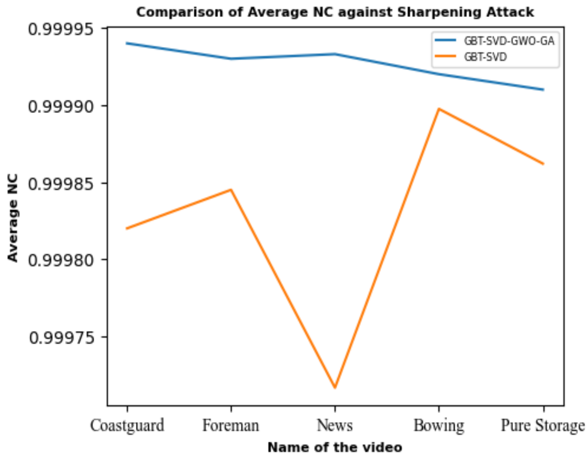
Plots in Figure 4.23 describe the comparative analysis of the proposed method with and without optimization against Sharpening attack variance 0.0001. The addition of 0.0001 does not impact the value of PSNR. The proposed techniques are found to be robust against this variance. The performance of the optimized watermarking scheme is better than GBT-SVD.



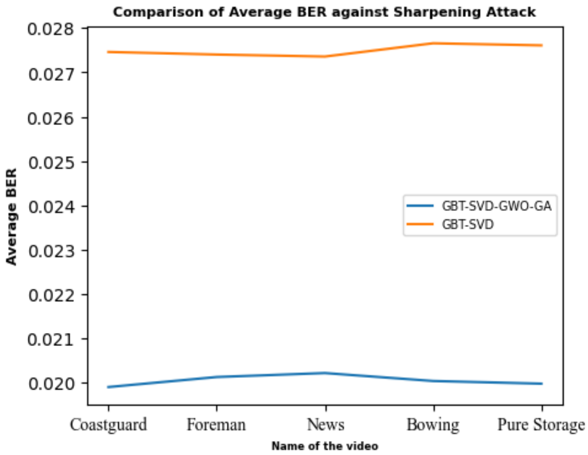
(a)Average PSNR against Sharpening Attack variance 0.001



(b) Average SSIM against Sharpening Attack variance 0.001



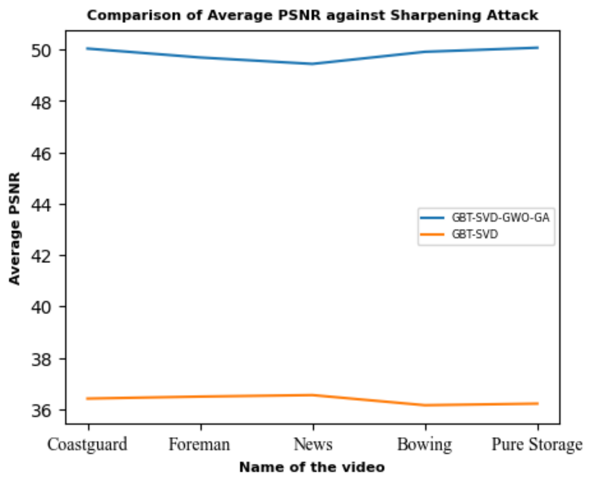
(c)Average NC against Sharpening Attack variance 0.001



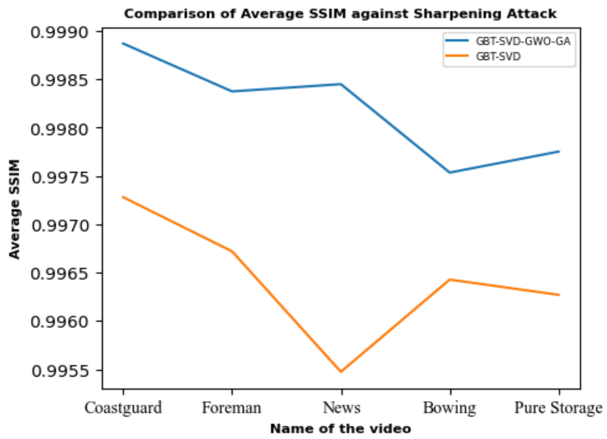
(d)Average BER against Sharpening Attack variance 0.001

Figure 4.24(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Sharpening Attack Variance 0.001

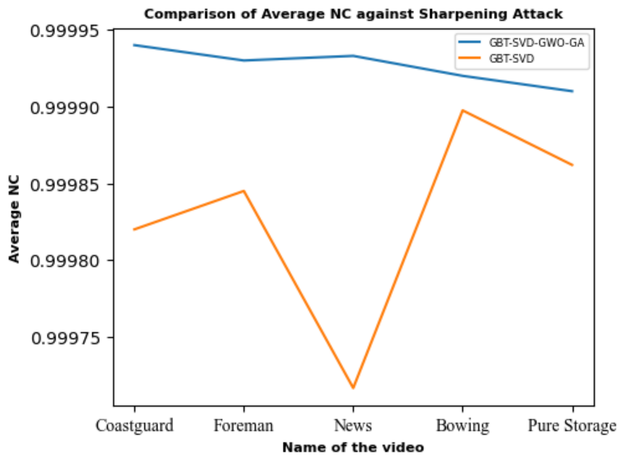
Plots in Figure 4.24 describe the comparative analysis of the proposed method with and without optimization against Sharpening attack variance 0.001. The addition of 0.001 does not impact the value of PSNR. The proposed techniques are found to be robust against this variance. The values were found similar to sharpening variance 0.0001, which implies there is not much variance after sharpening attack is applied. The performance of the optimized watermarking scheme is better than GBT-SVD.



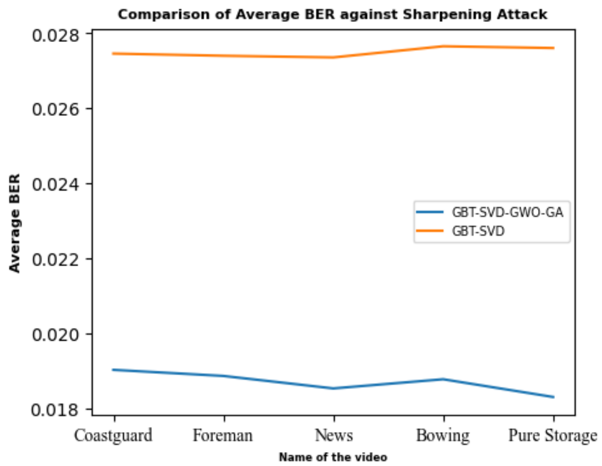
(a)Average PSNR against Sharpening Attack variance 0.01



(b) Average SSIM against Sharpening Attack variance 0.01



(c)Average NC against Sharpening Attack variance 0.01



(d)Average BER against Sharpening Attack variance 0.01

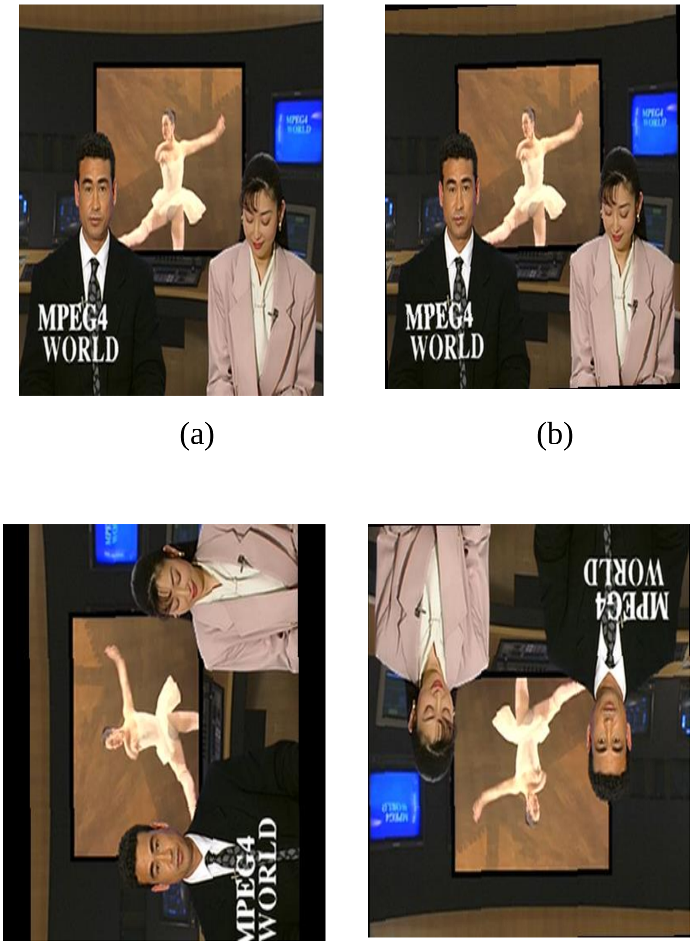
Figure 4.25(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Sharpening Attack Variance 0.01

Plots in Figure 4.25 describe the comparative analysis of the proposed method with and without optimization against Sharpening attack variance 0.01. The proposed techniques achieve the good value of robustness against this variance of sharpening attack. The performance of the optimized watermarking scheme is better than GBT-SVD.

4.4.3 Rotation Attack

In a Rotation attack, a watermarked frame is rotated with an angle of {0,1, 90,180} using watermark 1. The value 0 indicates no attack is applied. As shown in Figure 4.27 (a-d), as the average

PSNR, NC, SSIM deteriorates with an increase in attack value and BER increases with an increase in attack value. PSNR, SSIM, NC, and BER values of all the videos are similar. NA in graphs' value means no attack is applied. Higher values of PSNR, NC, SSIM will be obtained for NA. Figure 4.26(a-d) represents attacked watermarked frame after using different rotation attacks. The result calculation of these watermarked frames after rotation attack is described in table 4.28. Rotation attack directly impacts watermarked frames' quality as the pixels in the frames are rotated, so the major change is done. The proposed technique can only generate high values in rotation attack if we have a higher number of iterations. The performance of two methods GBT-SVD and GBT-SVD-GWO-GA, are similar after applying rotation attack.



(a) (b)

(c) (d)

Figure 4.26(a-d): Attacked watermarked frames of News Video (a) No Attack (b) Rotation attack with 10 degree, (c) Rotation attack with 90 degree and (d) Rotation attack with 180 degree

Table 4.28: Results of GBT-SVD-GWO-GA(T1) Embedding against Rotation attack (1 degree)

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	18.0658	0.44888	0.85343	0.055353
Foreman	20.8930	0.86287	0.92672	0.047878
News	18.2612	0.77991	0.88350	0.054761
Bowing	21.9432	0.75382	0.92522	0.045576
Pure_Storage	21.5925	0.81772	0.91337	0.046315

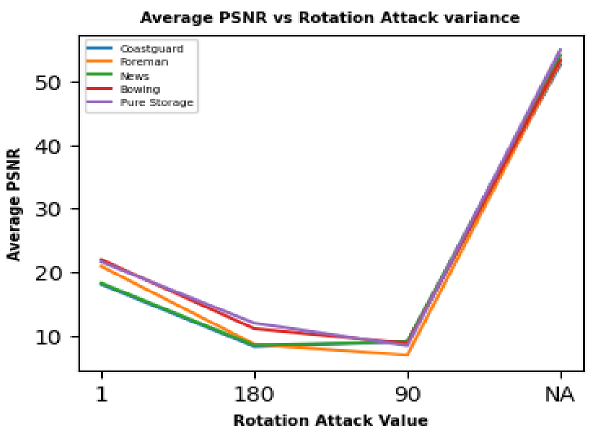
Table 4.29: Results of GBT-SVD(T2) Embedding against Rotation attack (1 degree)

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	18.1206	0.45904	0.85983	0.055186
Foreman	20.8504	0.86267	0.92807	0.047972
News	18.1076	0.77866	0.88263	0.055226
Bowing	21.9060	0.76837	0.93037	0.045652
Pure_Storage	21.408	0.80801	0.91819	0.046713

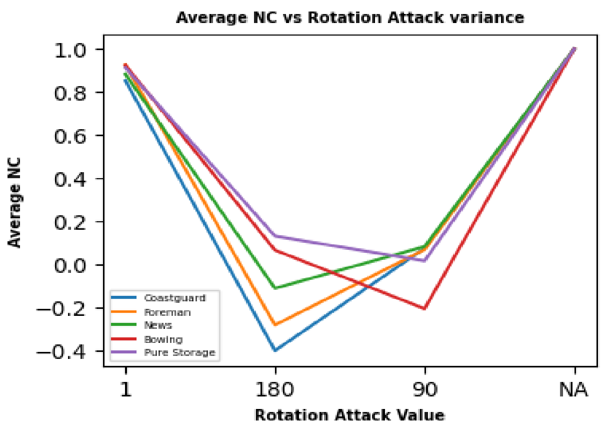
Table 4.30: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after rotating the watermarked frame by 1 degree

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	18.06	18.12	20.89	20.85	18.26	18.10	21.94	21.90	21.59	21.40
SSIM	0.448	0.459	0.862	0.862	0.779	0.778	0.753	0.768	0.817	0.808
NC	0.853	0.859	0.926	0.928	0.883	0.882	0.925	0.930	0.913	0.918
BER	0.055	0.055	0.047	0.047	0.054	0.055	0.045	0.045	0.046	0.046

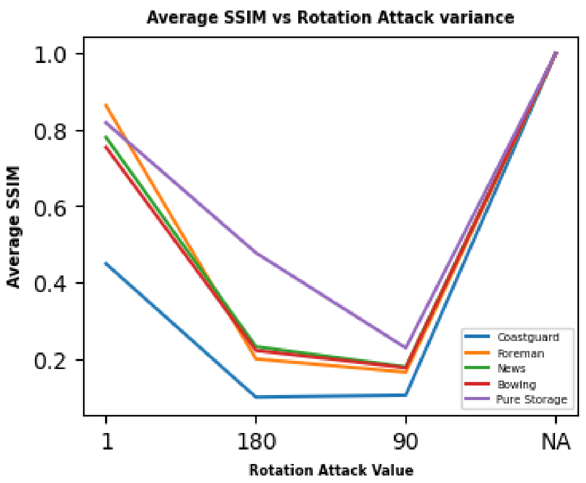
Table 4.28 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.29 describes the estimation of the proposed technique's performance parameters without optimization, and Table 4.30 represents the comparative analysis of both of them against rotation attack.



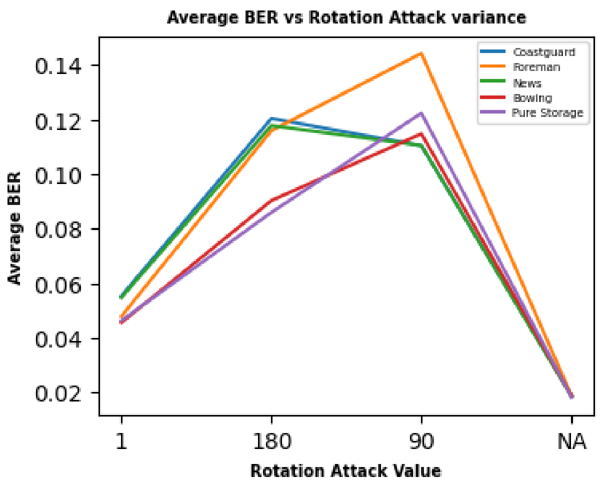
(a) Average comparison of PSNR against Rotation attack Variance



(b) Average comparison of NC against Rotation attack Variance



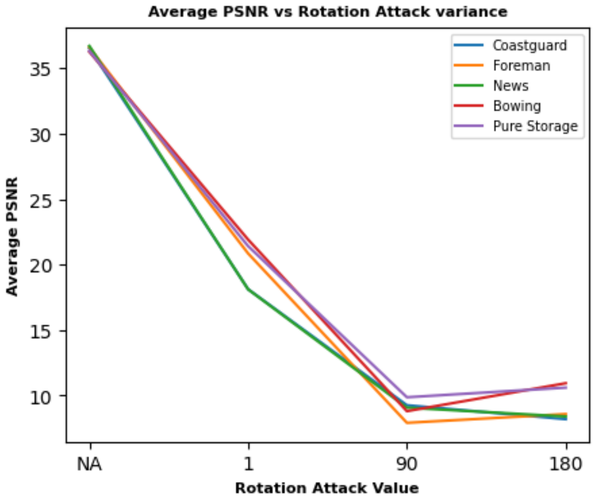
(c) Average comparison of SSIM against Rotation attack Variance



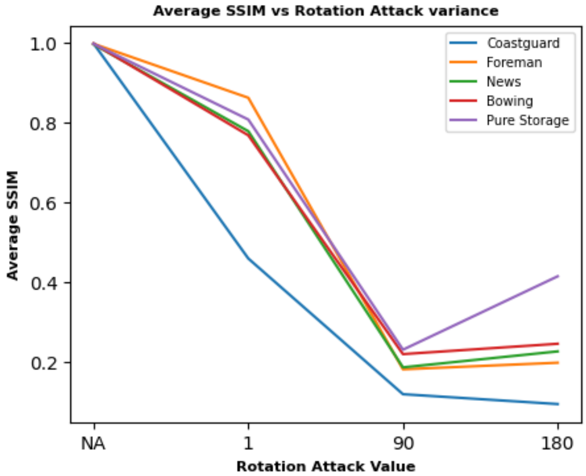
(d) Average comparison of BER against Rotation attack Variance

Figure 4.27(a-d): Plot of PSNR, NC, SSIM, and BER for GBT-SVD-GWO-GA against Rotation attack using watermark1

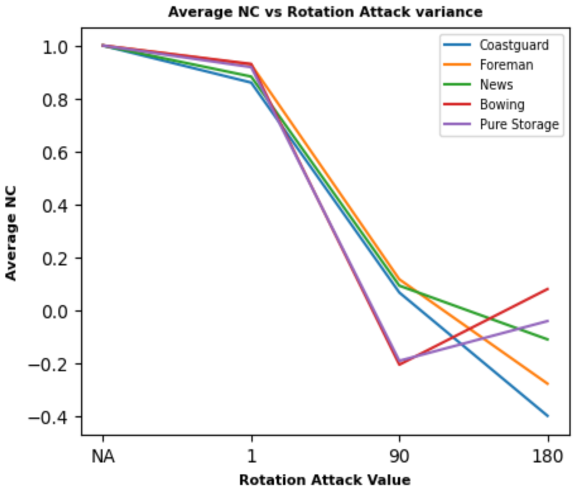
Figure 4.27 explains the performance of the proposed technique GBT-SVD-GWO-GA after attacks have been applied. The proposed technique is generating better robustness values comparative to rotation attacks. This attack directly changes pixel values. That is why we are getting lower values of quality metrics with increase in values of rotation degree.



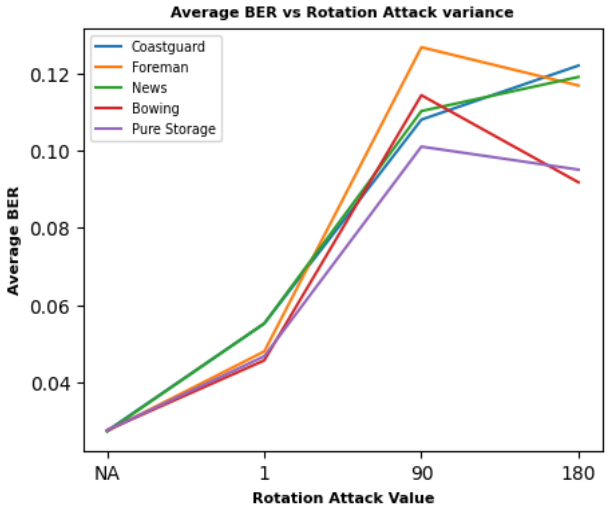
(a)Average PSNR against Rotation Attack Variance



(b) Average SSIM against Rotation Attack Variance



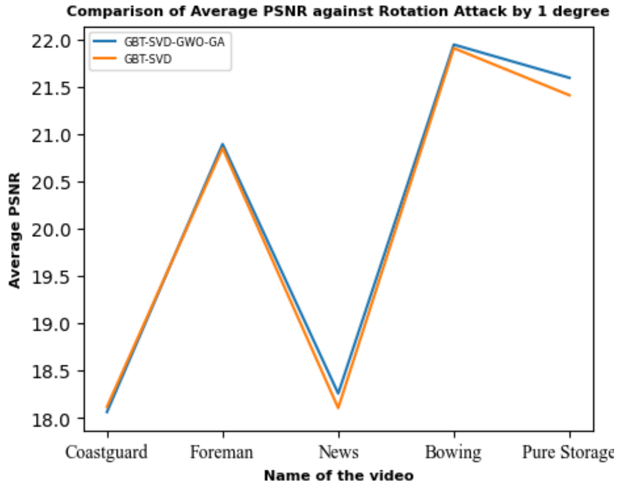
(c)Average NC against Rotation Attack Variance



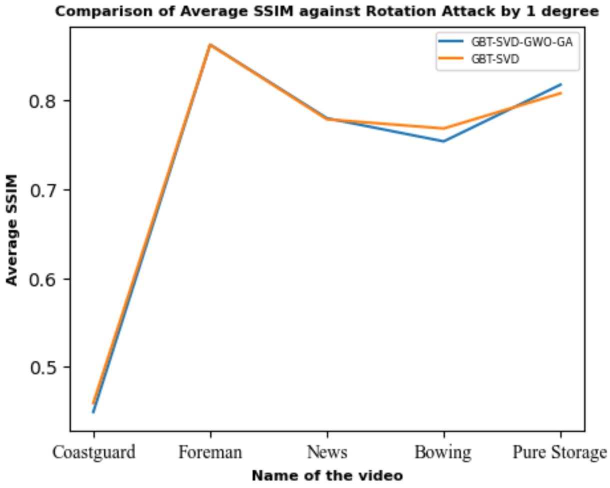
(d)Average BER against Rotation Attack Variance

Figure 4.28(a-d): Plot of PSNR, SSIM, NC, BER w.r.t the videos taken in the proposed work for GBT-SVD against Rotation Attack

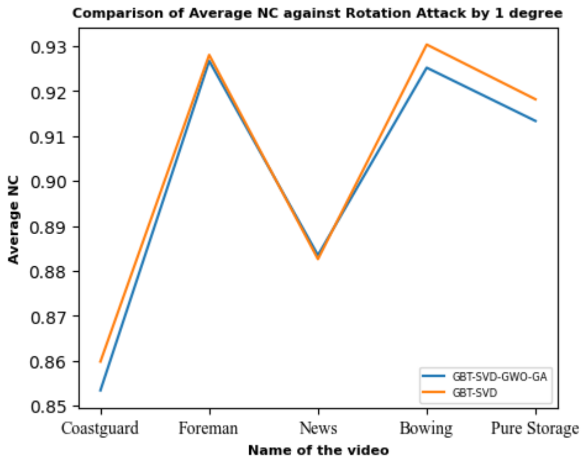
Plots in Figure 4.28 describe performance parameters calculation against rotation noise variance 1,90,180 and 0 for the proposed technique(GBT-SVD) without optimization.



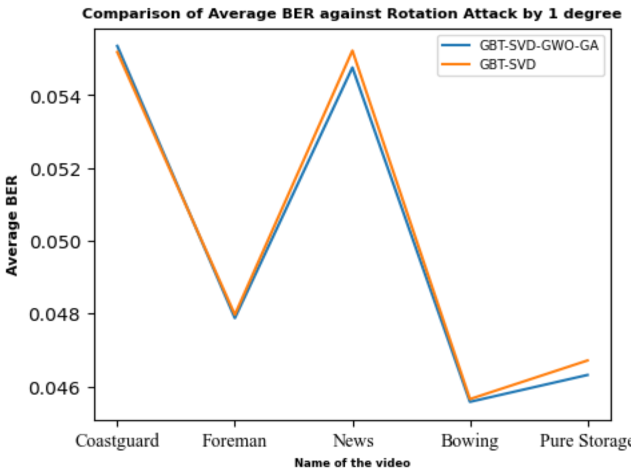
(a)Average PSNR with Rotation Attack (1 degree)



(b) Average SSIM with Rotation Attack (1 degree)



(c)Average NC with Rotation Attack (1 degree)



(d)Average BER with Rotation Attack (1 degree)

Figure 4.29(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Rotation Attack (1 degree)

It can be identified from the plots in Figure 4.29 that there is no significant difference when rotation attack is applied on watermarked frames using both techniques. The proposed optimization technique will provide high values of PSNR if the number of iterations is increased. The increasing number of iterations will also result in the high value of quality metrics in the proposed optimized technique.

4.4.4 Blurring Attack

In blurring attack, a random sequence of real values {0,2.05, 3.05, 4.05} is added to the watermarked video's all frames using watermark 1. The value 0 indicates no attack is applied.It can be seen from plots in figure 4.30, the average PSNR, NC, and SSIM decrease with an increase in attack value, and BER increases with an increase in attack value. Plots in Figure 4.32 compiles the blurring attack for all quality parameters using values {0,2.05, 3.05, 4.05} for all 5 videos taken in research work. PSNR, SSIM, NC, and BER values of all the videos are similar. The value of NA in graphs means no attack is applied, and higher values of PSNR, NC, SSIM will be obtained for NA. Lower values of BER are obtained for NA. The watermarked frames after this attack are represented using Figure 4.31(a-d). Table 4.31 represents the calculation of quality parameters after blurring attack. It has been observed that a higher number of frames were selected from the Pure_Storage video, so maximum embedding time is consumed for this video. The watermarked frames are represented in figure 4.30.

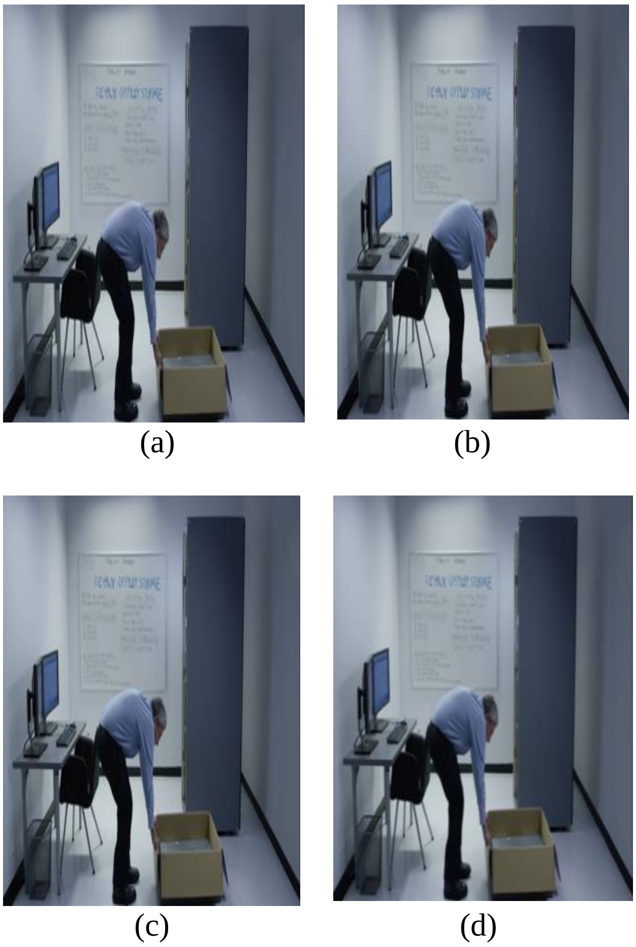


Figure 4.30(a-d): Attacked watermarked frames of Pure_Storage Video (a) No Attack (b) Blurring attack with 2.05 value, (c) Blurring attack with 3.05 value and (d) Blurring attack with 4.05 value

Table 4.31: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using Blurring Attack variance 2.05

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	39.5519	0.99313	0.99897	0.025283
Foreman	43.4012	0.99725	0.99966	0.023055
News	36.0007	0.99299	0.99808	0.027777
Bowing	40.9786	0.99301	0.99908	0.024403
Pure_Storage	37.8222	0.98741	0.99787	0.026453

Table 4.32: Results of GBT-SVD using Watermark 1 after Blurring Attack Variance 2.05

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	34.3011	0.98957	0.99831	0.029154
Foreman	35.6484	0.99507	0.99934	0.028053
News	32.6903	0.988183	0.99706	0.030599
Bowing	34.7904	0.990425	0.99872	0.028744
Pure_Storage	34.0231	0.986454	0.99775	0.029394

Table 4.33: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after Blurring attack using variance 2.05

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	39.55	34.30	43.40	35.64	36.00	32.69	40.97	34.79	37.82	34.02
SSIM	0.993	0.989	0.997	0.995	0.992	0.988	0.993	0.990	0.987	0.986
NC	0.998	0.998	0.999	0.999	0.998	0.997	0.999	0.998	0.997	0.997
BER	0.025	0.029	0.023	0.028	0.027	0.030	0.024	0.028	0.026	0.029

Table 4.31 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.32 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.33 represents the comparative analysis of both of them against blurring attack variance 2.05.

Table 4.34: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using Blurring Attack variance 3.05

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.9133	0.98732	0.99811	0.02709
Foreman	40.8093	0.99514	0.99925	0.02452
News	33.3541	0.98715	0.99646	0.02998
Bowing	38.4473	0.98738	0.99833	0.02601
Pure_Storage	35.3929	0.97784	0.99626	0.02827

Table 4.35:Results of GBT-SVD using Watermark 1 after Blurring Attack Variance 3.05

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	33.0328	0.98181	0.99706	0.030273
Foreman	34.9142	0.99231	0.998865	0.028645
News	30.8777	0.98088	0.994844	0.032387
Bowing	33.8349	0.98329	0.997748	0.029555
Pure_Storage	32.7925	0.97718	0.996126	0.030499

Table 4.36: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after blurring attack using variance 3.05

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2
PSNR	36.91	33.03	40.80	34.91	33.35	30.87	38.44	33.83	35.39	32.79
SSIM	0.987	0.981	0.995	0.992	0.987	0.980	0.987	0.983	0.977	0.977
NC	0.998	0.997	0.999	0.998	0.996	0.994	0.998	0.997	0.996	0.996
BER	0.027	0.030	0.024	0.028	0.029	0.032	0.026	0.029	0.028	0.030

Table 4.34 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.35 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.36 represents the comparative analysis of both of them against blurring attack variance 3.05.

Table 4.37: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using Blurring Attack variance 4.05

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	32.8163	0.96796	0.99507	0.030473
Foreman	36.7963	0.988255	0.99805	0.027223
News	29.1031	0.967963	0.99049	0.034361
Bowing	34.6843	0.970265	0.99598	0.028832
Pure_Storage	32.8104	0.961798	0.99321	0.030504

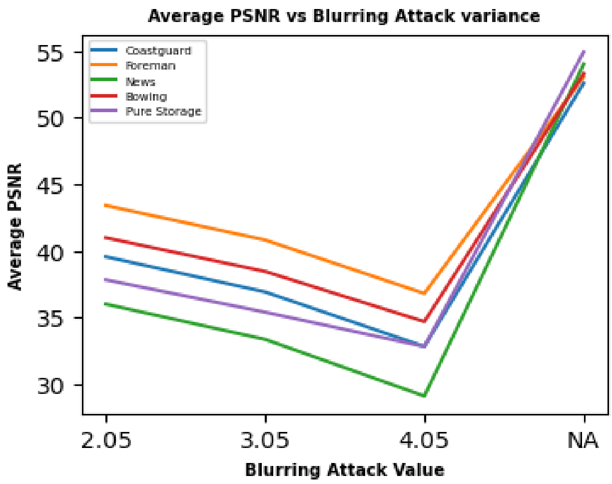
Table 4.38: Results of GBT-SVD using Watermark 1 after Blurring Attack Variance 4.05

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	30.5615	0.95923	0.99337	0.032721
Foreman	33.2171	0.98413	0.99737	0.030123
News	27.5892	0.95857	0.98748	0.036246
Bowing	32.0217	0.96522	0.99523	0.031229
Pure_Storage	31.0393	0.96054	0.99284	0.032223

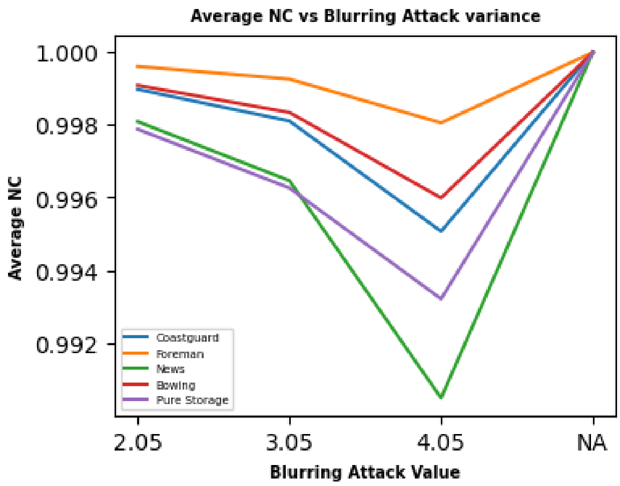
Table 4.37 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.38 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.39 represents the comparative analysis of both of them against blurring attack variance 4.05.

Table 4.39: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after sharpening attack using variance 4.05

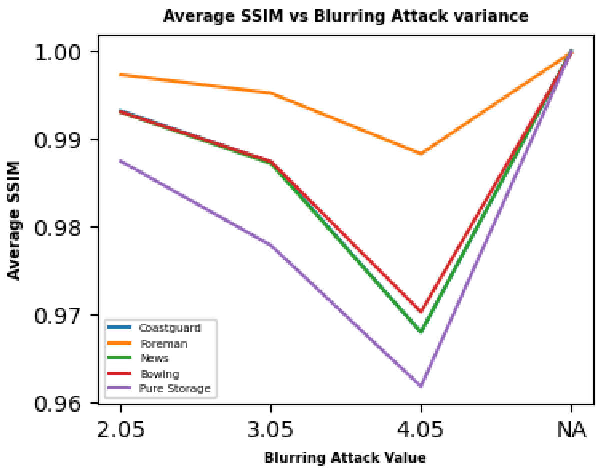
Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	32.81	30.56	36.79	33.21	29.10	27.58	34.68	32.02	32.81	31.03
SSIM	0.967	0.959	0.988	0.984	0.967	0.958	0.970	0.965	0.961	0.960
NC	0.995	0.993	0.998	0.997	0.990	0.987	0.995	0.995	0.993	0.992
BER	0.030	0.032	0.027	0.030	0.034	0.036	0.028	0.031	0.030	0.032



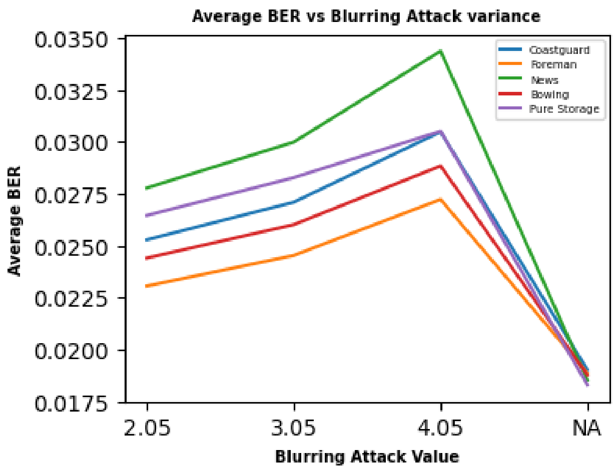
(a) Average comparison of PSNR VS Blurring attack Variance



(b) Average comparison of NC VS Blurring attack Variance



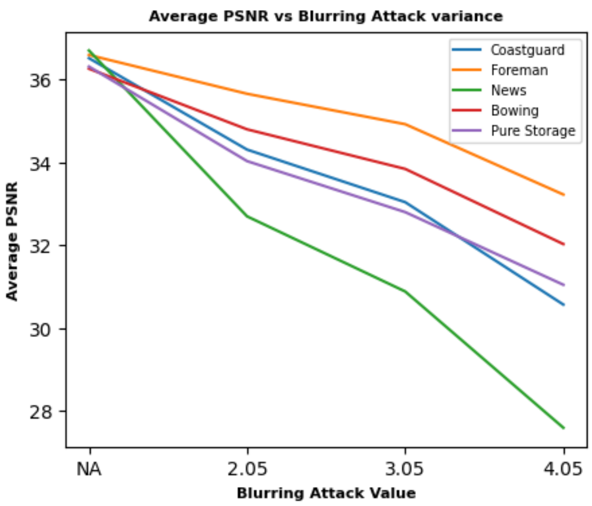
(c) Average comparison of SSIM VS Blurring attack Variance



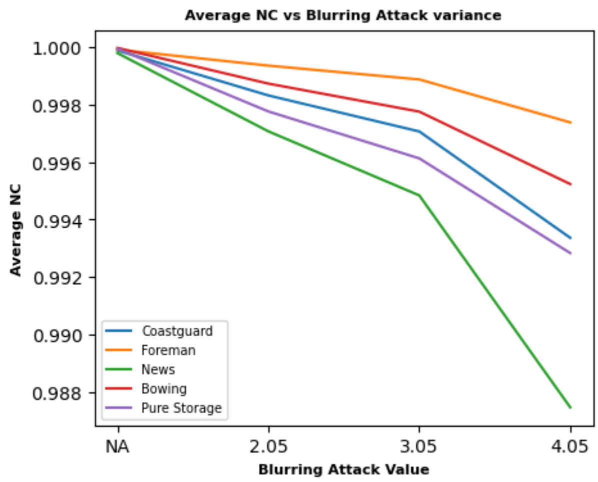
(d) Average comparison of BER VS Blurring attack Variance

Figure 4.31(a-d):Plot of PSNR, NC, SSIM, BER for optimized technique against Blurring Noise

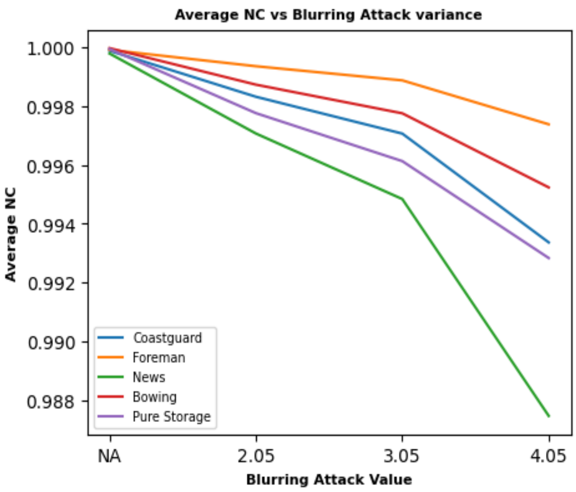
Plots in Figure 4.31 describe the calculation of performance parameters against Blurring noise variance 4.05,3.05,2.05 and 0 for the proposed optimized technique(GBT-SVD-GWO-GA). After applying this technique against different variance values, it was found that the value of quality metrics (PSNR) decreases with an increase in variance values.



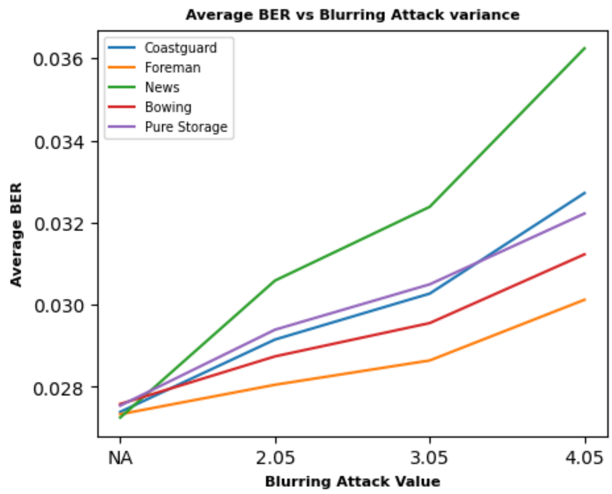
(a)Average PSNR V/s Blurring Attack Variance



(b) Average SSIM V/s Blurring Attack Variance



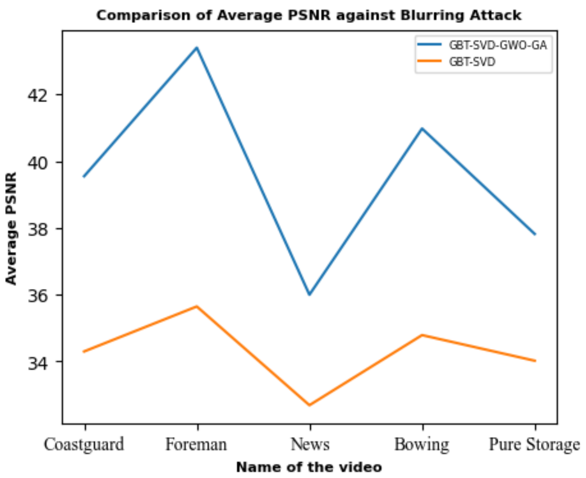
(c)Average NC V/s Blurring Attack Variance



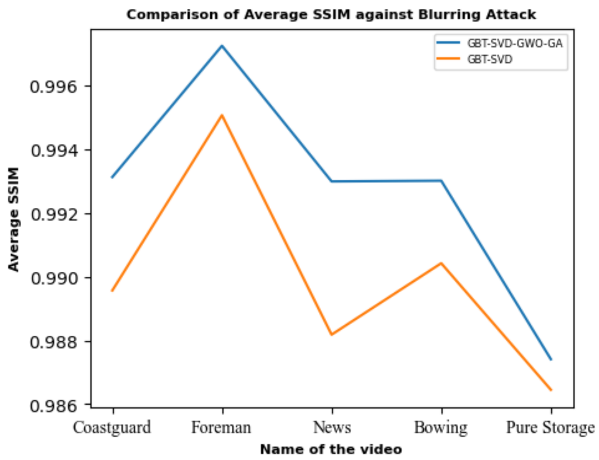
(d)Average BER V/s Blurring Attack Variance

Figure 4.32(a-d): Plot of PSNR, SSIM, NC, BER w.r.t the videos taken in the proposed work for GBT-SVD against Blurring Attack

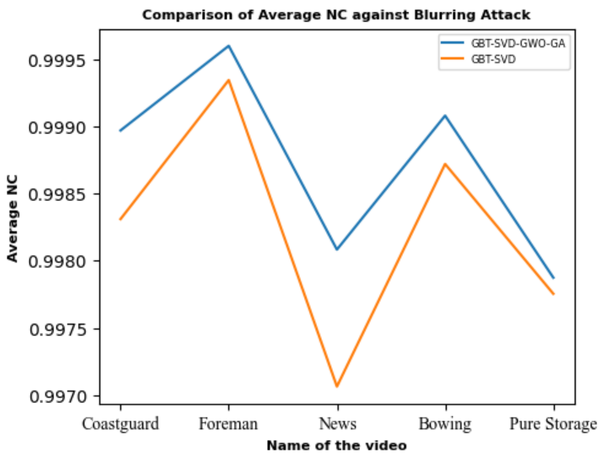
Plots in Figure 4.32 describe the calculation of performance parameters against Blurring noise variance 4.05,3.05,2.05 and 0 for the proposed technique(GBT-SVD) without optimization.



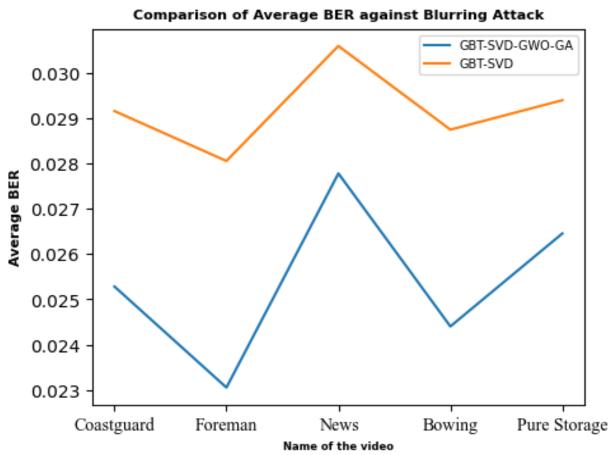
(a)Average PSNR against Blurring Attack variance 2.05



(b) Average SSIM against Blurring Attack variance 2.05



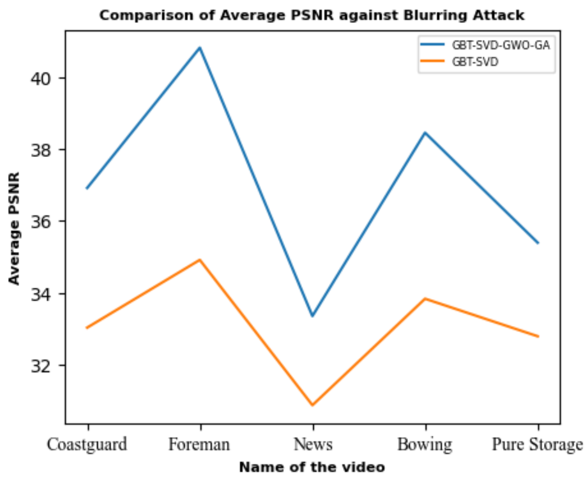
(c)Average NC against Blurring Attack variance 2.05



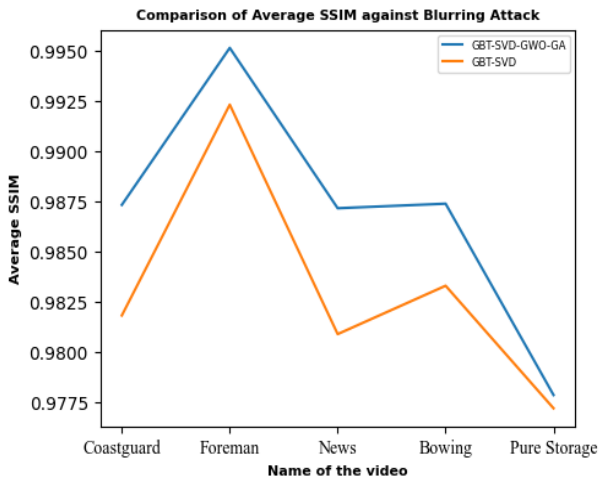
(d)Average BER against Blurring Attack variance 2.05

Figure 4.33(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Blurring Attack Variance 2.05

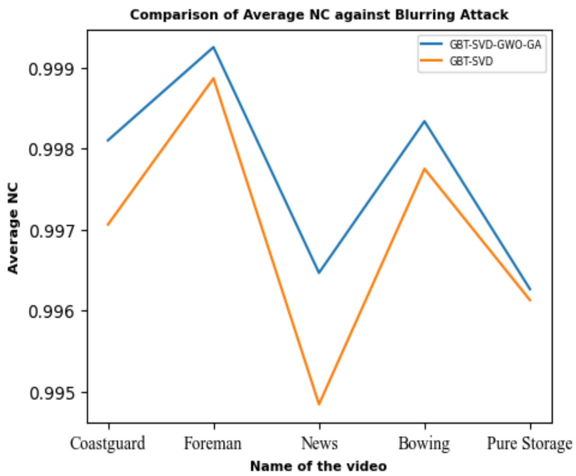
Plots in Figure 4.33 describe the comparative analysis of the proposed method with and without optimization against blurring attack variance 2.05. The optimized technique is yielding high performance of quality metrics over the proposed GBT-SVD technique. PSNR values of GBT-SVD-GWO-GA are comparatively higher than GBT-SVD.



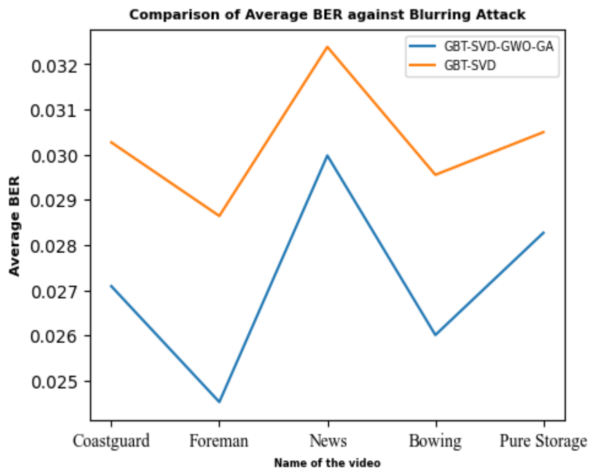
(a)Average PSNR against Blurring Attack variance 3.05



(b) Average SSIM against Blurring Attack variance 3.05



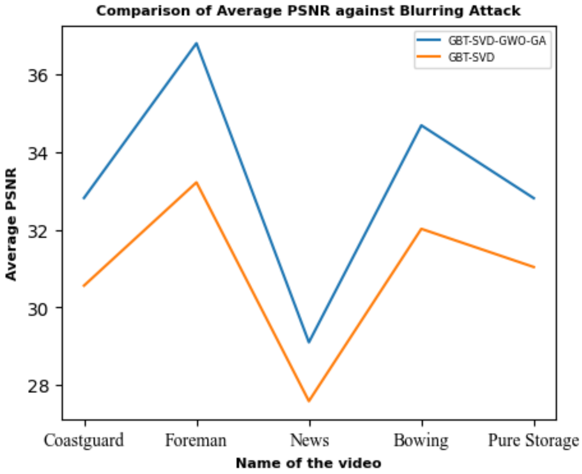
(c)Average NC against Blurring Attack variance 3.05



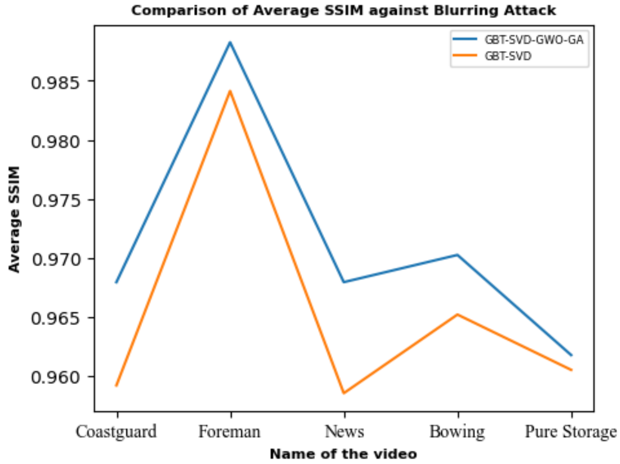
(d)Average BER against Blurring Attack variance 3.05

Figure 4.34(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Blurring Attack Variance 3.05

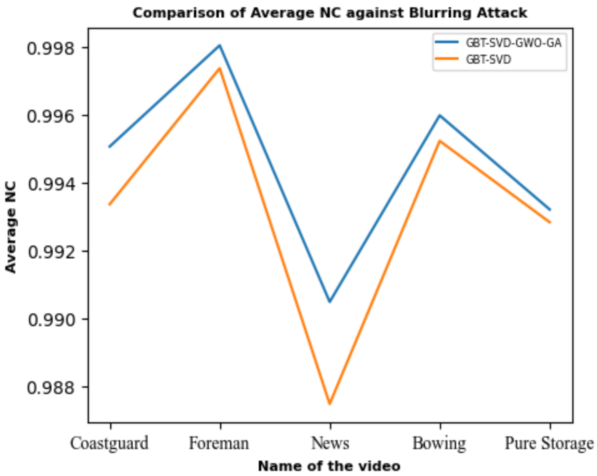
Plots in Figure 4.34 describe the comparative analysis of the proposed method with and without optimization against blurring attack variance 3.05. The optimized technique is yielding high performance of quality metrics over the proposed GBT-SVD technique. PSNR values of GBT-SVD-GWO-GA are comparatively higher than GBT-SVD.



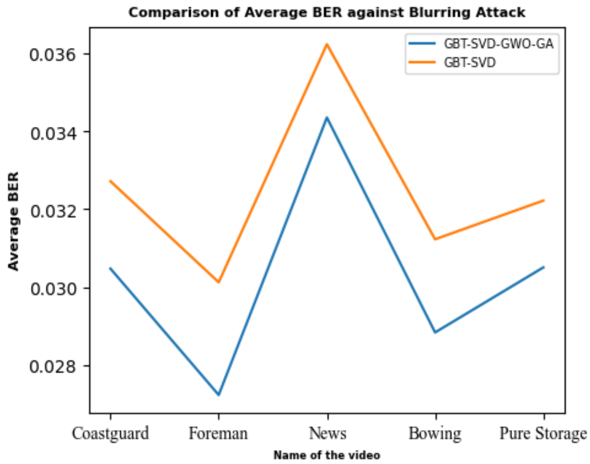
(a)Average PSNR against Blurring Attack variance 4.05



(b) Average SSIM against Blurring Attack variance 4.05



(c)Average NC against Blurring Attack variance 4.05



(d)Average BER against Blurring Attack variance 4.05

Figure 4.35(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against Blurring Attack Variance 4.05

Plots in Figure 4.35 describe the comparative analysis of the proposed method with and without optimization against blurring attack variance 4.05. The optimized technique is yielding high performance of quality metrics over the proposed GBT-SVD technique. PSNR values of GBT-SVD-GWO-GA are comparatively higher than GBT-SVD against this variance value of Blurring attack.

4.4.5 JPEG Compression Attack

In JPEG Compression attack, values {0,98, 96, 94} are taken that are applied to the all-watermarked video. The value 0 indicates no attack is used. It can be seen from plots in Figure 4.38(a-d) as that average PSNR, NC, SSIM decrease with decrease in value of compression attack value and BER increases with decrease in attack value. The higher value of PSNR, NC, SSIM justifies the proposed technique's robustness against compression attack. In Figure 4.38(a-d), plots compile compression attacks for all quality parameters using values {0,98, 96, 94} for all 5 videos taken in research work. PSNR, SSIM, NC and BER values of all the videos are similar. Lower values of BER are obtained for NA. Figure 4.36 represents watermarked frames after applying JPEG Compression attack to watermarked frames.

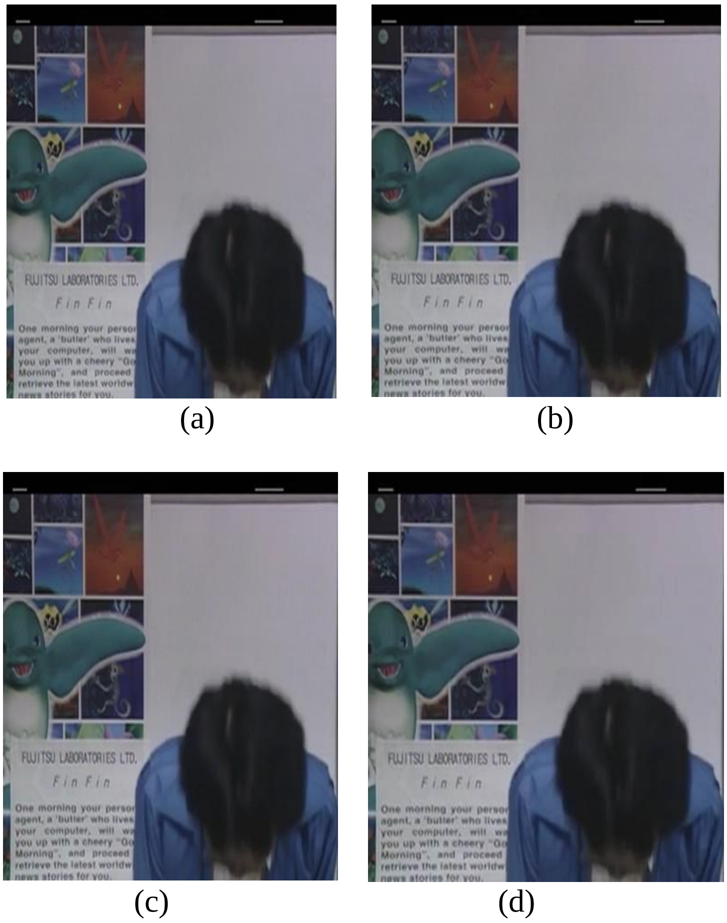


Figure 4.36(a-d): Attacked watermarked frames of Bowing Video (a) No Attack (b) JPEG Compression attack with 98 value, (c) JPEG Compression attack with 96 value and (d) JPEG Compression attack with 94 value

Table 4.40: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using JPEG Compression Attack variance 98

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	46.5895	0.9968	0.99982	0.021464
Foreman	44.7164	0.99578	0.99969	0.022371
News	42.8397	0.99348	0.99966	0.023344
Bowing	46.0870	0.99416	0.99974	0.021699
Pure_Storage	46.2146	0.99589	0.99971	0.021671

Table 4.41: Results of GBT-SVD Embedding of Watermark 1 on watermarked frames using JPEG Compression Attack variance 98

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.3922	0.99563	0.99972	0.027478
Foreman	36.1413	0.99499	0.99966	0.027671
News	36.0477	0.99083	0.99942	0.027741
Bowing	35.9181	0.99329	0.99976	0.027841
Pure_Storage	35.8626	0.99467	0.99971	0.027884

Table 4.42: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after JPEG Compression attack using variance 98

Parameters	**Coastguard**		**Foreman**		**News**		**Bowing**		**Pure_Storage**	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	46.58	36.39	44.71	36.14	42.83	36.04	46.08	35.91	46.21	35.86
SSIM	0.996	0.995	0.995	0.994	0.993	0.990	0.994	0.993	0.995	0.994
NC	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999
BER	0.021	0.027	0.022	0.027	0.023	0.027	0.021	0.027	0.021	0.027

Table 4.40 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.41 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.42 represents the comparative analysis of both of them against JPEG Compression attack variance 98.

Table 4.43: Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using JPEG Compression Attack variance 96

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	44.7796	0.99511	0.99971	0.02233
Foreman	43.7044	0.99462	0.99961	0.02288
News	41.96307	0.99149	0.99951	0.02383
Bowing	45.04628	0.99282	0.99966	0.02222
Pure_Storage	45.12032	0.99450	0.99962	0.02219

Table 4.44: Results of GBT-SVD Embedding of Watermark 1 on watermarked frames using JPEG Compression Attack variance 96

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	36.1583	0.99375	0.99959	0.027656
Foreman	36.5845	0.99812	0.99999	0.027335
News	35.8183	0.98877	0.99931	0.027919
Bowing	35.7991	0.99196	0.99968	0.027934
Pure_Storage	35.7317	0.99332	0.99962	0.027986

Table 4.45: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after JPEG Compression attack using variance 96

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	44.77	36.15	43.70	36.58	41.96	35.81	45.04	35.79	45.12	35.73
SSIM	0.995	0.993	0.994	0.998	0.991	0.988	0.992	0.991	0.994	0.993
NC	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999
BER	0.022	0.027	0.022	0.027	0.023	0.027	0.022	0.027	0.022	0.027

Table 4.43 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.44 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.45 represents the comparative analysis of both of them against JPEG Compression attack variance 96.

Table 4.46 : Results of GBT-SVD-GWO-GA Embedding of Watermark 1 on watermarked frames using JPEG Compression Attack variance 94

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	43.349	0.99326	0.99959	0.023069
Foreman	42.793	0.99338	0.99951	0.023373
News	41.129	0.98962	0.99944	0.024315
Bowing	44.201	0.99144	0.99959	0.022625
Pure_Storage	44.100	0.99294	0.99952	0.022706

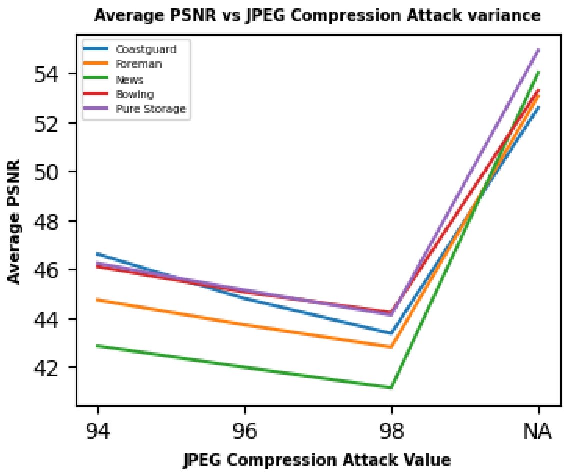
Table 4.47: Results of GBT-SVD Embedding of Watermark 1 on watermarked frames using JPEG Compression Attack variance 94

Video	PSNR (dB)	SSIM	NC	BER
Coastguard	30.5615	0.95923	0.99337	0.032721
Foreman	35.7971	0.99250	0.99946	0.027937
News	35.5926	0.98683	0.99922	0.028096
Bowing	35.6814	0.99059	0.99960	0.028026
Pure_Storage	35.5844	0.99177	0.99951	0.028102

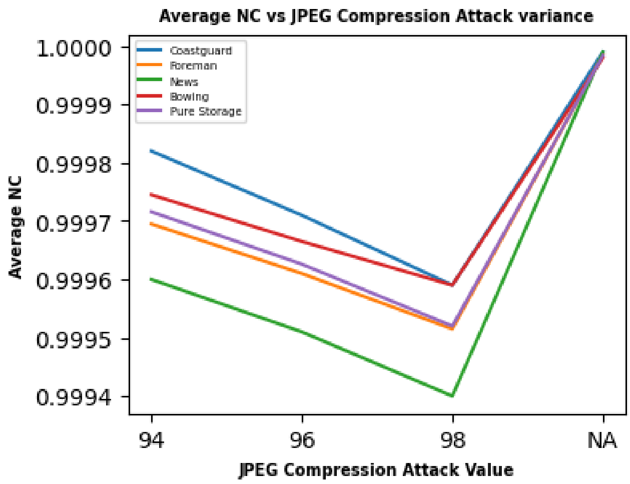
Table 4.48: Comparative Analysis of GBT-SVD-GWO-GA and GBT-SVD for watermark 1 after JPEG Compression attack using variance 94

Parameters	Coastguard		Foreman		News		Bowing		Pure_Storage	
	T1	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**	**T1**	**T2**
PSNR	43.34	30.56	42.79	35.79	41.12	35.59	44.20	35.68	44.10	35.58
SSIM	0.993	0.959	0.993	0.992	0.989	0.986	0.991	0.990	0.992	0.991
NC	0.999	0.993	0.999	0.999	0.999	0.999	0.999	0.999	0.999	0.999
BER	0.023	0.032	0.023	0.027	0.024	0.028	0.022	0.028	0.022	0.028

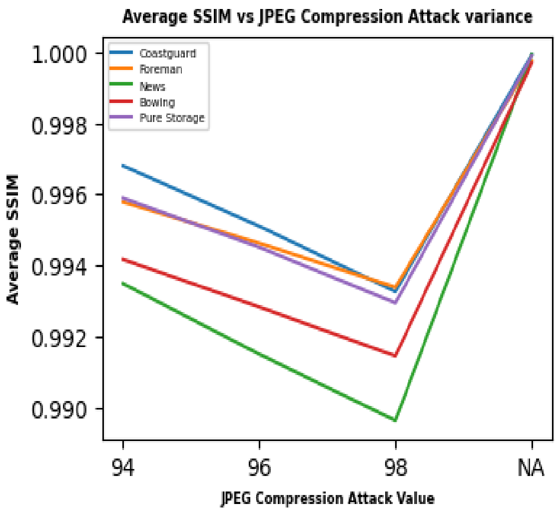
Table 4.46 represents the calculation of the proposed technique's performance parameters with optimization. Table 4.47 describes the calculation of the proposed technique's performance parameters without optimization, and Table 4.48 represents the comparative analysis of both of them against JPEG Compression attack variance 94.



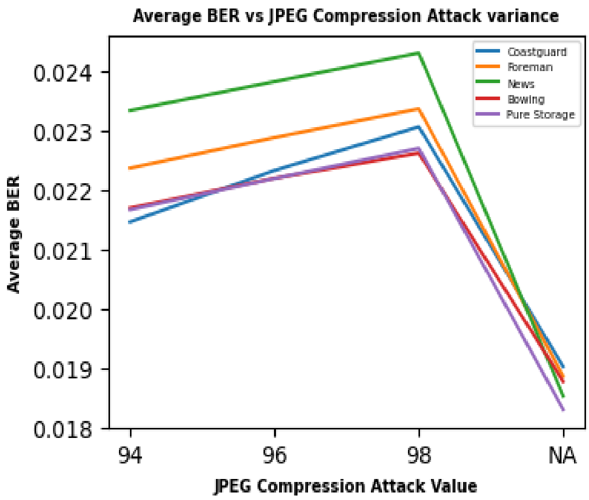
(a) Average comparison of PSNR against JPEG Compression attack Variance



(b) Average comparison of NC against JPEG Compression attack Variance



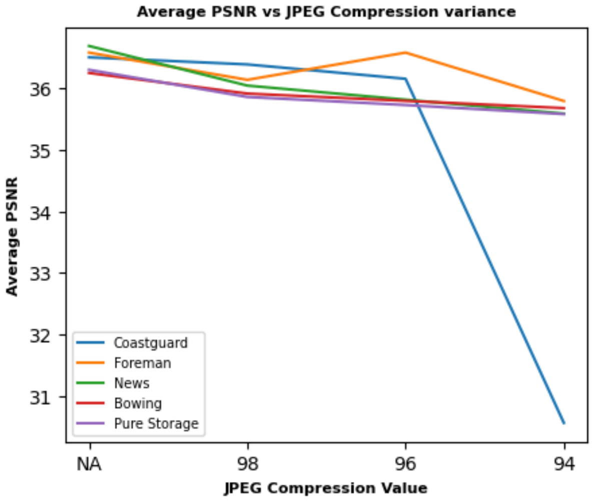
(c) Average comparison of SSIM against JPEG Compression attack Variance



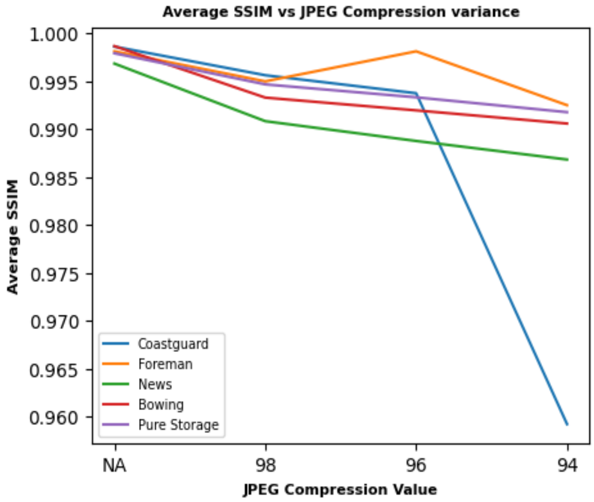
(d) Average comparison of BER against JPEG Compression Variance

Figure 4.37(a-d): Plot of PSNR, NC, SSIM and BER w.r.t JPEG Compression Attack Variance using watermark1

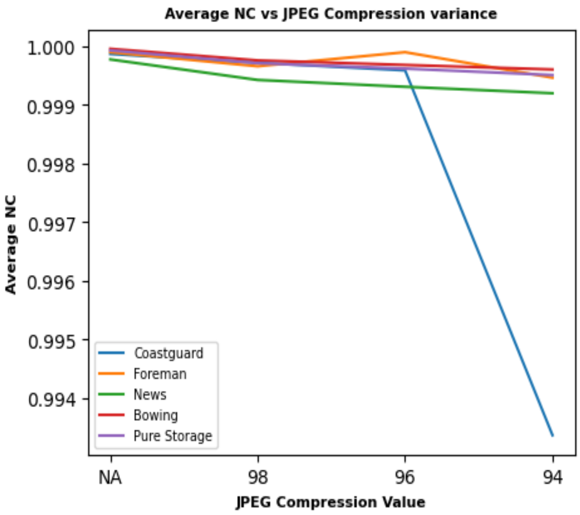
Plots in figure 4.37 describe the calculation of performance parameters against JPEG Compression variance 98,96,94 and 0 for the proposed technique(GBT-SVD-GWO-GA). High values of quality metrics (PSNR) are found against JPEG Compression attack.



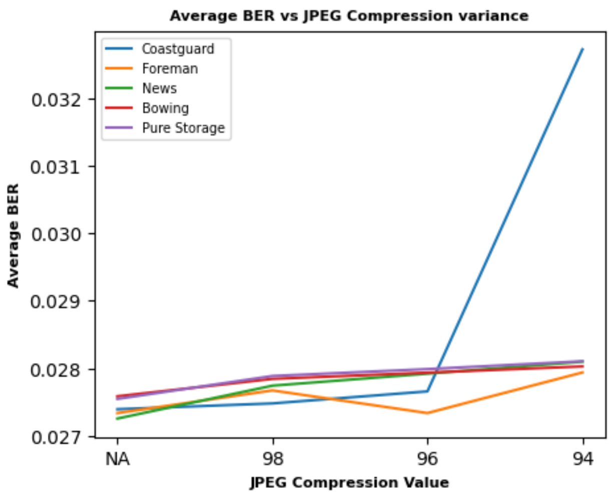
(a)Average PSNR against JPEG Compression Attack Variance



(b) Average SSIM against JPEG Compression Attack Variance



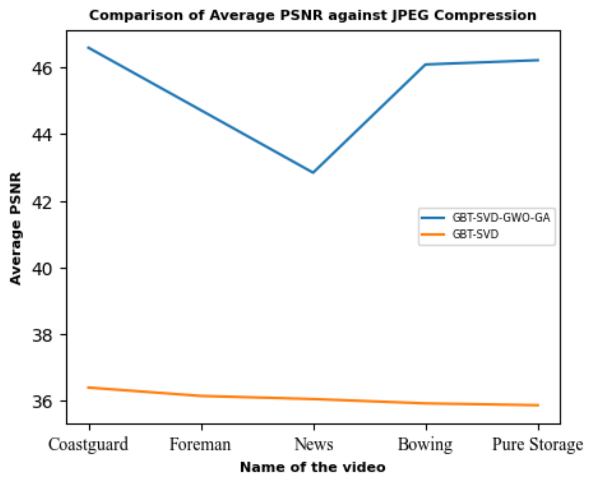
(c)Average NC against JPEG Compression Attack Variance



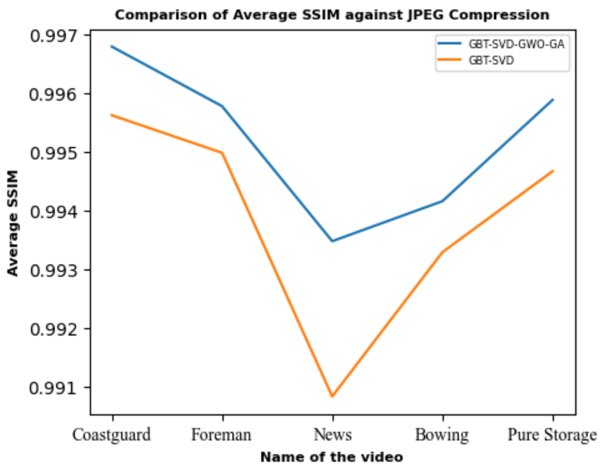
(d)Average BER against JPEG Compression Attack Variance

Figure 4.38(a-d): Plot of PSNR, SSIM, NC, BER w.r.t the videos taken in the proposed work for GBT-SVD against JPEG Compression Attack

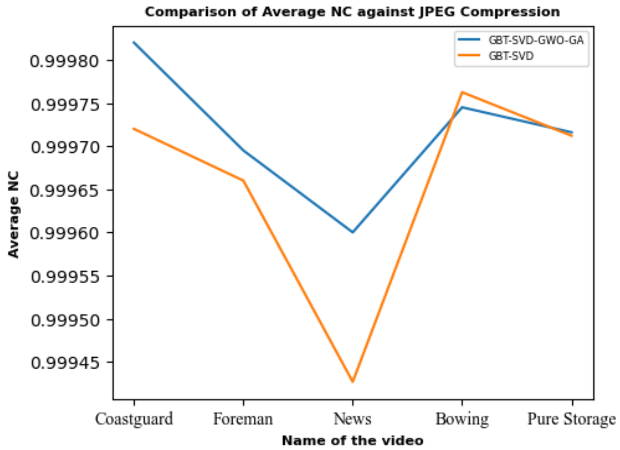
Plots in Figure 4.38 describe the calculation of performance parameters against JPEG Compression variance 98,96,94 and 0 for the proposed technique(GBT-SVD) without optimization. High values of quality metrics (PSNR) are found against JPEG Compression attack.



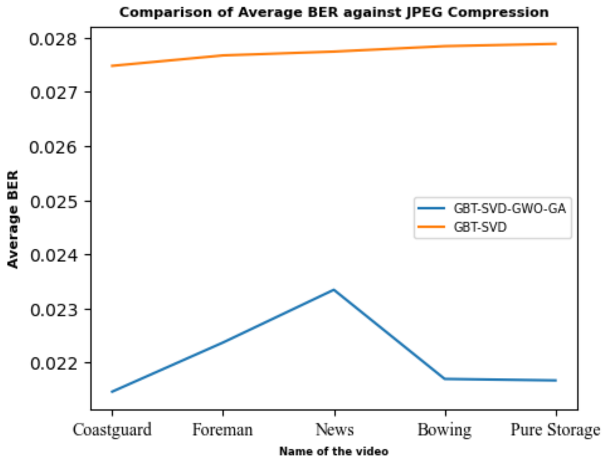
(a)Average PSNR against JPEG Compression Attack variance 98



(b) Average SSIM against JPEG Compression Attack variance 98



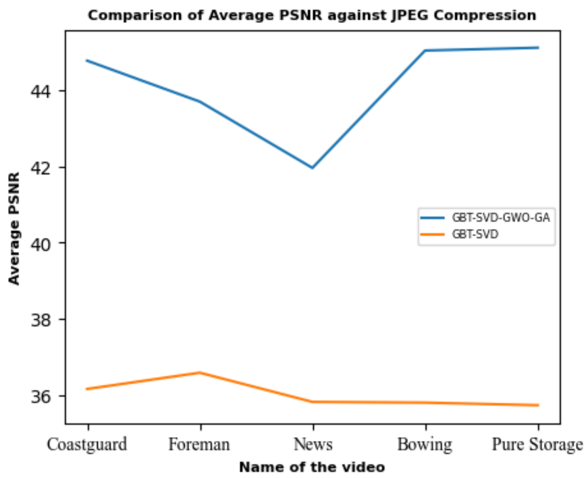
(c)Average NC against JPEG Compression Attack variance 98



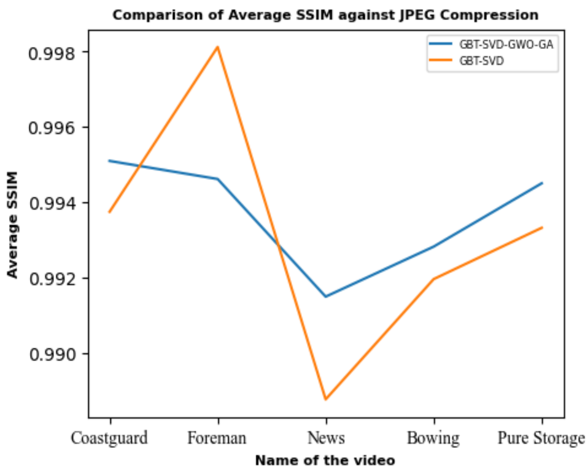
(d)Average BER against JPEG Compression Attack variance 98

Figure 4.39(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against JPEG Compression Attack Variance 98

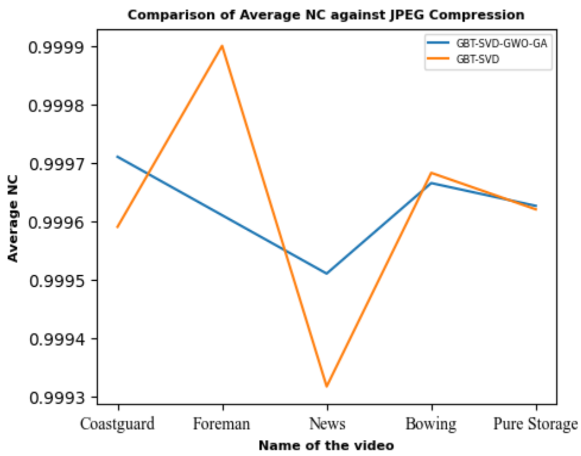
Plots in Figure 4.39 describe the comparative analysis of the proposed method with and without optimization against JPEG Compression variance 98. The performance of the optimized technique is better than GBT-SVD using the same variance value.



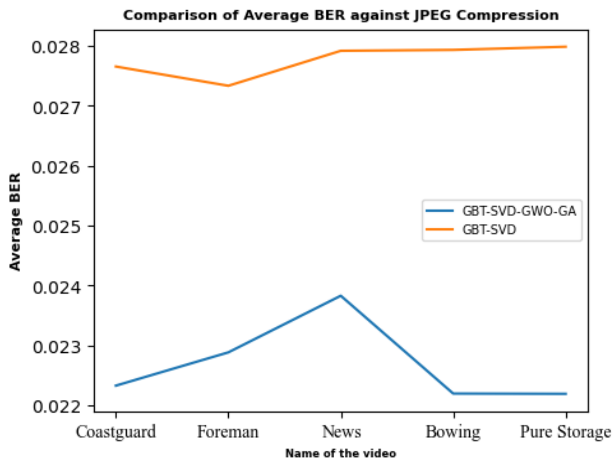
(a)Average PSNR against JPEG Compression Attack variance 96



(b) Average SSIM against JPEG Compression Attack variance 96



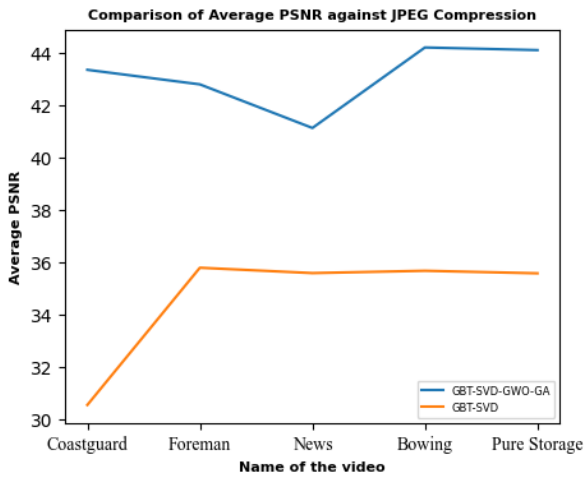
(c)Average NC against JPEG Compression Attack variance 96



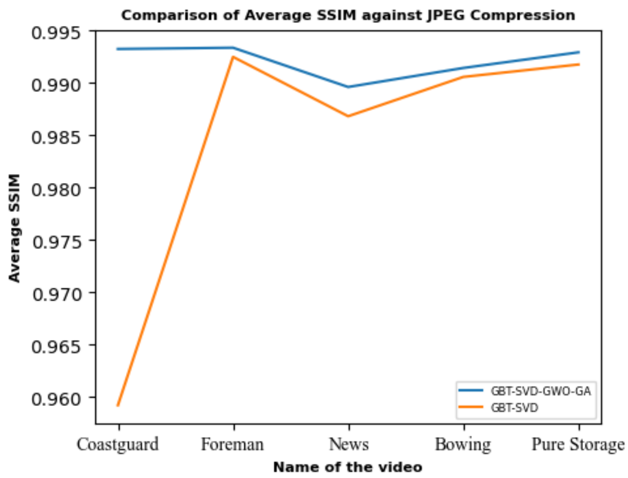
(d)Average BER against JPEG Compression Attack variance 96

Figure 4.40(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against JPEG Compression Attack Variance 96

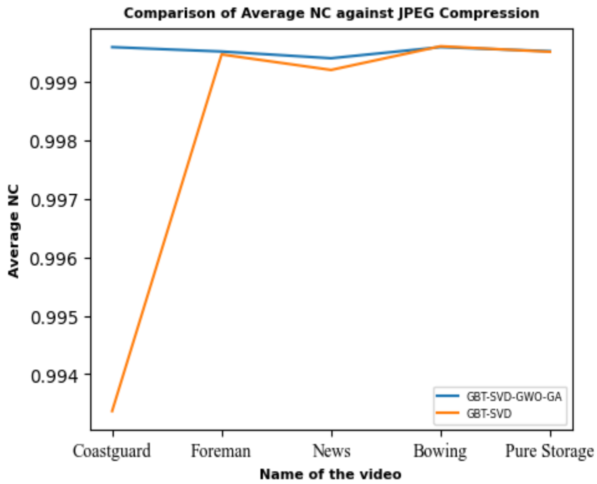
Plots in Figure 4.40 describe the comparative analysis of the proposed method with and without optimization against JPEG Compression variance 96. The optimized technique's performance is better than GBT-SVD using the same variance value in terms of quality metrics(PSNR).



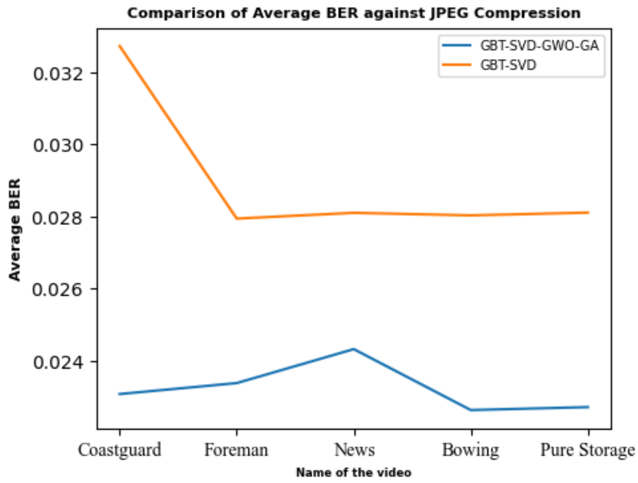
(a)Average PSNR against JPEG Compression Attack variance 94



(b) Average SSIM against JPEG Compression Attack variance 94



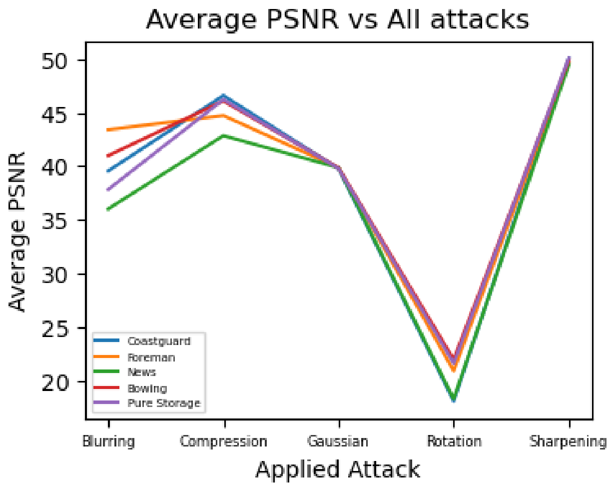
(c)Average NC against JPEG Compression Attack variance 94



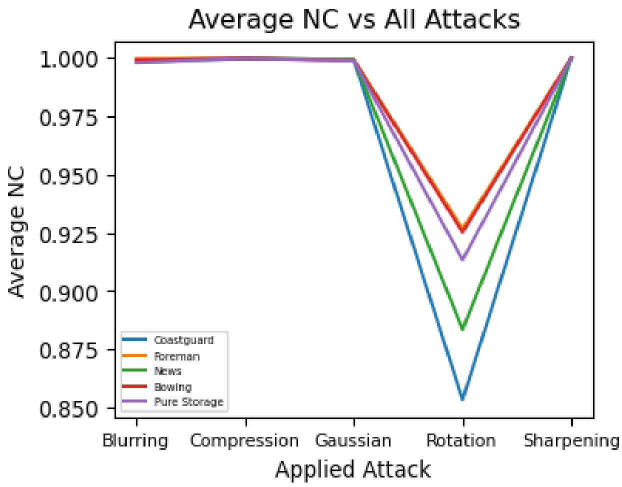
(d)Average BER against JPEG Compression Attack variance 94

Figure 4.41(a-d): Plot of Comparison Analysis of PSNR, SSIM, NC, BER for GBT-SVD and GBT-SVD-GWO-GA against JPEG Compression Attack Variance 94

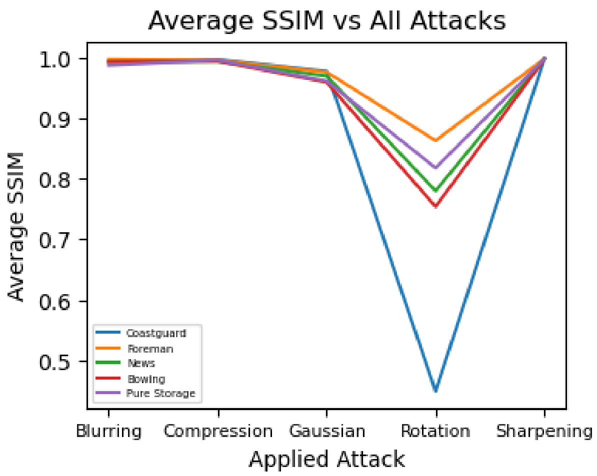
Plots in Figure 4.41 describe the comparative analysis of the proposed method with and without optimization against JPEG Compression variance 94. The optimized technique's performance is better than GBT-SVD using the same variance value in terms of quality metrics(PSNR).



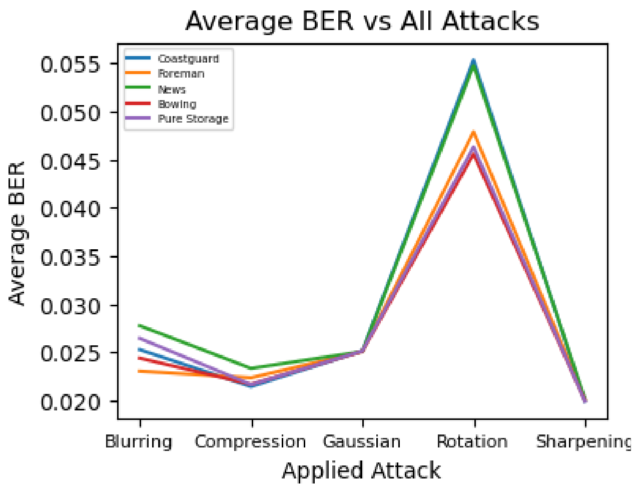
(a) Average comparison of PSNR against all attacks



(b) Average comparison of NC against all attacks



(c) Average comparison of SSIM against all attacks



(d) Average comparison of BER against all attacks

Figure 4.42(a-d): Plots of PSNR, NC, SSIM, and BER for GBT-SVD-GWO-GA w.r.t all attacks using watermark1(GBT-SVD-GWO-GA)

Figure 4.42 compiles the result calculation of all attacks applied to the optimized watermark frame. The plots represent the variance of performance parameters against all attacks.

4.5 Comparison with Existing Research Work

The proposed technique's performance is tested based on two properties: the degree of invisibility and robustness. Many researchers have researched over the years to improvise on existing mechanisms. This section explains the comparison of the proposed technique against previous research over the years. Table 4.49 presents the comparison of Quality Metrics (PSNR) of existing research work with the proposed work using a different set of videos.

Table 4.49: Comparison Analysis of Quality Metrics (PSNR) for existing techniques and proposed technique

Techniques used	PSNR (dB)	BER
Rajpal et.al [65]	39.15	0.025
Cao et.al [69]	57.02	0.017
Ji et.al [77]	39.65	0.025
Mehta et.al[79]	46.16	0.021
Xu et.al[80]	45.61	0.021
Proposed Technique(GBT-SVD-GWO-GA)	56.32	0.017

The plot in Figure 4.43 represents the calculated value of PSNR and BER for the existing and proposed method. It was found that our proposed method outperforms most of the methods for a different set of videos.

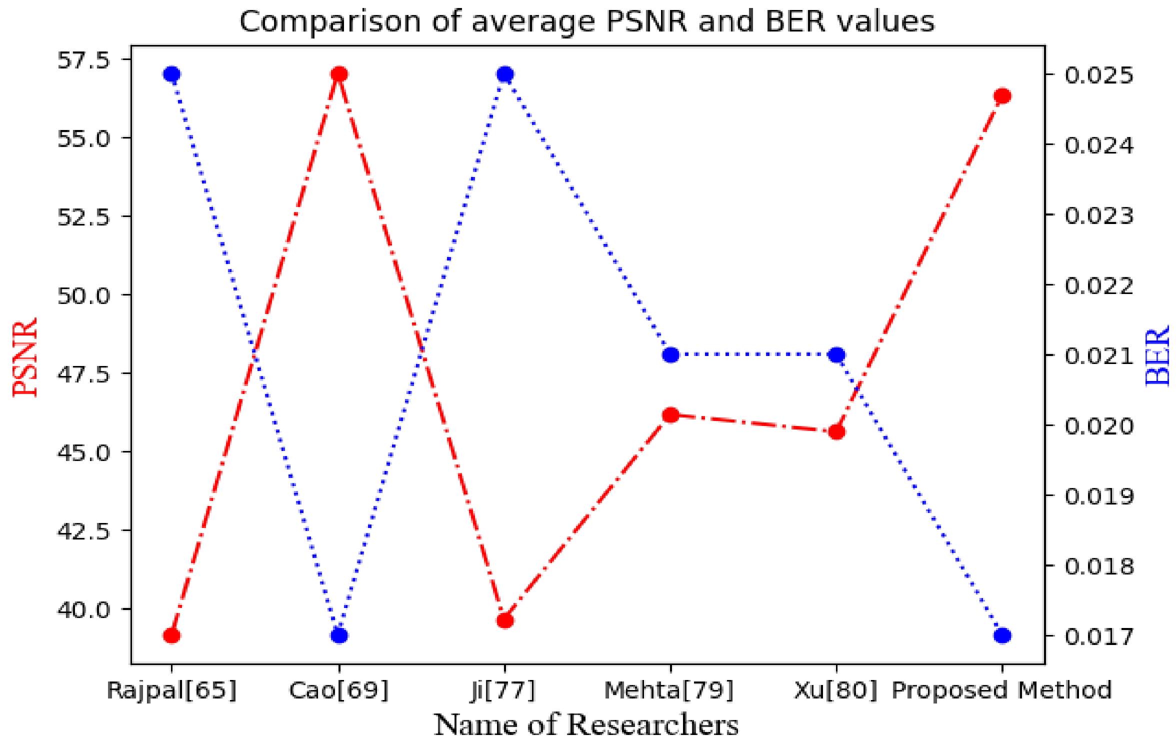


Figure 4.43: Comparison of calculated values of PSNR and BER for existing and proposed Method

The comparison analysis is applied on the same video data set (Coastguard Video) using watermark 2. It was found that our research work provides better results than Rajpal's [65] technique based on calculated values of PSNR. Table 4.50 represents the comparison of the proposed method and existing methods. Plots in Figure 4.44 represent the comparison of Proposed and existing embedding techniques for coastguard video.

Table 4.50: Comparison Analysis of Quality Metrics (PSNR) for existing techniques and proposed technique for Coastguard Video

Techniques used	PSNR (dB)	BER
Rajpal et.al [65]	41.20	0.024
Hammami [72]	45.31	0.022
Sadi et.al [59]	34.02	0.029
Proposed Technique (GBT-SVD)	36.50	0.027
Proposed Technique(GBT-SVD-GWO-GA)	55.02	0.018

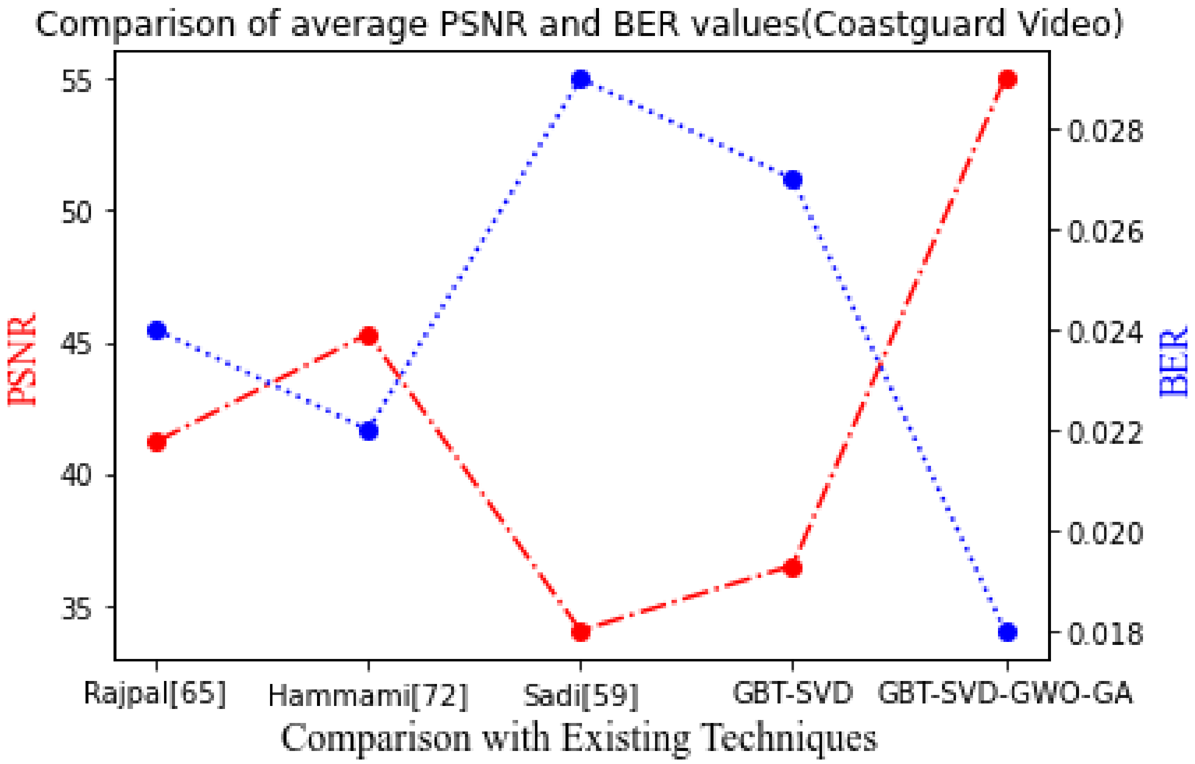


Figure 4.44: Comparison of Proposed and Existing Techniques for Coastguard Video

Table 4.51 represents the comparison of the proposed method and existing methods for football video. Plots in Figure 4.45 represent the comparison of proposed and existing embedding techniques for football video. GBT-SVD and GBT-SVD-GWO-GA are proposed methods of our research.

Table 4.51: Comparison Analysis of Quality Metrics (PSNR) for existing techniques and proposed technique for Football Video

Techniques used	PSNR (dB)	BER
Rajpal et.al [65]	40.20	0.024
Nouioua [64]	40.26	0.024
Ji et.al [77]	39.65	0.025
Proposed Technique (GBT-SVD)	37.02	0.027
Proposed Technique(GBT-SVD-GWO-GA)	56.31	0.017

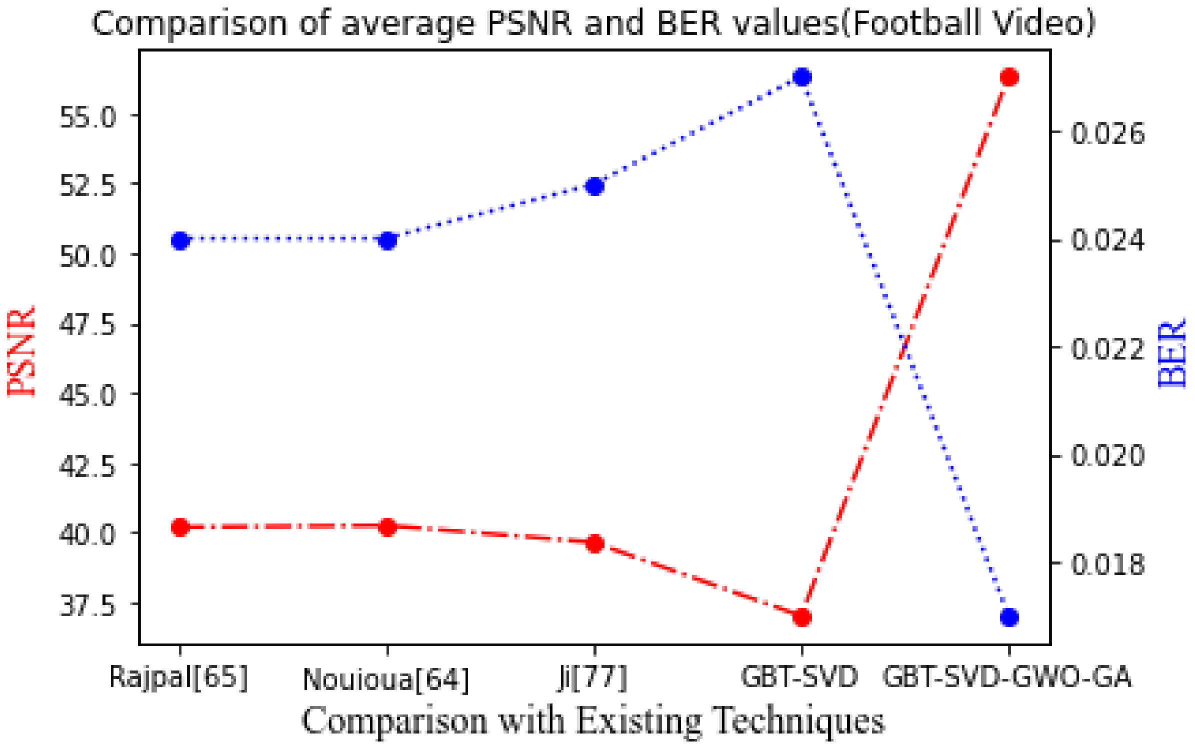


Figure 4.45: Comparison of Proposed and Existing Techniques for Football Video

Table 4.52 represents the comparison of the proposed method and existing methods for akiyo video. Plots in Figure 4.46 represent the comparison of Proposed and existing embedding techniques for akiyo video. GBT-SVD and GBT-SVD-GWO-GA are proposed methods of our research. It is observed that our proposed method provides better results than existing methods.

Table 4.52: Comparison Analysis of Quality Metrics (PSNR) for existing techniques and proposed technique for Akiyo Video

Techniques used	PSNR (dB)	BER
Rajpal et.al [65]	42.47	0.023
Farri [63]	37.62	0.026
Nouioua [64]	40.45	0.024
Sadi et.al [59]	38.20	0.026
Proposed Technique (GBT-SVD)	42.38	0.023
Proposed Technique(GBT-SVD-GWO-GA)	66.65	0.015

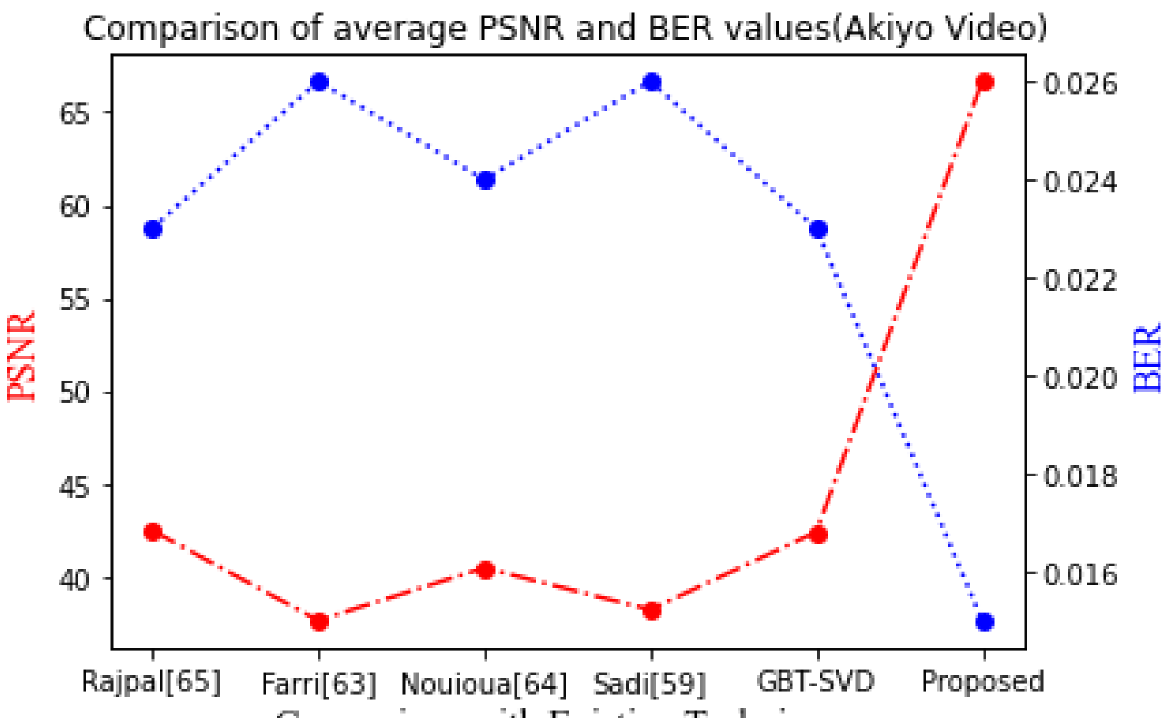


Figure 4.46: Comparison of Proposed and Existing Techniques for Akiyo Video

Table 4.53 represents the comparison of the proposed method and existing methods for news video. Plots in figure 4.47 represent the comparison of Proposed and existing embedding techniques for news video. GBT-SVD and GBT-SVD-GWO-GA are proposed methods of our research. It is observed that our proposed method provides better results than existing methods.

Table 4.53: Comparison Analysis of Quality Metrics (PSNR) for existing techniques and proposed technique for News Video

Techniques used	PSNR (dB)	BER
Farri [63]	43.13	0.023
Proposed Technique (GBT-SVD)	36.69	0.027
Proposed Technique(GBT-SVD-GWO-GA)	54.00	0.018

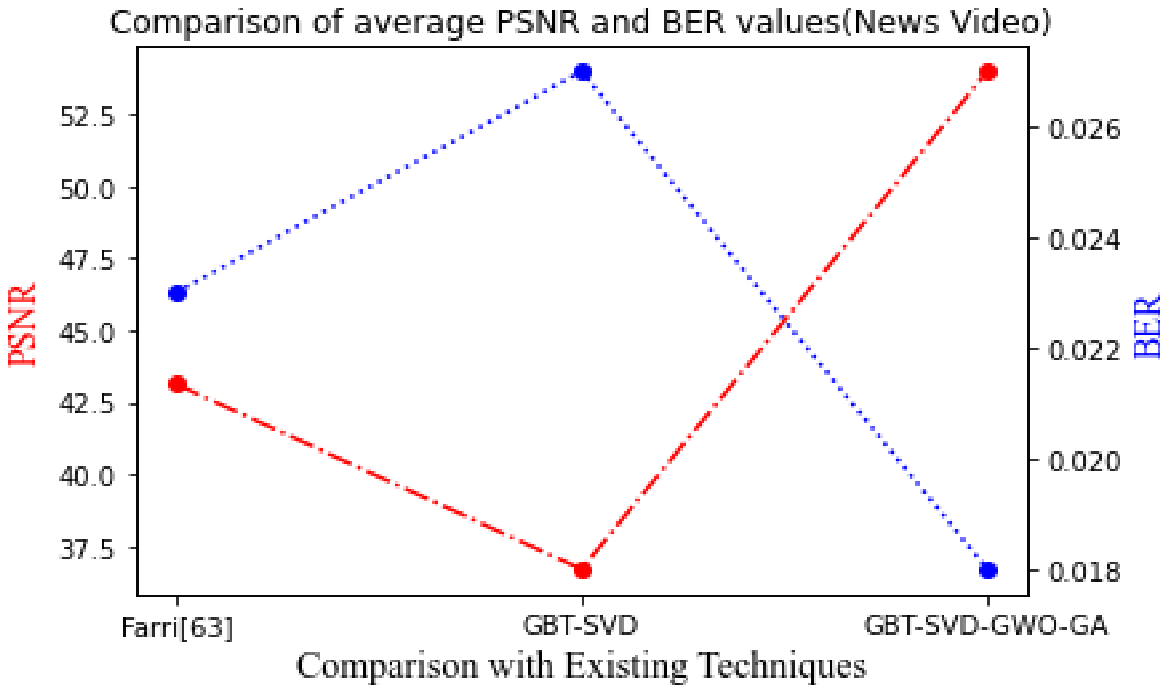


Figure 4.47: Comparison of Proposed and Existing Techniques for News Video

Table 4.54 represents the comparison of the proposed method and existing methods for Mother_daughter video. Plots in Figure 4.48 represent the comparison of Proposed and existing embedding techniques for Mother_daughter video. GBT-SVD and GBT-SVD-GWO-GA are proposed methods of our research.

Table 4.54: Comparison Analysis of Quality Metrics (PSNR) for existing techniques and proposed technique for Mother_daughter Video

Techniques used	PSNR (dB)	BER
Rajpal et.al [65]	42.21	0.023
Farri [63]	39.93	0.025
Proposed Technique(GBT-SVD)	41.63	0.024
Proposed Technique(GBT-SVD-GWO-GA)	69.43	0.014

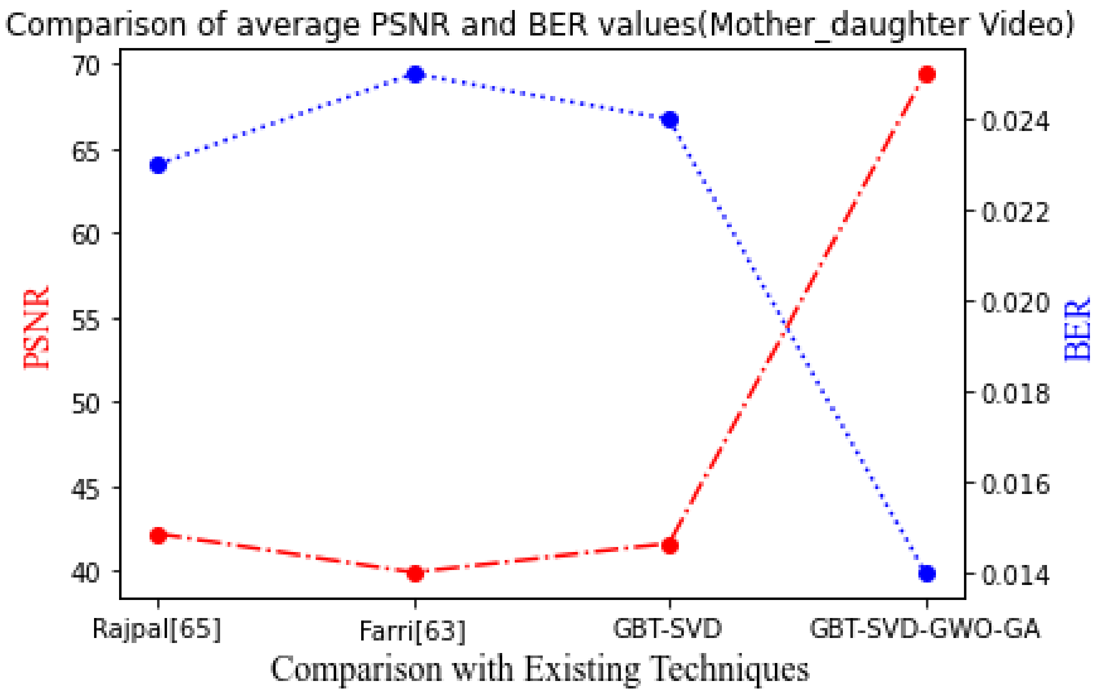


Figure 4.49: Comparison of Proposed and Existing Techniques for Mother_daughter Video

Rajpal [65] has taken sample videos named Akiyo, Mother_daughter, Pamphlet, Silent, and watermark to conduct his study. We have also calculated frame selection time, watermark embedding time, and the calculation of performance parameters. The comparison of frame selection and embedding time with Rajpal's[65] work is represented in table 4.55. The proposed technique of GBT-SVD-GWO-GA is taken for comparison.

Table 4.55: Comparison of Time Complexity of Proposed Work and Rajpal's[65] work

	Rajpal et.all[65]		**Proposed Work**	
Video	**Frame Selection Time(in seconds)**	**Embedding Time(in seconds)**	**Frame Selection Time(in seconds)**	**Embedding Time(in seconds)**
Akiyo	21.85	108.73	0.211	103.41
Mother_daughter	22.98	77.60	0.193	105.72
Pamphlet	22.64	121.22	0.175	21.38
Silent	27.09	44.15	0.166	108.05

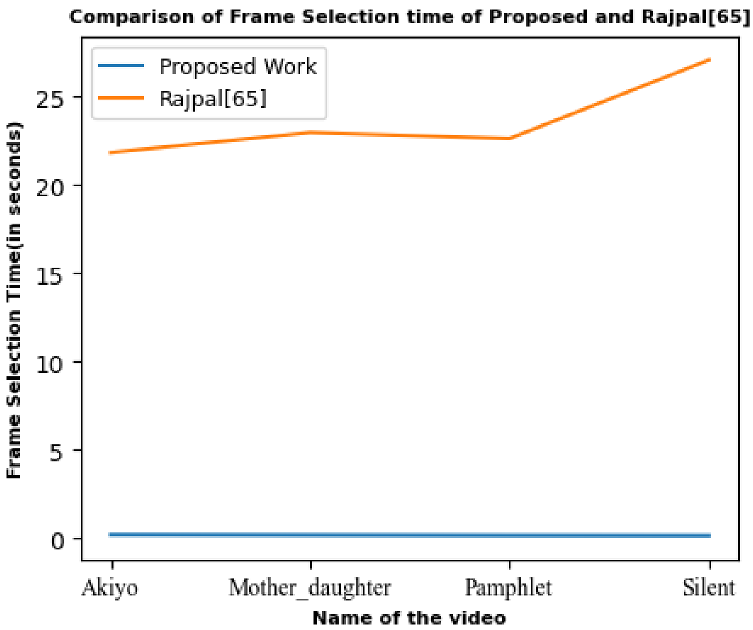


Figure 4.49: Comparison of Proposed and Rajpal's[65]Frame Selection Time

Figure 4.49 represents a comparison of the proposed technique with Rajpal[65] against frame selection time. It is observed that our proposed frame selection technique is fast.

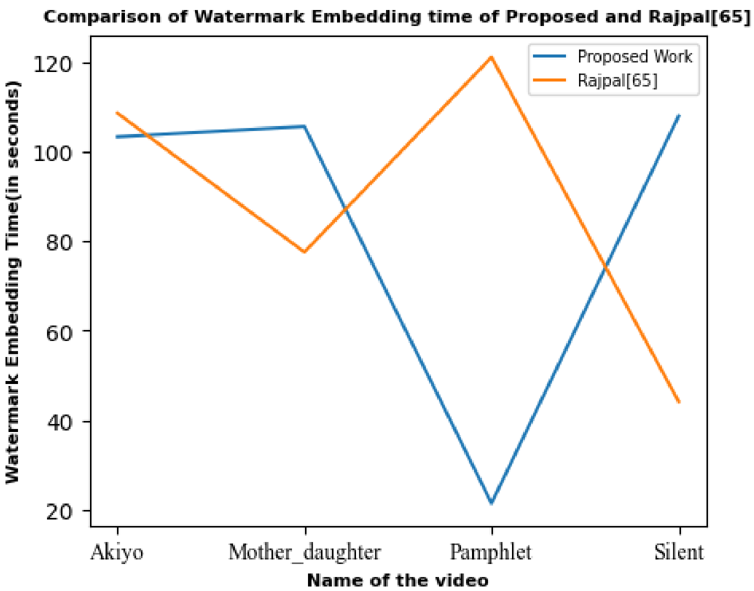


Figure 4.50: Comparison of Proposed and Rajpal's[65] Embedding Time

Figure 4.50 represents a comparison of the proposed technique with Rajpal[65] against watermark embedding time. It is observed that our proposed method is giving good results in embedding time. Embedding time also depends upon the number of iterations used in the optimized algorithm; we have employed five iterations for this purpose. Video Akiyo and Pamphlet have less embedding time compared to Rajpal[65].

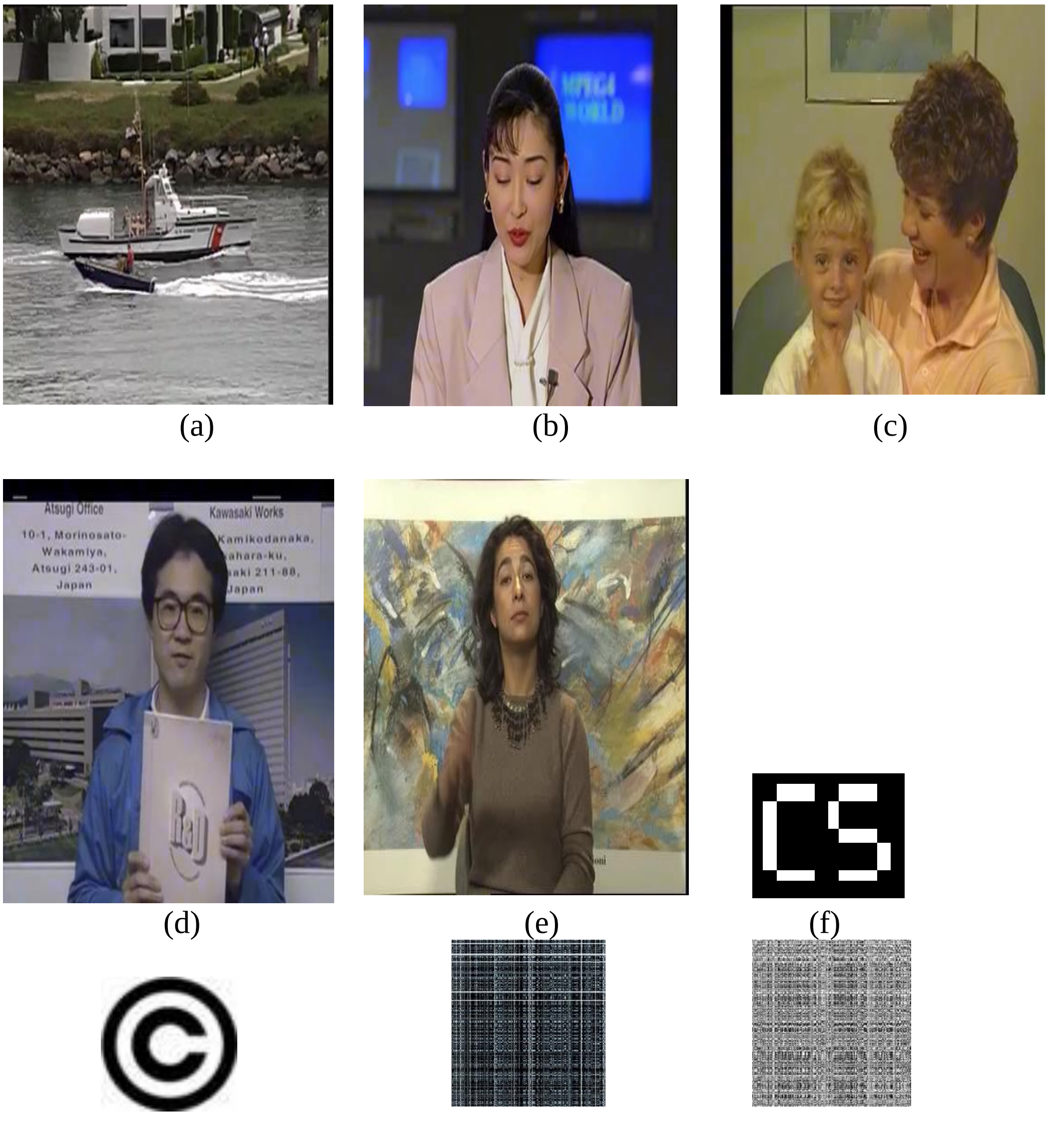


Figure 4.51 (a-i): Selected frames from videos (a) Coastguard (Frame # 64), (b) Akiyo (Frame # 251), (c) Mother_daughter (Frame # 54), (d) Pamphlet (Frame # 171) and (e) Silent (Frame #14); (f) original watermark1, (g)original watermark2 , (h) encrypted watermark1 ,(i) encrypted watermark2

Figure 4.51 represents selected frames from the video data sets taken by Rajpal[65]. The value of the threshold was reduced to 1.2 to carry out the frame selection process. The watermark in figure 4.47(f) was taken to carry out the watermarking process. The optimized technique proposed in our research is providing high PSNR values after watermarking process comparative to the technique proposed by Rajpal[65].

Table 4.56 represents the comparison of proposed work with Rajpal's[65] technique against Gaussian noise variance 0.001. Performance parameters PSNR, NC, and BER, are taken for comparison.

Table 4.56: Comparison Analysis with Rajpal[65] Technique using various videos after processing gaussian attack with variance 0.001

	Rajpal et.al[65]			Proposed Work		
Video	**PSNR**	**NC**	**BER**	**PSNR**	**NC**	**BER**
Akiyo	39.15	0.81	0.025	60.46	0.99	0.0165
Mother_daughter	38.83	0.87	0.025	59.45	0.99	0.0168
Pamphlet	38.77	0.86	0.025	55.70	0.99	0.0179
Silent	37.78	0.75	0.026	64.81	0.99	0.0264

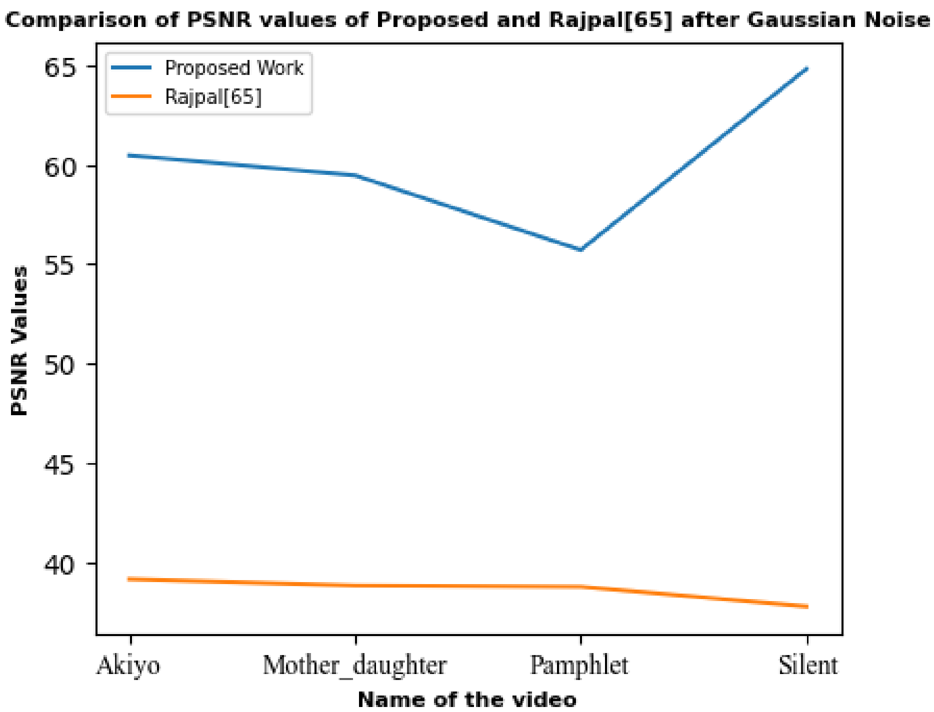


Figure 4.52: Comparison of Proposed, Rajpal's[65] PSNR values after Gaussian Noise variance

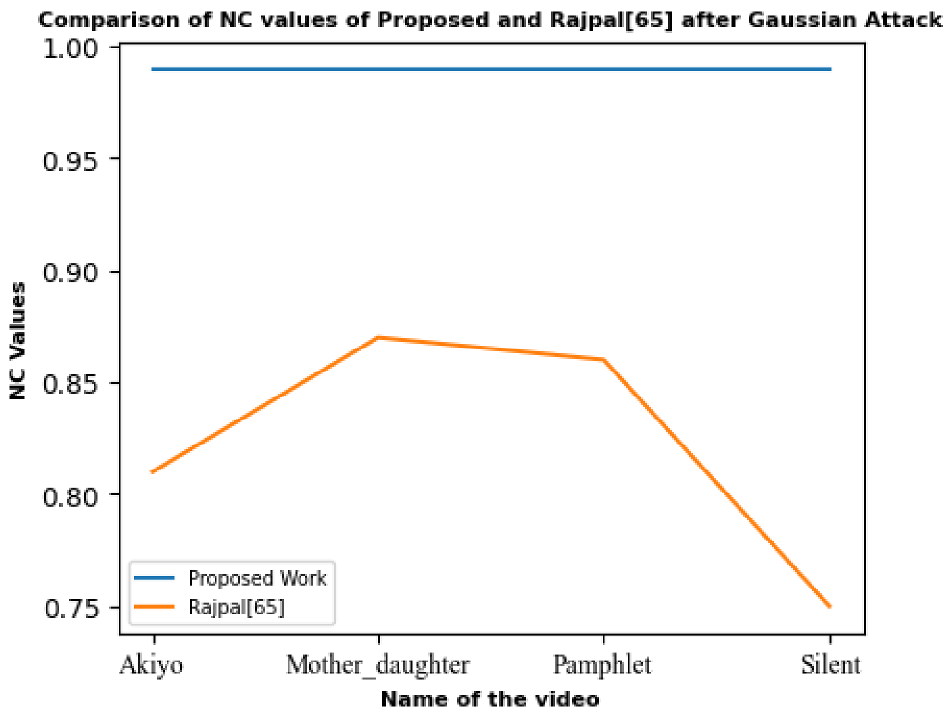


Figure 4.53: Comparison of Proposed, Rajpal's[65] NC values after Gaussian Noise variance

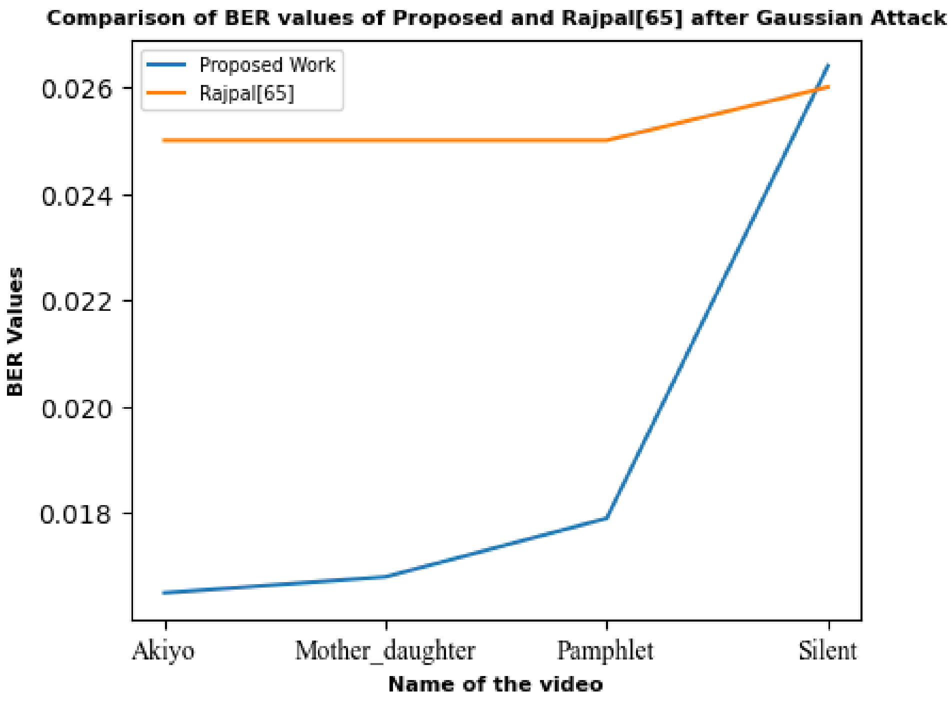


Figure 4.54: Comparison of Proposed, Rajpal's[65] BER values after Gaussian Noise variance

Plots in Figures 4.52,4.53,4.54 represent the comparison of PSNR, NC, and BER values of the proposed technique with Rajpal[65] against Gaussian noise variance 0.001. It has been observed that our method provides much better results for all parameters in comparison to Rajpal [65].

4.6 Validation of Proposed Technique

The proposed technique (GBT-SVD-GWO-GA) provides better results than existing methods on different sets of videos taken in this research. The validation of the proposed technique's performance against existing techniques in terms of frame selection time, embedding time and values of quality metrics can be tested by applying Paired Sample T-Test.

4.6.1 Validation Checks on Frame Selection Time

Paired Sample T-test is applied by taking Frame Selection Time of Rajpal[65] and Proposed Technique of different set of videos taken in Rajpal's[65] research.

Table 4.57: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Rajpal	23.6400	4	2.34820	1.17410
	Proposed	.1863	4	.01996	.00998

Table 4.58:Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Rajpal & Proposed	4	-.764	.236

Table 4.59:Paired Samples Test

		Paired Differences				
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference	
					Lower	Upper
Pair 1	Rajpal - Proposed	23.45375	2.36348	1.18174	19.69292	27.21458

Table 4.60:Paired Samples Test

		T	Df	Sig. (2-tailed)
Pair 1	Rajpal – Proposed	19.847	3	.000

Table 4.57,4.58,4.59,4.60 represents the application of paired sample T- Test on frame selection time of Rajpal[65] and proposed work. It is observed that $t(3) = 19.847$, $p = 0.000$. We have assumed that there is no significant difference in the frame selection time of Rajpal[65] and our method. Since $p<0.05$, that means there is a difference in frame selection time of both techniques and our frame selection time mean value is comparatively lesser than Rajpal's Method.

4.6.2 Validation Checks on Embedding Time

Paired Sample T-test is applied by taking Embedding Time of Rajpal[65] and Proposed Technique of different set of videos taken in Rajpal's[65] research.

Table 4.61:Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Rajpal	87.9250	4	34.46864	17.23432
	Proposed	84.6400	4	42.21585	21.10793

Table 4.62:Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Rajpal & Proposed	4	-.678	.322

Table 4.63: Paired Samples Test

		Paired Differences				
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference	
					Lower	Upper
Pair 1	Rajpal - Proposed	3.28500	70.30199	35.15099	-108.58115	115.15115

Table 4.64:Paired Samples Test

		T	Df	Sig. (2-tailed)
Pair 1	Rajpal – Proposed	.093	3	.931

Table 4.61,4.62,4.63,4.64 represents the application of paired sample T- Test on embedding time of Rajpal[65] and proposed work. It is observed that $t(3) = 0.093$, $p = 0.931$. We have assumed that there is no significant difference in the embedding time of Rajpal[65] and our method. Since $p>0.05$, that

means there is no difference in embedding time of both techniques, and our embedding time mean value is comparatively similar to Rajpal's Method. So our assumption is proven true.

4.6.3 Validation Checks on Performance of Proposed Techniques against Gaussian Noise Variance

Paired Sample T-test is applied by taking quality metric(PSNR) values of both proposed techniques: GBT-SVD and GBT-SVD-GWO-GA against different variance values of Gaussian Noise attack.

Table 4.65: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	GBT_SVD_GWO_GA	35.9881	20	12.57169	2.81112
	GBT_SVD	30.2548	20	6.47244	1.44728

Table 4.66: Paired Samples Statistics

		N	Correlation	Sig.
Pair 1	GBT_SVD_GWO_GA & GBT_SVD	20	.927	.000

Table 4.67: Paired Samples Statistics Paired Samples Test

		Paired Differences					T	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	GBT_SVD_GWO_GA - GBT_SVD	5.73334	7.00750	1.56693	2.45372	9.01295	3.659	19	.002

Table 4.65,4.66,4.67 represents the application of paired sample T- Test on both proposed techniques with and without optimization. It is observed that $t(19) = 3.659$, $p = 0.002$. We have assumed that there is no significant difference in both proposed techniques since $p<0.05$, which means there is a significant difference in both techniques' PSNR values, and our assumption is proven wrong.. GBT-SVD-GWO-GA outperforms GBT-SVD in terms of PSNR values.

4.6.4 Validation Checks on Performance of Proposed Techniques against Sharpening Attack Variance

Paired Sample T-test is applied by taking quality metric(PSNR) values of both proposed techniques: GBT-SVD and GBT-SVD-GWO-GA, against different variance values of the Sharpening attack.

Table 4.68: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	GBT_SVD_GWO_GA	50.7713	20	1.72245	.38515
	GBT_SVD	36.3925	20	.16736	.03742

Table 4.69: Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	GBT_SVD_GWO_GA & GBT_SVD	20	.159	.503

Table 4.70: Paired Samples Test

		Paired Differences					T	Df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	GBT_SVD_GWO_GA - GBT_SVD	14.37874	1.70387	.38100	13.58131	15.17618	37.740	19	.000

Table 4.68,4.69,4.70 represents the application of paired sample T- Test on both proposed techniques with and without optimization. It is observed that $t(19) = 37.740$, $p = 0.000$. We have assumed that there is no significant difference in both proposed techniques since $p<0.05$, which means there is a significant difference in both techniques' PSNR values, and our assumption is proven wrong. GBT-SVD-GWO-GA outperforms GBT-SVD in terms of PSNR values.

4.6.5 Validation Checks on Performance of Proposed Techniques against Rotation Attack Variance

Paired Sample T-test is applied by taking quality metric(PSNR) values of both proposed techniques: GBT-SVD and GBT-SVD-GWO-GA against different rotation values attack.

Table 4.71: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	GBT_SVD_GWO_GA	20.1512	5	1.85474	.82946
	GBT_SVD	20.0787	5	1.83184	.81922

Table 4.72:Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	GBT_SVD_GWO_GA & GBT_SVD	5	.999	.000

Table 4.73:Paired Samples Test

		Paired Differences					T	Df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	GBT_SVD_GWO_GA - GBT_SVD	.07251	.09662	.04321	-.04746	.19247	1.678	4	.169

Table 4.71,4.72,4.73 represents the application of paired sample T- Test on both proposed techniques with and without optimization. It is observed that $t(4) = 1.678$, $p = 0.169$. We have assumed no significant difference in both proposed techniques since $p>0.05$, which means there is no significant difference in both techniques' PSNR values, and our assumption is proven correct. The values of PSNR by GBT-SVD-GWO-GA technique are similar to GBT-SVD.

4.6.6 Validation Checks on Performance of Proposed Techniques against Blurring Attack Variance

Paired Sample T-test is applied by taking quality metric(PSNR) values of both proposed techniques: GBT-SVD and GBT-SVD-GWO-GA against different blurring variance values attack.

Table 4.74:Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	GBT_SVD_GWO_GA	40.8366	20	8.21447	1.83681
	GBT_SVD	33.6838	20	2.43848	.54526

Table 4.75: Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	GBT_SVD_GWO_GA & GBT_SVD	20	.902	.000

Table 4.76: Paired Samples Test

		Paired Differences					T	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	GBT_SVD_GWO_GA - GBT_SVD	7.15282	6.10700	1.36557	4.29465	10.01098	5.238	19	.000

Table 4.74,4.75,4.76 represents the application of paired sample T- Test on both proposed techniques with and without optimization. It is observed that $t(19) = 5.238$, $p = 0.000$. We have assumed that there is no significant difference in both proposed techniques since $p<0.05$, which means there is a significant difference in both techniques' PSNR values, and our assumption is proven wrong. GBT-SVD-GWO-GA outperforms GBT-SVD in terms of PSNR values against blurring attack variance.

4.6.7 Validation Checks on Performance of Proposed Techniques against JPEG Compression Attack Variance

Paired Sample T-test is applied by taking quality metric(PSNR) values of both proposed techniques: GBT-SVD and GBT-SVD-GWO-GA against different variance values of JPEG Compression Attack.

Table 4.77:Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	GBT_SVD_GWO_GA	46.5242	20	4.40706	.98545
	GBT_SVD	35.8007	20	1.28172	.28660

Table 4.78:Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	GBT_SVD_GWO_GA & GBT_SVD	20	.350	.130

Table 4.79:Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	GBT_SVD_GWO_GA - GBT_SVD	10.72356	4.13652	.92495	8.78761	12.65951	11.594	19	.000

Table 4.77,4.78,4.79 represents the application of paired sample T- Test on both proposed techniques with and without optimization. It is observed that $t(19) = 11.594$, $p = 0.000$. We have assumed that there is no significant difference in both proposed techniques since $p<0.05$, which means there is a significant difference in both techniques' PSNR values, and our assumption is proven wrong. GBT-SVD-GWO-GA outperforms GBT-SVD in terms of PSNR values against JPEG compression attack variance.

4.6.8 Validation Checks on Performance of Proposed Techniques against Rajpal[65] on Gaussian Noise Variance 0.01

Paired Sample T-test is applied by imparting a Gaussian noise variance of 0.01 for both Rajpal[65] and the proposed method. The validation checks are performed on videos taken in Rajpal's[65] work.

Table 4.80: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Rajpal	38.6325	4	.59230	.29615
	Proposed	60.1050	4	3.74594	1.87297

Table 4.81:Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Rajpal & Proposed	4	-.685	.315

Table 4.82:Paired Samples Test

		Paired Differences			
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference
					Lower
Pair 1	Rajpal - Proposed	-21.47250	4.17426	2.08713	-28.11468

Table 4.83: Paired Samples Test

		Paired Differences	T	Df	Sig. (2-tailed)
		95% Confidence Interval of the Difference			
		Upper			
Pair 1	Rajpal - Proposed	-14.83032	-10.288	3	.002

Table 4.80,4.81,4.82,4.83 represents the application of paired sample T- Test on Rajpal[65] and proposed technique. It is observed that $t(3) = -10.288$, $p = 0.002$. We have assumed no significant difference in proposed and Rajpal's[65] method since $p<0.05$, which means there is a significant difference in both techniques' PSNR values, and our assumption is proven wrong. GBT-SVD-GWO-GA outperforms Rajpal's[65] method in terms of PSNR values against Gaussian noise variance 0.001.

It has been proven that our proposed technique performs better after attack scenarios are applied.

CHAPTER 5
SUMMARY AND CONCLUSION

This chapter explains the summary and conclusion of the research work.

5.1 Summary

The doctoral thesis topic is the design and development of frame selection based watermarking technique to address the quality loss of data. The proposed work focuses on frame selection algorithm and watermark embedding algorithm, and quality checks. The purpose of the work is to embed the encrypted watermark to address quality loss. The proposed work is organized in various chapters where chapter 1 focuses on the introduction, multiple techniques of frame selection and watermarking techniques, problem formulation, and objectives of the work. Chapter 2 explains the literature survey done through the study and research gaps in this area. Chapter 3 summarizes the materials and methods used in the study and describes the frame selection algorithm, watermark embedding, and extraction algorithms. Chapter 4 focuses on the calculation of results of the proposed techniques against various attacks scenarios along with a comparison with existing techniques of watermarking.

5.2 Conclusion

Watermarking is a technique to embed hidden or unnoticeable signals inside multimedia data so that any unidentified user can't manipulate the data without the owner's information. In this thesis, we have proposed the Frame Selection technique to select an appropriate number of frames and the watermark embedding technique to embed a watermark in the selected frames. Videos are the most distributed multimedia data across the internet. The proposed method aims to address the issues related to copyright protection and ownership identification. The addition of a watermark inside the multimedia data poses the challenge of quality loss of output video. This doctoral work addresses the issues related to quality loss and aims at high robustness values. For this purpose, some attack scenarios have been applied on watermarked frames to calculate the proposed technique's efficiency.

An extensive literature survey has been done on frame selection and watermark embedding mechanisms. The frame selection mechanism used in existing research [65] is time-consuming. The effectiveness of the watermark embedding technique is calculated using Quality Metrics (PSNR). Most researchers have used methods like an extreme learning machine, meta-heuristic techniques combined with frequency-domain techniques to carry out watermark embedding. The proposed research overcomes the existing studies gap by finding an optimal way to get high values of Peak Signal to Noise Ratio. In this doctoral research, a frame selection algorithm is proposed to find optimal numbers from the video frames. The processing of video starts by converting video into several frames using the approach of frame extraction. Embedding the watermark into several frames is time-consuming, as well as it is not secure as the watermark can be retrieved by an unknown user. The selection of frames is crucial in this research; a scene change detection mechanism implements it. The next step is to embed a watermark in selected frames. Hyperchaotic encryption is applied to the watermark before embedding the watermark to add more security to the proposed scheme. The watermark embedding is carried out by Graph-Based transform and Singular Value Decomposition.

There are different types of videos with fast scene changes and no frame changes, We have set the threshold to check the variation to select the number of frames. It is very challenging to find high accuracy of frame selection algorithm for fast motion videos and videos with no scene changes. The alternate selection criteria must be proposed in the future to detect frames from fast motion videos and constant videos. The frame content in low contrast videos is very dull, where any variation is easily detectable presents challenges in this work. The overall system is suitable for all applications, in some cases, videos get distorted very easily after embedding, so challenges of reconstructing the video can be faced in such scenarios.

However, the proposed technique (GBT-SVD) can be optimized using a hybrid algorithm to get high values of quality metrics (PSNR). Grey Wolf Optimization and Genetic Algorithm are used to optimize the embedding factor. The Optimized watermarking technique is known as GBT-SVD-GWO-GA. The performance parameters used in this research are PSNR (Peak Signal to Noise Ratio), NC (Normalized Correlation), SSIM (Structural Similarity Index Measure), and Bit Error Rate (BER). The proposed technique's robustness is tested after applying various signal processing attacks such as Gaussian Noise, Sharpening Attack, Rotation Attack, Blurring Attack, and JPEG Compression. The comparison analysis of GBT-SVD and GBT-SVD-GWO-GA is performed against different variance values of separate attacks. The experimental results indicate the optimized watermarking technique (GBT-SVD-GWO-GA) outperforms the other technique (GBT-SVD) in terms of quality metrics. The performance of the proposed technique is compared with existing research against frame selection time, robustness. The results indicate improved values of PSNR, NC, SSIM, BER over existing research.

5.3 Future Directions

The future directions in the area of watermarking are outlined below:

I. The proposed work can be enhanced for visible watermarking methods.

II. Design and development of run-time watermarking embedding technique will be one of the areas to be addressed in future work.
III. This work can be extended by adding audio, and the effects of watermark on audio can be addressed in future work.
IV. It would be interesting to design the framework for uncompressed(raw) videos with less embedding time.
V. The Image enhancement techniques on the selected frames will gain a lot of popularity in the future.
VI. The combination of Metaheuristic Techniques like PSO, GWO, and others for optimization of embedding factor will have most of the researchers working on it.
VII. The use of AES in the encryption mechanism in encryption of watermark will increase time complexity, so various techniques will be designed to reduce time complexity in this scenario.
VIII. The combination of GBT-DWT Transform for watermark embedding will be one of the areas to be worked on.

[1] F. H. Hartung, B. Girod, “Digital watermarking of raw and compressed video”, in proc. Digital Compression Technologies and Systems for Video Communications, International Society for Optics and Photonics, vol. 2952 ,1996, pp. 205–214.

[2] M. D. Swanson, B. Zhu, A. H. Tewfik, Transparent robust image watermarking, *in Proc. 3rd IEEE International Conference on Image Processing,* vol. 3, IEEE, 1996, pp. 211–214.

[3] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[4] J. K. Su, F. Hartung, B. Girod, “Digital watermarking of text, image, and video documents”, *Computers & Graphics*, vol. 22, no.6,1998, pp. 687–695.

[5] S. P. Mohanty, K. Ramakrishnan, M. Kankanhalli, A dual watermarking technique for images, *in: Proc. of the seventh ACM international conference on Multimedia (Part 2), ACM*, 1999, pp. 49–51.

[6] J.Zhang, J.Li, L.Zhang, "Video watermark technique in motion vector," in *Proc. XIV Brazilian Symposium on Computer Graphics and Image Processing*, Florianopolis, Brazil, 2001, pp. 179-182.

[7] M. Barni, F. Bartolini, T. Furon, “A general framework for robust watermarking security”, *Signal Processing*, vol. 83, no.10, 2003, pp. 2069–2084.

[8] C.S. Shieh, H.C. Huang, F.H. Wang, J.S.Pan, “Genetic watermarking based on transform-domain techniques”, *Pattern recognition*, vol. 37,no. 3, 2004,pp.555–565.

[9] G.B. Huang, Q.Y. Zhu, C.K. Siew, “Extreme learning machine: a new learning scheme of feedforward neural networks”, *in proc. IEEE International Joint Conference on Neural Networks*, Vol.2, 2004, pp. 985–990.

[10] R.M. Shen, Y.G. Fu, H.T. Lu,” A novel image watermarking scheme based on support vector regression”, *Journal of Systems and Software*, vol.78, no.1, 2005, pp. 1–8.

[11] M. Barni, F. Bartolini, N. Checcacci, “Watermarking of MPEG-4 video objects”, *IEEE Transactions on Multimedia*, vol. 7, no. 1, 2005, pp. 23–32.

[12] C.R. Piao, W.Z. Fan, D.M. Woo, S.S. Han, “Robust digital image watermarking algorithm using BPN neural networks”, *International Symposium on Neural Networks,* Springer, 2006, pp. 285–292.

[13] S. Bhattacharya, T. Chattopadhyay and A. Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC*," in proc. 2006 IEEE International Symposium on Consumer Electronics*, St. Petersburg, Russia, 2006, pp. 1-6

[14] C.R. Piao, S. Beack, D.M. Woo, S.S. Han, " A blind watermarking algorithm based on HVS and RBF neural network for digital image, *in International Conference on Natural Computation,* Springer, 2006, pp. 493–496.

[15] D. Ye, C. Zou, Y. Dai, Z. Wang, "A new adaptive watermarking for real time MPEG videos", *Applied Mathematics and Computation*, vol. 185, no.2, 2007, pp. 907–918.

[16] Q. Li, C. Yuan and Y. Zhong, "Adaptive DWT-SVD Domain Image Watermarking Using Human Visual Model*," in 9th International Conference on Advanced Communication Technology*, 2007, pp. 1947-1951,

[17] G.B. Huang, L. Chen, *Convex incremental extreme learning machine,* Neurocomputing, vol. 70, no. 16, 2007, pp. 3056–3062.

[18] P. Wang, Z. Zheng and J. Ying, "A novel video watermark technique in motion vectors", *in International Conference on Audio, Language and Image Processing*, 2008, pp. 1555-1559.

[19] D. Choi, H. Do, H. Choi, T. Kim, "A blind MPEG-2 video watermarking robust to camcorder recording", Signal processing, vol.90, no. 4, 2010, pp.1327–1332.

[20] R. Mehta, A. Mishra, R. Singh, N. Rajpal, "Digital image watermarking in DCT domain using finite Newton support vector regression", *in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) Sixth International Conference on IEEE*, 2010, pp. 123–126.

[21] C. Wu, Y. Zheng, W. Ip, C. Chan, K. Yung, Z. Lu, "A flexible H. 264/AVC compressed video watermarking scheme using particle swarm optimization-based dither modulation", *AEU-International Journal of Electronics and Communications*, vol. 65,no.1 ,2011,pp. 27–36.

[22] M. Jiang, Z.F. Ma, X.X. Niu, Y.X. Yang, "Video watermarking scheme based on MPEG-2 for copyright protection", *Procedia Environmental Sciences*, vol. 10, 2011, pp. 843–848.

[23] P.C. Su, C.S. Wu, F. Chen, C.Y. Wu, Y.C. Wu, A practical design of digital video watermarking in H. 264/AVC for content authentication, *Signal Processing: Image Communication*, vol. 26 ,no.8-9, 2011,pp. 413–426.

[24] G. Cheung, W. Kim, A. Ortega, J. Ishida and A. Kubota, "Depth map coding using graph based transform and transform domain sparsification*", in IEEE 13th International Workshop on Multimedia Signal Processing,* 2011, pp. 1-6,

[25] Y.-R. Wang, W.-H. Lin, L. Yang, "An intelligent watermarking methodbased on particle swarm optimization", *Expert Systems with Applications*, vol. 38, no. 7, 2011, pp. 8024–8029.

[26] C. Sharma, D. Prashar, “DWT Based Robust Technique of Watermarking”, *International Journal of Soft Computing and Engineering*, vol.2, no.2, 2012, pp.399-402.

[27] M.J. Lee, D.H. Im, H.Y. Lee, K.S. Kim, H.K. Lee, “Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues”, *Digital Signal Processing*, vol. 22, no.1, 2012, pp. 190–198.

[28] T. Tabassum, S. M. Islam, “A digital video watermarking technique based on identical frame extraction in 3-Level DWT”, *in: Computer and Information Technology (ICCIT) 15th International Conference (IEEE)*, 2012, pp. 101–106.

[29] Y. Yang, Y. Wang, X. Yuan, “Bidirectional extreme learning machine for regression problem and its learning effectiveness”, *IEEE Transactions on Neural Networks and Learning Systems* ,vol. 23, no. 9,2012, pp.1498–1505.

[30] G.B. Huang, H. Zhou, X. Ding, R. Zhang, “Extreme learning machine for regression and multiclass classification”, *IEEE Transactions on Systems, Man,and Cybernetics, Part B (Cybernetics)* ,vol. 42 ,no.2, 2012,pp. 513–529.

[31] V. Chaudhary, A. Mishra, R. Mehta, M. Verma, R. P. Singh, N. Rajpal, “Watermarking of Grayscale Images in DCT Domain Using Least-Squares Support Vector Regression”, *International Journal of Machine Learning and Computing*, vol. 2,no.6, 2012, pp. 725-728.

[32] N. Ramamurthy, S. Varadarajan, “The robust digital image watermarking scheme with back propagation neural network in DWT domain”, *Procedia Engineering*, vol. 38, 2012, pp. 3769–3778.

[33] Y. He, G. Yang, N. Zhu, “A real-time dual watermarking algorithm of H.264/AVC video stream for Video-on-Demand service”, *AEU-International Journal of Electronics and Communications*, vol. 66, no. 4, 2012, pp. 305–312.

[34] O. S. Faragallah, “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain”, *AEU-International Journal of Electronics and Communications*, vol. 67, no.3, 2013, pp.189–196.

[35] T. R. Singh, K. M. Singh, S. Roy, “Video watermarking scheme based on visual cryptography and scene change detection”, *AEU-International Journal of Electronics and Communications,* vol. 67, no. 8, 2013, pp. 645–651.

[36] C. Agarwal, A. Mishra, A. Sharma, “Gray-scale image watermarking using GA-BPN hybrid network”, *Journal of Visual Communication and Image Representation,* vol.24,no.7, 2013, pp.1135–1146.

[37] E.Mansoor, C.C.Wai , “Secure Force: A Low-Complexity Cryptographic Algorithm for Wireless Sensor Network (WSN)", *in International Conference on Control System, Computing and Engineering(IEEE)*, 2013, pp.557-562

[38] A. Mishra, C. Agarwal, A. Sharma, P. Bedi, “Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm, Expert Systems with Applications”, vol.41, no. 17, 2014, pp. 7858–7867.

[39] A. Mishra, P. Chuttani, “Motion vector estimation based uncompressed video watermarking using extreme learning machine”, *International Journal of Scientific & Engineering Research*, 2014, pp. 762–768.

[40] M. Masoumi, S. Amiri, “Content protection in video data based on robust digital watermarking resistant to intentional and unintentional attacks”, *The International Arab Journal of Information Technology*, vol.11, no.2, 2014, pp. 204–212.

[41] C. Agarwal, A. Mishra, A. Sharma, G. Chetty, “A novel scene based robust video watermarking scheme in DWT domain using extreme learning machine”, *in: Extreme Learning Machines 2013: Algorithms and Applications, Springer*, 2014, pp. 209–225.

[42] B.Patel, RC Patel, Overview of watermarking and cryptography both for real time speech communication,*ISETR*,vol.3,no.2,2014,pp.279-285

[43] S. Gonge, A. Ghatol, “Combination of encryption and digital watermarking techniques used for security and copyright protection of still image. International Conference on Recent Advances and Innovations in Engineering”,*ICRAIE*, 2014, pp. 1-6.

[44] M. Ali, C. W. Ahn, P. Siarry, Differential evolution algorithm for the selection of optimal scaling factors in image watermarking, *Engineering Applications of Artificial Intelligence* ,2014) 15–26.

[45] P. Venugopala, H. Sarojadevi, N. N. Chiplunkar, V. Bhat, “Video watermarking by adjusting the pixel values and using scene change detection”, *in: Signal and Image Processing (ICSIP), 2014 Fifth International Conference (IEEE)*, 2014, pp. 259–264.

[46] S. Mirjalili, SM. Mirjalili, A.Lewis, “Grey Wolf Optimizer”, *Advances in Engineering Software*, vol.69, 2014,pp.46-61

[47] C.T. Yen, Y.J. Huang, “Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network”, *Multimedia Tools and Applications* ,2015, pp. 1–11.

[48] A. Rajpal, A. Mishra, R. Bala, “Robust blind watermarking technique for color images using Online Sequential Extreme Learning Machine”, *in: Computing, Communication and Security (ICCCS), International Conference (IEEE)*, 2015, pp. 1–7.

[49] S. Kulakarni , C.Sharma, "Efficient Watermarking Technique using DWT, SVD, Rail Fence and 10's Complement Applied on Digital Images", *IJAER*, 2015,vol. 10,no.55,pp.164-169.

[50] D. Thind, S.Jindal , "A Semi Blind DWT-SVD Video Watermarking", *Procedia Computer Science*, 2015, pp. 1661- 1667.

[51] C. Agarwal, A. Mishra, A. Sharma, "A novel gray-scale image watermarking using hybrid Fuzzy-BPN architecture", *Egyptian Informatics Journal*, vol.16, no. 1, 2015, pp. 83–102.

[52] B.Sridhar , C. Arun, "An Enhanced Approach in Video Watermarking with Multiple Wavelets", *International Journal of communication Technology and Electronics*, vol. 61, no.2,2016, pp. 165-175.

[53] P.Rasti , S.Samiei, M.Agoyi, S.Escalera, G.Amharjafari, "Robust Non Blind Color Video Watermarking using QR Decomposition and Entropy Analysis", *Journal of Visual Communication and Image Representation*,2016,pp. 838-847.

[54] Su Po-Chyi,Kuo Tien-Yin and Li Meng-Huan, "A Practical Design of Digital Watermarking for Video Streaming Services", *International Journal of Visual Communication and Image Represenation*,vol.38,2016,pp-1-33.

[55] C.Sharma , G.Singh, G.Saini, "Efficient Video Watermarking Technique for Quality Loss of Data*", Indian Journal of Science and Technology*, Vol 9(47),2016,pp.1-5.

[56] A. Rajpal, A. Mishra, R. Bala, "Multiple scaling factors based Semi-Blind watermarking of grayscale images using OS-ELM neural network", *in: Signal Processing, Communications and Computing (ICSPCC) International Conference (IEEE)*, 2016, pp. 1–6.

[57] J. Hou, H. Liu and L. Chau, "Graph-based transform for data decorrelation", *in IEEE International Conference on Digital Signal Processing (DSP)*, 2016, pp. 177-180

[58] N.Mittal, U.Singh, B.Singh Sohi, "Modified Grey Wolf Optimizer for Global Engineering Optimization", *Applied Computational Intelligence and Soft Computing*, vol. 2016.

[59] K. Ait Sadi, A. Guessoum, A. Bouridane, F. Khelifi, "Content Fragile Watermarking for H.264/AVC Video Authentication", *International Journal of Electronics*,vol.104,2016,pp-673-691.

[60] A. Mishra, C. Agarwal, "Toward optimal watermarking of grayscale images using the multiple scaling factor–based cuckoo search technique", *Bio-Inspired Computation and Applications in Image Processing*,2017, pp. 131–155.

[61] Li Y, Wang C, Chen H, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation", *Optics and Lasers in Engineering*,vol. 90,2017,pp. 238–246.

[62] A. Fouad, “A Hybrid grey wolf optimizer and genetic algorithm for minimizing potential energy function”, *Memetic Computing*, vol.9,no.4, 2017,pp.347-359.

[63] E.Farri,P.Ayubi,"A Blind and Robust Video Watermarking Based On IWT and New 3D Generalized Chaotic Sine Map", *Non Linear Dynamics*,vol.9,no.4, ,2018, pp.19875-1897.

[64] I.Nouioua, N. Amardjia, S. Belilita, “A Novel Blind and Robust Video Watermarking Technique in Fast Motion Frames Based on SVD and MR-SVD”, Security and Communication Network,2018.

[65] A.Rajpal, A .Mishra, R .Bala, “A Novel fuzzy frame selection based watermarking scheme for MPEG-4videos using Bi-directional extreme learning machine”,*Applied Soft Computing Journal*,2019,pp.603-620.

[66] C. Sharma , A. Bagga, “Video Watermarking Scheme Based on DWT, SVD, Rail Fence for Quality Loss of Data”, *in 4th International Conference on Computing Sciences (ICCS)*, 2018, pp. 84-87

[67] Q.Gu, X. Li,S. Jung, “Hybrid Genetic Grey Wolf Algorithm for Large Scale Global Optimization”, *Advances in Architecture, Big Data,and Machine Learning techniques for complex Internet of Things Systems*,2019.

[68] H.Egilmez,Y.Hsuan,C. Ortega, “Graph-based Transforms for Video Coding”, *IEEE Transactions on Image Processing*,vol.29,2019.

[69] Z.Cao., L. Wang, “A secure video watermarking technique based on hyperchaotic Lorentz system”, Multimedia Tools and Applications, vol.78, no.18, 2019.

[70] L.Chen,L.Lei, Z.Jie, “A Hyperchaotic Color Image Encryption Algorithm and Security Analysis”, *Security and Communication Networks*,2019.

[71] Wang, JS., Li, SX. An Improved Grey Wolf Optimizer Based on Differential Evolution and Elimination Mechanism. *Scientific Reports* ,vol.9, no.1,2019.

[72] A.Hammami, A.Hamida, C.Amar, "A Robust Blind Video Watermarking Scheme based on Discrete Wavelet Transform and Singular Value Decomposition", *in proc. of the 14th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications* , pp. 597-604,2019.

[73] P.Hu, J.Pan, S.Chu, “Improved Binary Grey Wolf Optimizer and Its application for feature selection”, *Knowledge-Based Systems*,vol. 195, 2020.

[74] H. Nsour, Al, M. Alweshah, A.Hammouri, H.Ofeishat,S.Mirjalili, “A Hybrid Grey Wolf Optimiser Algorithm for Solving Time Series Classification Problems”, *Journal of Intelligent Systems,* vol. 29, no. 1, 2020, pp. 846-857.

[75] Z.Yue, S.Zhang , W.Xiao, “A Novel Hybrid Algorithm Based on Grey Wolf Optimizer and Fireworks Algorithm”, *Sensors*, vol. 20, no.7, 2020.

[76] C. Sharma , A.Bhaskar , “A review on video watermarking techniques for compressed domain with optimization algorithms”, *Materials Today: Proceedings,2020*.

[77] J. Sang, Q.Liu, C. Song, Robust video watermarking using a hybrid DCT-DWT approach, *Journal of Electronic Science and Technology*, vol.18, no. 2,2020.

[78] M. Begum, M. Uddin, “Digital Image Watermarking Techniques: A Review”, *information*, mdpi, 2020.

[79] R. Mehta, K.Gupta, A.K.Yadav, “An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain”, *Multimedia Tools and Applications,* vol. 79**,** 2020, pp**.** 18657–18678.

[80] E.Houby, N.Yassin, “Wavelet-Hadamard based blind image watermarking using genetic algorithm and decision tree”, *Multimedia Tools and Applications,*vol.79, ,2020, pp.28453–28474.

[81] C.Xu, J.Sun, C.Wang, “An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems”, *International Journal of Bifurcation and Chaos*, vol. 30, no. 04, 2020.

[82] N. Yadav, D. Rajpoot and S. K. Dhakad, “Optimization of Watermarking in Image by Using Particle Swarm Optimization Algorithm”, *in 6th International Conference on Signal Processing and Communicati-on (ICSC)*, 2020, pp. 85-90.

[83] Z. Shuqin, Z. Congxu, “Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding”,*Entropy*, mdpi, 2020.

[84] V.Shankar, R.Prasad, R.Adiraju, R.Krishna, “A Review Paper Based on Image Security Using Watermarking*”, in Proc. of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications* ,2021, pp.697-706.

[85] F. Kahlessenane, A. Khaldi, R. Kafi , S. Euschi, “A robust blind medical image watermarking approach for telemedicine applications”, *Cluster Computing*,2021.

[86] A. Seyyedabbasi ,F. Kiani, “I-GWO and Ex-GWO: improved algorithms of the Grey Wolf Optimizer to solve global optimization problems”, *Engineering with Computers,* vol.37**,** 2021**,** pp. 509–532.

[87] W.Jinwei, Q. Jiasheng, S. Wei, L. Xiangchun, Z. Lizhi, Z. Xiaobing,A Novel Improved Reversible Visible Image Watermarking Algorithm Based on Grad-CAM and JND, *Security and Communication Network*,2021.

[88] P.Khare, V.K Srivastava, "A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain", *Multidimensional Systems and Signal Processing*, vol. 32**,** 2021, pp.131–160

[89] G. Negi,A. Kumar,S. Pant,M. Ram, "GWO: a review and applications", *International Journal of System Assurance Engineering and Management*,vol.12,2021,pp.1-8

[90] C. Sharma, A. Bagga , R. Sobti ,T. Lohani, M.Shabaz, "A Secured Frame Selection Based Video Watermarking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption", Security and Communication Network,2021.

DISSEMINATION OF WORK

Published Work in Journals

C. Sharma, A. Bagga , R. Sobti ,T. Lohani, M.Shabaz, "A Secured Frame Selection Based Video Watermarking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption", Security and Communication Network,2021(SCI-Indexed).

C.Sharma , G.Singh, G.Saini, "Efficient Video Watermarking Technique for Quality Loss of Data*"*, *Indian Journal of Science and Technology*, Vol 9(47),2016,pp.1-5(Scpus Indexed).

C. Sharma , A.Bhaskar , "A review on video watermarking techniques for compressed domain with optimization algorithms", *Materials Today: Proceedings,2020*(Scopus Indexed).

C. Sharma, A. Bagga, B.Singh, M.Shabaz, "A Novel Optimized Graph Based Transform Watermarking Technique to Address Security Issues in Real Time Application", *Mathematical Problems in Engineering,*2021(SCI-Indexed).

Published Work in Conferences

C. Sharma , A. Bagga, "Video Watermarking Scheme Based on DWT, SVD, Rail Fence for Quality Loss of Data", *in 4th International Conference on Computing Sciences (ICCS)*, 2018, pp. 84-87(Scopus Indexed).

Accepted Paper in Conferences

C.Sharma, A.Bagga, "Frame selection based video watermarking technique based on DWT, K-SVD, rail fence to address quality loss of data", *in 3rd International Conference on Intelligent Circuits and Systems (ICICS 2020),*2020(Scopus Indexed).

Paper Under Review

C.Sharma, A.Bagga, "A Secured Graph-Based Transform Watermarking Technique in Real-Time Applications", *Journal of Real-Time Image Processing* ,2021(SCI-Indexed).

C.Sharma, A.Bagga, R.Sobti, "A Robust Image Encrypted Watermarking Technique in Medical Field Application", *Informatics in Medicine-Unlocked,* 2021(Scopus-Indexed).