Hindawi
Security and Communication Networks
Volume 2021, Article ID 5536170, 19 pages
https://doi.org/10.1155/2021/5536170

Research Article

A Secured Frame Selection Based Video Watermarking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption

Chirag Sharma,[1] **Bagga Amandeep**,[2] **Rajeev Sobti**,[1] **Tarun Kumar Lohani**,[3] **and Mohammad Shabaz**[1]

[1]*Department of Computer Science and Engineering, Lovely Professional University, Punjab, India*
[2]*Department of Computer Application, Lovely Professional University, Punjab, India*
[3]*Arba Minch University, Arba Minch, Ethiopia*

Correspondence should be addressed to Chirag Sharma; chiragsharma1510@gmail.com

Received 29 January 2021; Revised 10 February 2021; Accepted 16 February 2021; Published 8 March 2021

Academic Editor: Manjit Kaur

The advancement of Internet technologies has led to the availability of audios, images, and videos in different forms. The unauthorized users are exploiting the use of multimedia by transmitting them on various Internet sites to earn money unethically without the intervention of the original copyright holder. Watermarking is a technique used to hide the signal known as watermark inside multimedia data that is not visible to the intruder to manipulate any information. In this paper, a secured watermarking approach is developed to tackle issues related to copyright protection and ownership identification. A Secured Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption hybrid techniques are proposed. The watermark cannot be embedded in every frame of the video as it adds to the size of the video and watermark can be easily retrieved by an intruder. Therefore, the frame selection algorithm has been proposed in the given work. Adding watermark in the frame adds to the challenge of quality loss. The quality loss is addressed in this work. Various attacks have been applied on the watermarked frames to calculate the performance of the proposed technique using quality metrics: Peak Signal to Noise Ratio, Structural Similarity Index, Normalized Correlation, and Bit Error Rate. The results indicate that the proposed technique is effective against various attack scenarios.

1. Introduction

The availability of multimedia data across Internet has prompted unauthorized persons to illegally distribute multimedia data such as videos across the Internet. The issues like copyright protection and ownership identification are prominent and the development of the secured technique is required to counter these issues. Videos are the most attackable multimedia data and unauthorized people are distributing videos for their own benefits and are earning lots of money in this regard. The illegal distribution of video is illustrated in Figure 1 where videos are exposed to the Internet after DVD release or movie release and this problem has led to huge loss of movie industry. The real time videos are gaining lots of popularity with various OTT platforms like NETFLIX and AMAZON PRIME. The problem of copyright protection again emerges as the videos from these platforms are getting released to the Internet and thus drops the number of users accessing these websites. There is a need of a secured technique to identify these unauthorized users, thus stopping this illegal distribution. Watermarking is a technique that embeds secret and unnoticeable signal inside the video which is unidentifiable to any unauthorized user. The watermarking embeds encrypted watermark inside the multimedia data and the process of extraction is done from the researcher's side to test validity of scheme. The videos need to be watermarked before they are distributed across the network.

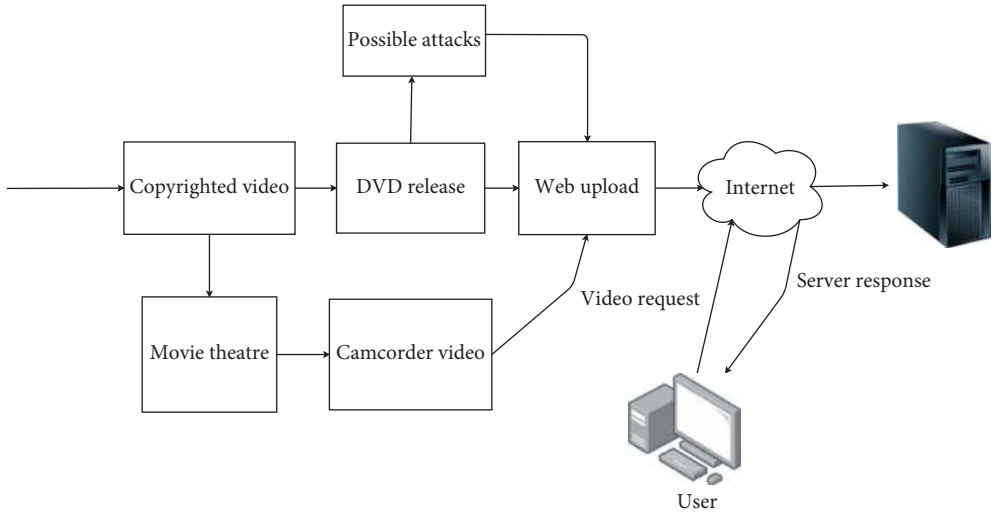


Figure 1: Illegal distribution of multimedia data.

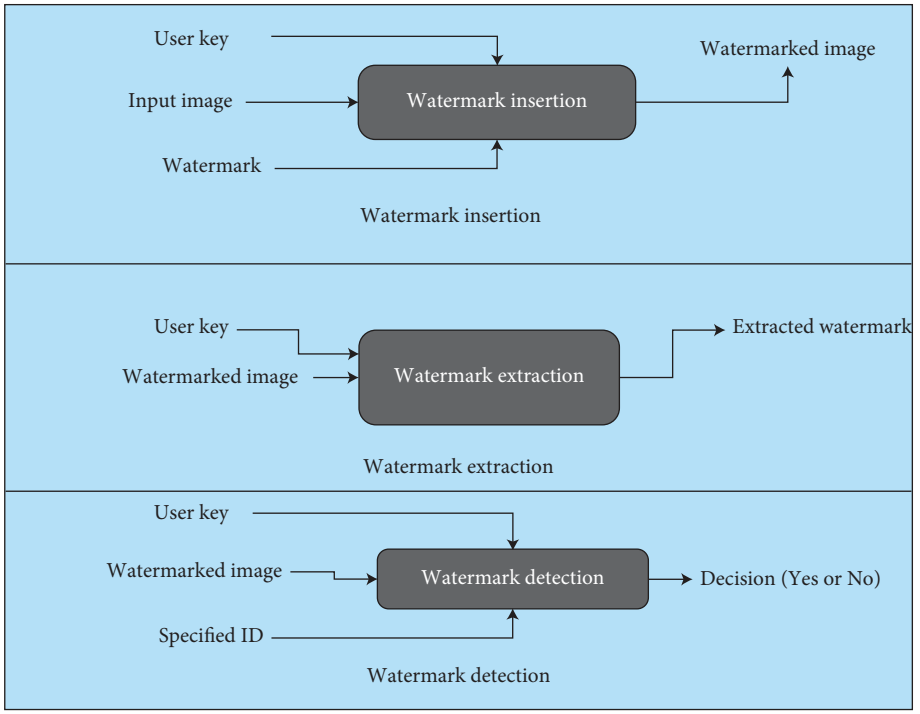


Figure 2: Process of watermarking.

Figure 2 describes the process of watermarking with the addition of key inside the watermark being embedded.

The proposed technique in this paper embeds the secret signal with additional security feature so that unauthorized person cannot identify it. The real time videos are available in compressed domain because it is very challenging to distribute uncompressed domain videos across the Internet. The uncompressed videos are raw videos and compressed domain videos are encoded versions of raw videos. The videos are available in many codecs like XVID, H.264, H.265, and WMV. The codec used for real time video is H.264. The proposed technique will embed the watermark in compressed domain videos. The major challenges in embedding the watermark in the video are the selection of frames and quality loss after embedding.

The selection of frames is done because watermark cannot be embedded in every frame of the video as it will be very easy for the unauthenticated user to detect watermark and remove it. The quality loss is the major constraint in the research as embedding of watermark affects quality of the video. There are many watermarking techniques available. The different types of techniques are described in Figure 3. The most common types of watermarking techniques are frequency domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Many researchers are applying these techniques to provide

solution to these problems. Although these techniques are good, improvement can be done in many aspects. The encryption mechanism used in the proposed technique adds to additional security feature as it would be very difficult for any intruder to detect watermark and recover watermark from watermarked video. The proposed technique used in the research is based on Graph Based Transform along with Singular Valued Decomposition. This combination is applied to encrypted watermark. The encryption can be done in many ways such as Ciphers, AES, and DES. The reason why AES and DES are not used for encrypting watermark is that they are very compressed and make the watermarking algorithm even more complex so the hyperchaotic encryption [1] is used in the research.

The validity of the proposed technique is tested after applying certain signal processing attacks to watermarked video. Gaussian Noise, Sharpening Attack, Rotation, Blurring, and JPEG Compression attacks have been applied on watermarked video. Quality parameters, Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), Normalized Correlation (NC), and Bit Error Rate (BER), have been used in the research. The major contribution of this manuscript is summarized as follows.

(a) We proposed the frame selection algorithm that identifies best suitable frames from the compressed domain video.

(b) We proposed novel technique Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption for watermark embedding.

(c) We evaluated the performance of the proposed technique against various signal processing attacks.

The organization of this paper is as follows: Section 2 reviews all the related work done in this area, Section 3 presents the research methodology of the proposed technique, Section 4 presents results gathered from various experiments performed on selected set of videos, and Section 5 describes conclusion obtained from the given research.

2. Related Work

The number of video watermarking techniques has been proposed in the field of watermarking. The most prominent watermark embedding technique is Discrete Wavelet Transform (DWT). This technique has been applied by many researchers as transformation of a frame to DWT is a reliable method. Spatial Domain Methods given in this paper are fast but not robust enough to handle any signal processing attacks [2, 3]. Frequency domain techniques like DWT and DCT have been used by many researchers. The techniques are good but suffer from the problem of dimensionality reduction; that is why these techniques were coupled with another technique named as Singular Valued Decomposition (SVD). The major constraint in watermarking is the area where watermark is embedded. Many techniques and methods have been proposed nowadays where study is made on feature selection and feature extraction. The fast methods like SLFNs have been proposed in [4] which are based on extreme learning machine. The optimization algorithms such as PSO [5] improve the efficiency of existing algorithms by targeting high values of fitness function with their respective mathematical model. The watermarking technique can be made more secure by adding encryption mechanism in it. The technique proposed in [6] adds security features to the abovementioned mechanism. The performance of the frequency domain techniques can be optimized using optimization algorithms like genetic algorithm [7]. The PSO algorithm [8] also optimizes the performance of watermarking technique by taking quality parameter into consideration. Graph Based Transform is a new kind of transform that interprets graph in the form of signal. A new transform based on graphs was proposed for depth map coding [9]. The process of frame selection is very important aspect of the research. The frame selection algorithm is proposed by using identical frame extraction concept [10]. The process of scene change detection was applied by Masoumi [11]. The proposed work is inspired from the research done over the years on the videos and intends to solve problems of existing research. Different frequency domain techniques are used in watermarking [12] but DWT has been used by many researchers. The application of SVD was to extract good number of features for performing transformation as largest coefficients in S component of SVD Matrix can resist image compression and processing attacks and embedding of watermark will not be affected when any of frequency domain methods is coupled with SVD [13]. Fourier Transform is also the part of Frequency Domain Technique [14] but the technique does not produce good results in terms of imperceptibility. The process of frame selection is done on the basis of number changes in scenes of the frames. The calculation is done using histogram difference [15]. A new Grey Wolf Optimizer is used to solve local optimum problems and find optimal solution from given set of solutions. GWO is an efficient PSO technique [16]. Hybrid combination of DWT-SVD was proposed by

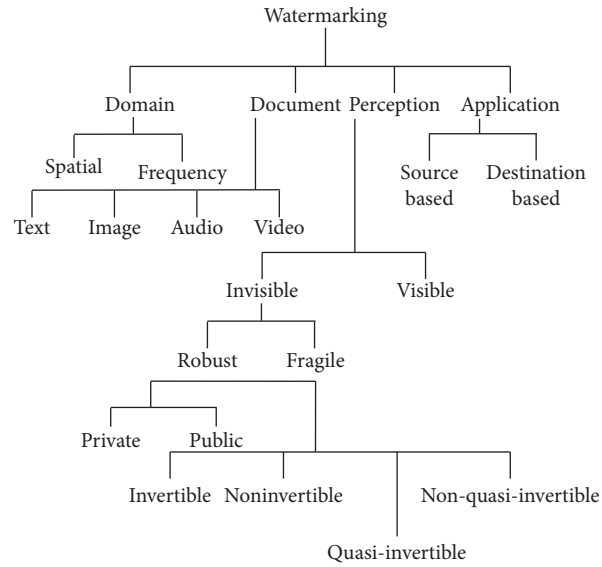


Figure 3: Watermarking techniques.

various researchers. A hybrid technique based on DWT-SVD along with firefly algorithm got high values of quality parameters [17]. A video watermarking technique was proposed using multiple wavelets with the application of DWT-SVD [18]. GBT Transform is applied for data decorrelation [19] which is also an effective transform that can be applied to multimedia data. A semiblind DWT-SVD technique was proposed on compressed domain videos [20]. Graph Fourier Transform is used for depth map coding. This technique produces good results in multimedia data [21]. The hybrid transform DWT-SVD produces favorable results in terms of quality parameters. The hybrid transform is combined with Fuzzy BPN Architecture for grey scale images. It was producing good visual quality of watermarked image [22]. The DWT-SVD was applied on videos by Sharma [23]. The watermark embedding techniques hide the signal in the multimedia data but, to ensure security of data, various encryption techniques have been used along with frequency domain techniques. Wang [24] proposed encrypted watermarking technique using multiple kinds of chaos. A Hybrid Genetic Algorithm combined with fruit fly optimization [25] addresses QOS parameter that helps to solve the problem in less computation time. The same technique can be used in watermarking to produce good results. A hybrid technique that combines BWT-SVD and optimization algorithm was proposed [26] to embed watermark in multimedia data. The blind H.264 compressed domain technique was proposed to find certain areas of the frames to embed watermark. Pattern recognition technique was proposed [27]. Sharma [28] enhanced the work by adding transpositional cipher in the combined transform of DWT-SVD to enhance security. Transpositional cipher used in [29] had issues in security. The cipher used in research [30] enhances security of any watermarking technique. Combined approach on Graph Based Transform and Singular Valued Decomposition was proposed for images in the respective work [31]. Cao [1] proposed an encryption technique that produces good results compared to others. The GBT-SVD Transform produces better results than GBT used in previous research [9, 19]. Table 1 illustrates the gaps found in recent studies in this field.

3. The Proposed Methodology

In this section, we propose a frame selection mechanism followed by watermark embedding and application of certain attacks on the proposed technique. In this research, frame selection process is important as watermark information is sensitive that should not be leaked to any intruder. Embedding watermark in every frame makes the information easily accessible to unidentified user and adding watermark in every frame increases the size of watermarked video. Therefore, frame selection mechanism is important. This mechanism is followed by watermark embedding and then evaluation of proposed technique is done by applying certain attack scenarios.

3.1. Frame Extraction and Selection. The first phase in the proposed work is to find the suitable number of frames from extracted frames of the video. The process of finding suitable frames in real time is done using scene change detection. The watermark cannot be embedded on all frames of the video as it becomes every easy for any intruder to detect the watermark and add watermarking to all frames which also increases the size of the video. The process of finding suitable frames becomes significant. To select significant frames, scene change detection mechanism is applied. The comparison of adjacent frames with one another is performed. The grouping of identical frames is done. The value of the frame difference will decide whether frame will be considered as the part of the same group or different group. If difference is large, then it will be considered as part of different group. The parameter of decision will be taken as threshold; if the value of frame difference is higher than the value of threshold, the next frame will be the part of next group. The same is illustrated in Figure 4. The temporal sampling is performed that enhances the process of frame selection that gives better results compared to [10]. The selection of the first frame is done from all different groups. Frame difference can be represented as histogram difference that can be expressed as

$$\mathrm{FD}_k = \sum_{k=1}^{I} T_k(m) - T_k(m+1), \tag{1}$$

where FD_k is representing frame difference and T_k is the histogram value of k^{th} frame of level m and I is the number of levels of the histogram. The grouping of similar images is based on scene change detection. The threshold is maintained to detect intensity histogram difference to calculate sudden transition amongst frames (in order to find larger frame difference). This scenario is expressed as

$$K_b = \mu + \alpha\sigma, \tag{2}$$

K_b is threshold value. σ and μ are the standard deviation and mean value of selected frame intensity histogram difference. The selected value of α in the research is 2.8. The temporal sampling has also enhanced the process of frame selection. The criteria of frame selection depend upon the comparison of FD_k with K_b. The algorithm was tested on 6 videos. Relevant frame selection was done. The standard frame rate taken is 29.97. A total of 6 videos have been taken as data set for this process.

The videos with a greater number of scene changes will have a greater number of selected frames. This process is illustrated with the help of algorithm given as Algorithm 1.

The Akiyo video did not have any scene changes; hence, no frames will be selected and watermark embedding will not take place. Watermark embedding follows frame selection process only. The evaluation parameter of this step is total frame selection time from extracted frames of the video. The process of frame extraction is done followed by frame selection. Some videos have a smaller number of scene changes; hence, less frames will be selected. In case there is no detection of any scene done, then no selection of frame takes place. The pure storage video has higher number of scene changes;

Table 1: Analysis with related work.

Reference	Main contribution	Gaps
Tabassum [10]	In this research, identical frame extraction technique is proposed with 3-level DWT frame selection done using frame difference method. DWT is applied to higher band coefficients to get robustness against signal processing attacks.	The quality is compromised and watermark embedding technique could be more efficient.
Masoumi [11]	In this research, frame extraction is done by taking motioned part of the video; scene change detection is applied. Color separation of selected frame is done and watermark embedding is done in blue channel. Watermark is considered as pseudorandom numbers; each bit of watermark can be taken as scattered randomly through video frames in order to provide additional security feature.	The proposed algorithm becomes complex by applying a secured, encrypted technique.
Mishra [17]	In this research, DWT-SVD technique is proposed along with optimization firefly algorithm using multiple scaling factors. The optimization adds to high values of quality parameters.	The technique is applied on grey scale images and additional security feature can be added.
Sridhar [18]	In this research, hybrid DWT-SVD is applied on the videos with multiple wavelets. The efficiency of hybrid technique is always better than DWT.	The efficiency of frame selection algorithm is compromised.
Rajpal [29]	In this research, fuzzy frame selection scheme with bidirectional extreme learning machine is done. Fuzzy rules are based on luminance, edge, and texture sensitivity. Fuzzy frame selection is based on scene change detection; weighting factor is based on these 3 parameters.	Security is compromised using transposition cipher.

hence more frames will be selected. The importance of frame selection comes from the fact that watermarking on still number of frames will give a chance to any unauthorized person to get access of watermark content because of similar properties [32]. Figure 4 depicts the process of frames selection. Frame selection using scene change detection is giving better results especially in uncompressed domain. The grouping of similar images is done and threshold is calculated using (2); the moment scene change is detected, the first frame in the individual frame is selected and the same process follows till all the extracted frames are processed [33]. The process is fast avoiding similar frames to be selected, thus saving the time for frame selection and saving overall embedding time for embedding process. The results are formulated in MATLAB 2019b using i5 processor.

3.2. The Proposed Technique of Watermarking. The next step after selection of frames is to embed encrypted watermark. Watermark is encrypted before it is embedded to selected frame [34]. Watermark embedding poses a great challenge of quality loss. To counter the problem of quality loss after embedding, the technique is supposed to be proposed that aims at high values of quality parameters like PSNR. Hybrid combination of Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption is proposed to counter the security issues in multimedia data. Graph Based Transform (GBT) is a transform that uses signal in the form of graph and produces better results in terms of adapting signal structure of an image [35]. GBT is used as it is robust against various attack scenarios in the field of image processing. Singular Valued Decomposition counters the issues of dimensionality reduction [36]. After frame selection is done, selected frames are applied with GBT Transform followed by SVD and at the same time watermark is encrypted with Hyperchaotic Encryption before being applied to selected frame. The selected frame is taken as a signal in the form of a graph and transformation is applied using GBT [37]. The S value is taken after SVD is applied. The watermark is encrypted using Hyperchaotic Encryption and SVD is applied to it [38]. The S values of the selected frame and watermark are combined to form modified S value of watermarked frame. The proposed watermark embedding technique is further discussed in the following sections.

3.2.1. Embedding Technique. Graph Based Transform is a newly formed transform that is represented by $G = \{V; E; s\}$ where V and E are the vertices and edges of the graph, and s represents the frame signal [39] for graph G

$$M(i, j) = \left\{ \begin{array}{ll} \sum mi, j, & \text{if } i = j, \\ 0, & \text{otherwise} \end{array} \right\}, \tag{3}$$

where $m_{i,\ j}$ represents the weight of the edge. The degree matrix $D \in N \times N$ is a diagonal matrix, where elements are

$$K(i, j) = \left\{ \begin{array}{ll} \sum mi, j, & \text{if } i = j, \\ 0, & \text{otherwise} \end{array} \right\}. \tag{4}$$

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

$$L = K - M, \tag{5}$$

where the operator L is also known as Kirchhoff operator, which is represented as adjacency matrix A. Eigenvalue decomposition is done to set of real nonnegative eigenvalues which are represented by $\wedge = \{\lambda 1, \lambda 2, \ldots \lambda \mathbf{N}\}$; 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.

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

$$A = \sum_{A=1}^{r} EA * SA * (RA)^T = \sum_{i=1}^{r} Ei * Si * (Ri)^T, \tag{8}$$

$$E_A = [e1, e2, e3, e4 \ldots\ldots eN], \tag{9}$$

$$R_A = [r1, r2, r3, r4 \ldots\ldots rN], \tag{10}$$

$$S_y = \begin{pmatrix} S_1 & \cdots & N \\ \vdots & \ddots & \vdots \\ 0 & \cdots & S_N \end{pmatrix}, \tag{11}$$

$$A = \mathrm{E}SR^T, \tag{12}$$

$$WF''(i, j) = A(i, j) + \alpha W(i, j). \tag{13}$$

Singular Valued Decomposition is done using equation number 10 where transform is done using S as it is more resistant to image processing attacks.

3.2.2. Encryption of Watermark before Embedding. The watermark embedded on selected frames is encrypted using Hyperchaotic Encryption to add security feature to the proposed technique [1]. The value of x, y, z, and w calculated from above equation will be used for encrypting the watermark image to be used in a frame. The standard values of a, b, and c were taken as per the values in reference [1]. The second step is the conversion of R; S is done into x, y for column and row of the encrypted watermark image. The 3rd step is to interchange the coefficients of m^{th} row and $x(m)^{\text{th}}$ row of image $W - m = 1, 2, \ldots i, N = 1, 2, \ldots j$; see Algorithm 2.

$$\left\{ \begin{array}{c} x = a(y - x) + w \\ y = cx - y - xz \\ z = xy - bz \\ w = -yz + rw \end{array} \right\}, \tag{14}$$

$$X = \mathrm{mod}(\mathrm{floor}(R + 100) * 105, i) + 1, \tag{15}$$

$$Y = \mathrm{mod}(\mathrm{floor}(S + 100) * 105, j) + 1, \tag{16}$$

$$W(m, :) = W(x(m), :), \tag{17}$$

$$W1 = W, \tag{18}$$

$$W1(:, n) = W1(:, y(n)). \tag{19}$$

The encryption of a watermark image is represented as $W(i, j)$ where image size is represented as $m * n$. The first step is generating the sequence of R, S using Lorenz system. The security feature added here adds to security feature by encrypting watermark before being embedded, thus making the technique more secure. Real time applications like broadcasting face security issues and copyright protection; the proposed technique combined with Hyperchaotic Encryption adds to security feature and also adds to copyright protection. Figure 5 depicts watermark embedding process.

3.3. Extraction Procedure. The next section in the proposed work describes watermark extraction procedure so as to recover watermark from watermarked video. The extraction of a watermarked from watermarked video is a reverse process of embedding when watermark was embedded with the help of (13). The extraction of frames is followed by applying GBT and SVD and the extraction is calculated as per the following equation. This is followed by inverse GBT and inverse SVD; then decryption is done using a key; then watermark is recovered. Figure 6 depicts watermark extraction process:

$$W_{i,j} = WF'_i - \frac{A_{i,j}}{\alpha}, \tag{20}$$

where $W(i, j)$ is extracted watermark, $\mathrm{WF}'(i, j)$ is watermarked frame, and $A(i, j)$ is selected frame.

The extraction procedure is used to find the difference between original and extracted watermarks. High difference between both of the watermarks suggests that the technique is not efficient; however, as per result calculation, it was found that there is a negligible difference amongst both watermarks after extraction is done, as shown in Algorithm 3.

3.4. Performance Evaluation. The performance evaluation of the watermarking technique is typically calculated in terms of quality parameters of the video and robustness against various attack scenarios such as Gaussian Noise, Sharpening, Rotation, Blurring, and JPEG Compression. The parameters are PSNR, SSIM, NC, and BER.

(a) PSNR (Peak Signal to Noise Ratio) is a major quality parameter that differentiates original and watermark frame based on Mean Square Error. The average PSNR is sum of PSNR of all selected frames divided by number of frames. The objective of the proposed technique is obtaining high values of PSNR as embedding of watermark causes quality loss. Higher values of PSNR indicate the efficiency of the technique. It is calculated by following equation:

$$\mathrm{MSE} = \sum_{i=0}^{G-1} \sum_{j=0}^{H-1} \frac{1}{G * H} ([AI(i, j) - EI(i, j)])^2, \tag{21}$$

where G and H are rows and columns of the image:

$$\mathrm{PSNR} = \frac{10 \log_{10} (255)^2}{\mathrm{MSE}}, \tag{22}$$

$\mathrm{AI}(i, j)$ is selected frame;

$\mathrm{EI}(i, j)$ is watermarked frame.

$$\text{Average PSNR} = \frac{\sum_i^n \mathrm{PSNR}_i}{n}. \tag{23}$$

(b) Normalized Correlation (NC): this parameter is used to find correlation between watermarked frame and

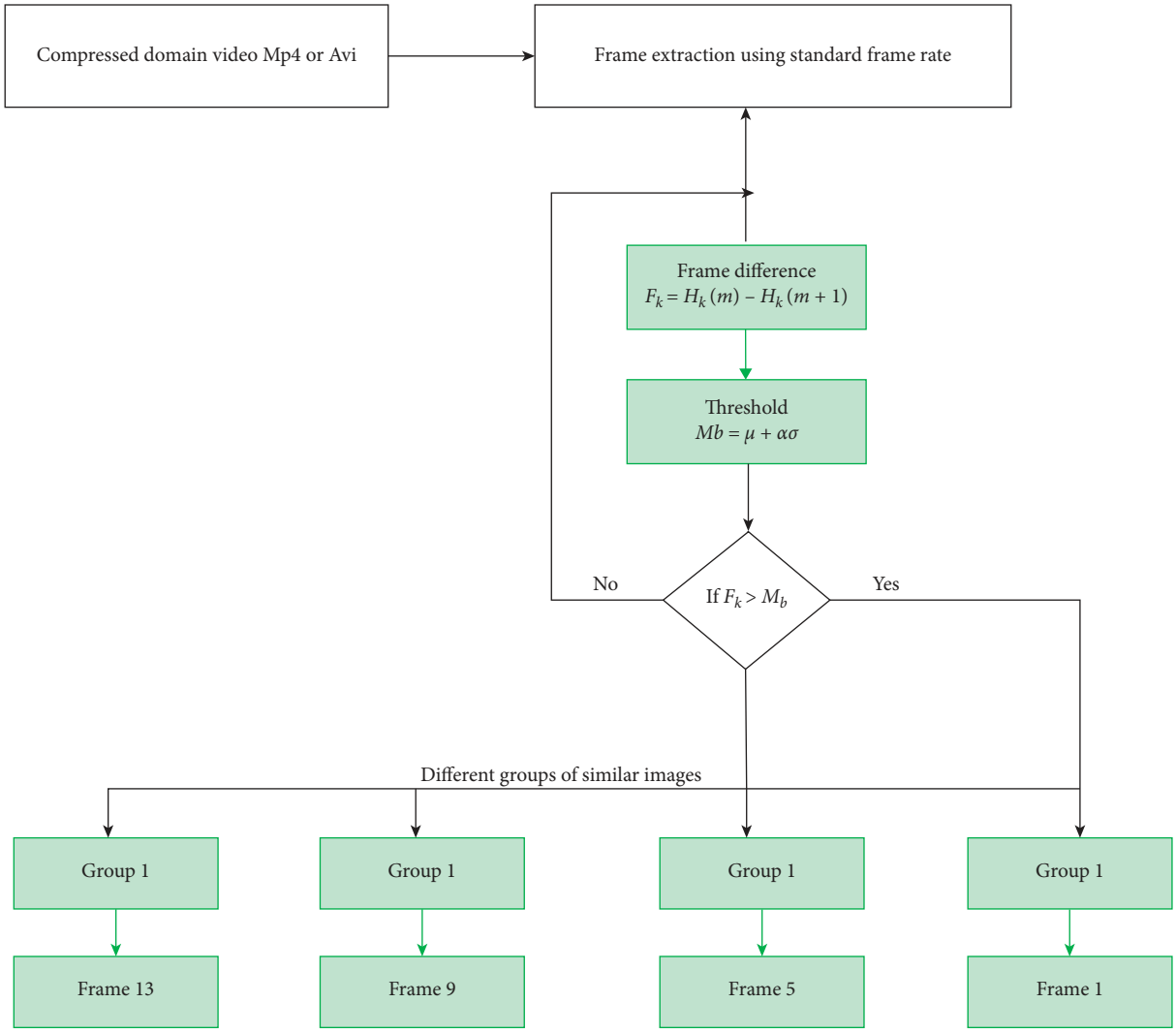


Figure 4: Selected frames to be watermarked from different groups.

Input: $T \longleftarrow$ No. of Frames, $\mathbf{K} \longleftarrow$ Mean(T), $\mathbf{S} \longleftarrow$ Std Deviation
$\mathbf{K_b} \longleftarrow K + \alpha S$
$\mathbf{FD_k} \longleftarrow$ Frame difference
Output-Selected T
(1) **for** $i \longleftarrow 1$ to T
(2) **Read** (T) and store in variables
(3) **Compute** the difference amongst frames and group them in different groups and store in FD_k.
(4) **if** ($FD_k > K_b$)
(5) **Select** and group them
(6) **Apply** random key amongst frames from different groups and write them to disk
(7) **End if**
(8) **Write** selected frames on disk
(9) **End for**
(10) **End**

Algorithm 1: Frame selection algorithm.

Input: Selected Frames
Output: Watermarked Video
Begin
(1) **for** selected frames from 1 to k
(2) **Input** binary image watermark (i, j).
(3) **Implement** layer separation on selected RGB frame $A(i, j)$ and watermarked image $W(i, j)$.
(4) **Encrypt** the watermark image $W(i, j)$.
(5) **Convert** selected frame into GBT Transform on each layer of $A(i, j)$.
(6) **Use** SVD Transform and extract S Feature of USV of $A(i, j)$ and $W(i, j)$.
(7) **Target** S value from both sides to be merged.
(8) **Embed** watermark $W(i, j)$ to $A(i, j)$ using value α as 0.02 using equation $WF'(i, j) = A(i, j) + \alpha W(i, j)$
(9) **Get** modified S value from both $A(i, j)$ and $W(i, j)$
(10) **Repeat** steps from 1 to 9 till all the selected frames are processed.
(11) **End for**
(12) **for** frames $1 : m$
(13) **Replace** watermarked frames with selected frames from the directory.
(14) **Use** same frame rate to combine all frames including watermarked and rest of extracted frames
(15) **End for**
(16) **End**

Algorithm 2: GBT-SVD-chaotic algorithm.

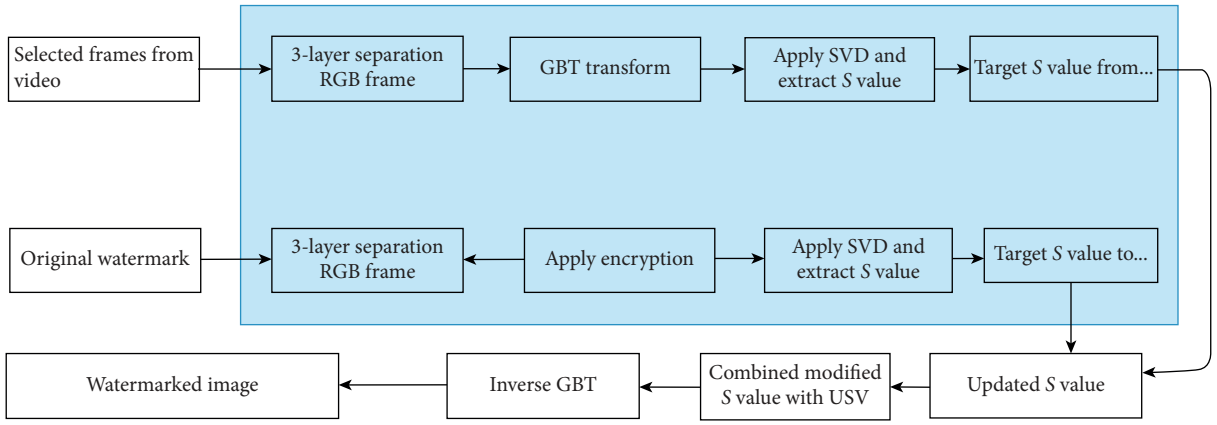


Figure 5: Watermark embedding procedure.

selected frame. It is calculated using the following equation:

$$\mathrm{NC} = \frac{\sum_{i=1}^{G}\sum_{j=1}^{H} A(i,j)E(i,j)}{\sum_{i=1}^{G}\sum_{j=1}^{H} E(i,j)^2}. \tag{24}$$

(c) Structural Similarity Index Measure (SSIM): this parameter is used to find structural similarity between watermarked frame and selected frame. It is calculated from the following equation:

$$\mathrm{SSIM}(m,n) = \frac{(2P_mP_n + \mathrm{c1})(2K_{mn} + c2)}{(P_m^2 + P_n^2 + c1)(K_m^2 + K_n^2 + c2)}, \tag{25}$$

where P_m and P_n represent average of m and n column; K_m and K_n represent variance of m and n; K_{mn} represents covariance of m and n and $c1$ and $c2$ are variables.

(d) Bit Error Rate (BER): this is the inverse of PSNR calculated in the following equation:

$$\mathrm{BER} = \frac{1}{\mathrm{PSNR}}. \tag{26}$$

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 of them are preferred and BER is inversely proportional to PSNR so lower values indicate the efficiency of technique.

4. Experimental Results

The results were evaluated in MATLAB 2019b using i5 processor. The frame selection time and embedding time are dependent on the type of processor used. The compiled results are dependent upon watermark embedding time and

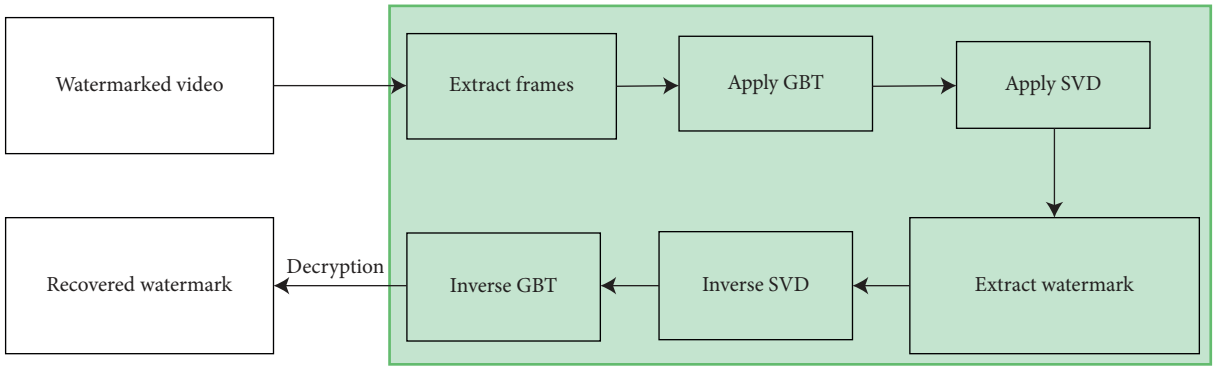


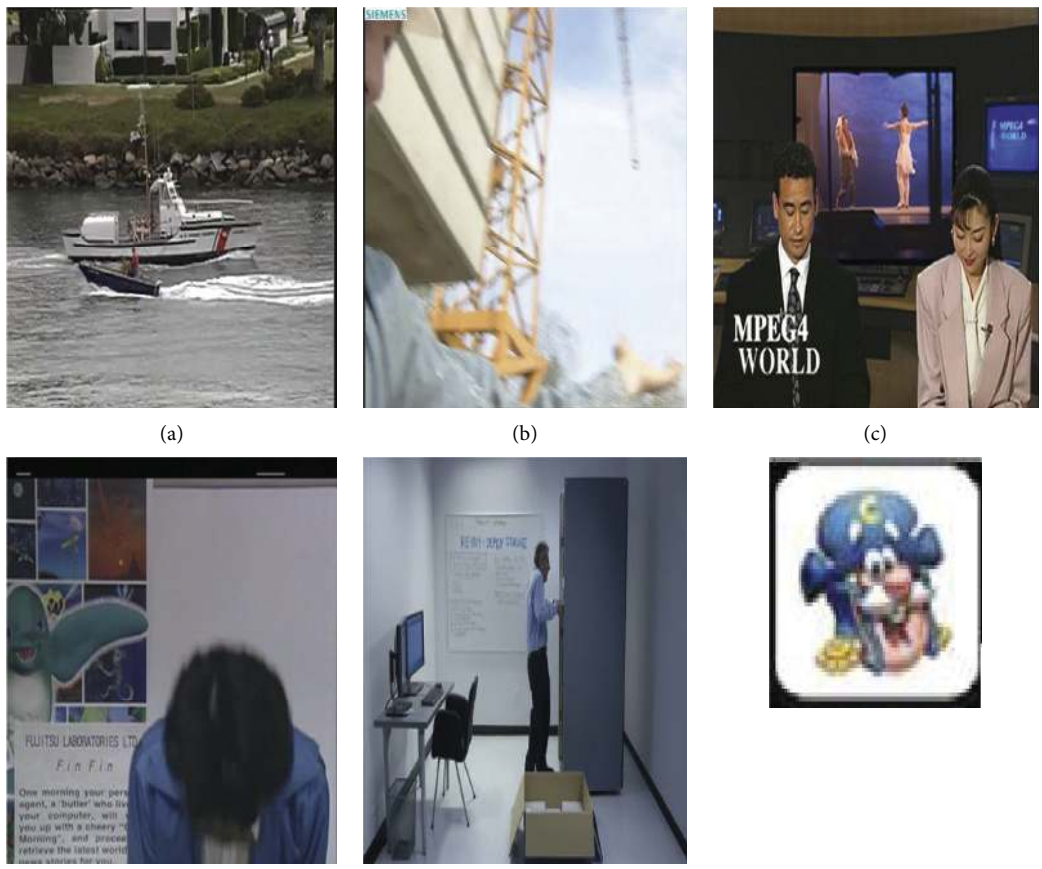
Figure 6: Watermark extraction procedure.

Input: Watermarked Video
Output-Recovered Watermark
Begin
(1) **Input** watermarked video
(2) **Apply** frame extraction mechanism using frame rate 29.97
(3) **for** frames from 1 to k
(4) **Implement** layer separation of watermarked frame
(5) **Convert** Watermarked frame into GBT Transform on each layer of $WF'(i, j)$.
(6) **Perform** extraction of USV feature of each layer of $WF'(i, j)$.
(7) **Extract** S value of watermarked frame.
(8) **Extract** watermark $W(i, j)$ from $WF'(i, j)$ using formula $W(i, j) = (WF'(i, j) - A(i, j))/\alpha$
(9) **Extract** S value of the watermark
(10) **Perform** inverse SVD to combine S value with USV of each layer.
(11) **Perform** inverse GBT Transform of watermark images
(12) **Apply** decryption mechanism to get extracted watermark
(13) **Repeat** Steps 4–12 to get extracted watermark.
(14) **End for**
(15) **End**

Algorithm 3: Watermark extraction algorithm.

frame selection time. A total of 6 Common Interchange Format (Cif) encoded videos have been taken and frame selection mechanism entirely depends upon number of scene changes in the video. Some videos have a greater number of scene changes; hence more frames will be selected. Akiyo did not have sufficient scene change detection so the watermarking technique could not be applied on that as the value of FD_k (frame difference) was not greater than K_b (threshold) so no significant frames were selected from the video; rest of the videos have significant frames selected as per frame selection algorithm.. The data sets of the videos were obtained from Figures 7(a)–7(e) which signifies some selected frames from the data set of videos. Along with these videos 2 binary watermarks and their encrypted versions have been shown; the compressed domain videos taken in the research are the same type of videos used in broadcast application; to remove unauthorized access to these videos, the given videos are embedded with encrypted watermark that addresses the issues faced by real time application. The encrypted watermark not only addresses security issues but also adds to copyright protection to achieve ownership identification. Higher values of PSNR and lower values of BER implicate the proposed technique to be efficient that leads to less loss in quality of output video. Every video will have different properties that mean frame selection in every video will be different. The same is demonstrated in this research where different videos have different number of frames getting selected.

4.1. Experimental Tests for Quality Check. The experimental results were divided into certain phases, starting with taking the input video in Avi or Mp4 file; this phase is followed by frame extraction. Frames are extracted in.png format as.jpeg is a compression format. Frames are extracted using a standard frame rate 29.97. The next phase is to embed the watermark by combining both S values of watermark and selected frames. The last phase is to check efficiency of the proposed technique by applying signal processing attacks on them which are taken in further section. The watermark embedding is done on selected frames depicted in Figures 7(a)–7(e); the videos are taken in compressed domain as uncompressed domain videos will take more time to process. The Cif format is known as Common Interchange



(a) (b) (c)

(d) (e) (f)

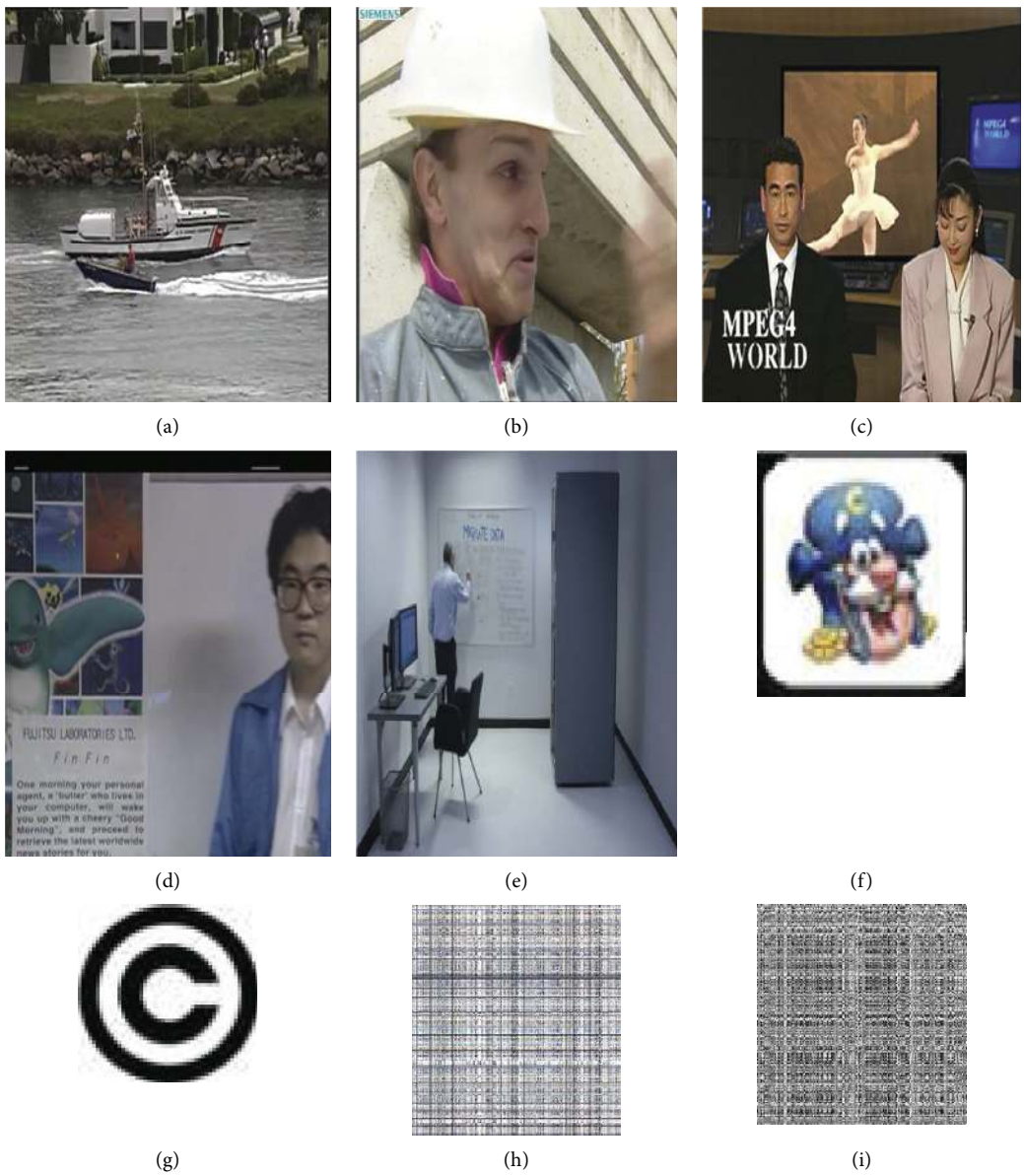
Figure 7: (a–e) Watermarked frames from the video; (f) selected binary watermark.

Format and it is referred to as a standardized format for picture resolution and the data has been obtained from website named https://media.xiph.org/video/derf/. Figures 8(a)–8(h) describe selected frames along with selected watermark. All videos are of the same resolution and selection of frame $I\ s$ done in real time. The videos are encoded to standardized MPEG-4 format using codec x264. The value of quality parameters is taken as per comparison with original and watermarked frames.

Table 2 represents the comparison of the input videos and the number of frames selected from the given videos. It was found that Pure Storage video has higher number of frames selected out of all videos. Table 3 represents the embedding of watermark 1 on selected frames without any attack. The performance of the proposed technique is calculated with various factors represented in Table 3. Figures 9(a)–9(d) describe the performance of embedding technique against no attacks applied to it.

4.2. Experimental Tests for Time Complexity. Table 4 compiles the processing time (in seconds) required to carry out frame selection, embedding time taken for the given set of videos. The time is entirely based on processor requirements. The total time consumed depends upon selection of frames from the video. Pure Storage video has got 5 frames selected and the time for every frame varies from 20 to 35 seconds for every frame. The value of embedding time is directly proportional to number of selected frames. Total of 5 frames were selected from Pure Storage video; thus, total embedding time is the highest for the same video. The watermark embedding factor is kept being 0.02 and GBT was followed by SVD on selected frames and mixed with S value of watermark. The proposed technique is fast and, as per processor requirements, works considerably at good speed. The plots in Figures 10(a) and 10(b) signify time taken for selection of frame from 5 videos. More number of changes in the video is directly proportional to the frame selection time and watermark embedding in selected frames for a single video is dependent upon number of frames selected. The plot in Figures 10(a) and 10(b) signifies the embedding time taken by selected frames from the video. Table 4 represents the total frame selection time and embedding time of the input videos.

4.3. Processing Attacks. The robustness of the proposed technique is tested against various attack scenarios such as Gaussian Noise, Sharpening, Rotation, Blurring, and JPEG Compression. A series of experiments have been conducted to attack every watermarked frame to measure quality loss. The robustness of the technique entirely depends upon the values of PSNR, SSIM, NC, and BER.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 8: (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 watermark 1, (g) original watermark 2, (h) encrypted watermark 1, and (i) encrypted watermark 2.

Table 2: Comparison of videos in terms of frame selection.

S. no.	Video name	Selected frames
1	Akiyo	0
2	Coastguard	1
3	Foreman	2
4	News	3
5	Bowing	4
6	Pure Storage	5

Table 3: Results after embedding of watermark 1 on selected frames.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	36.5062	0.99862	0.99987	0.027393
Foreman	36.6527	0.997625	0.999885	0.027284
News	36.6823	0.996863	0.99978	0.027261
Bowing	36.27048	0.99862	0.999955	0.027571
Pure Storage	36.32226	0.998002	0.999924	0.027531

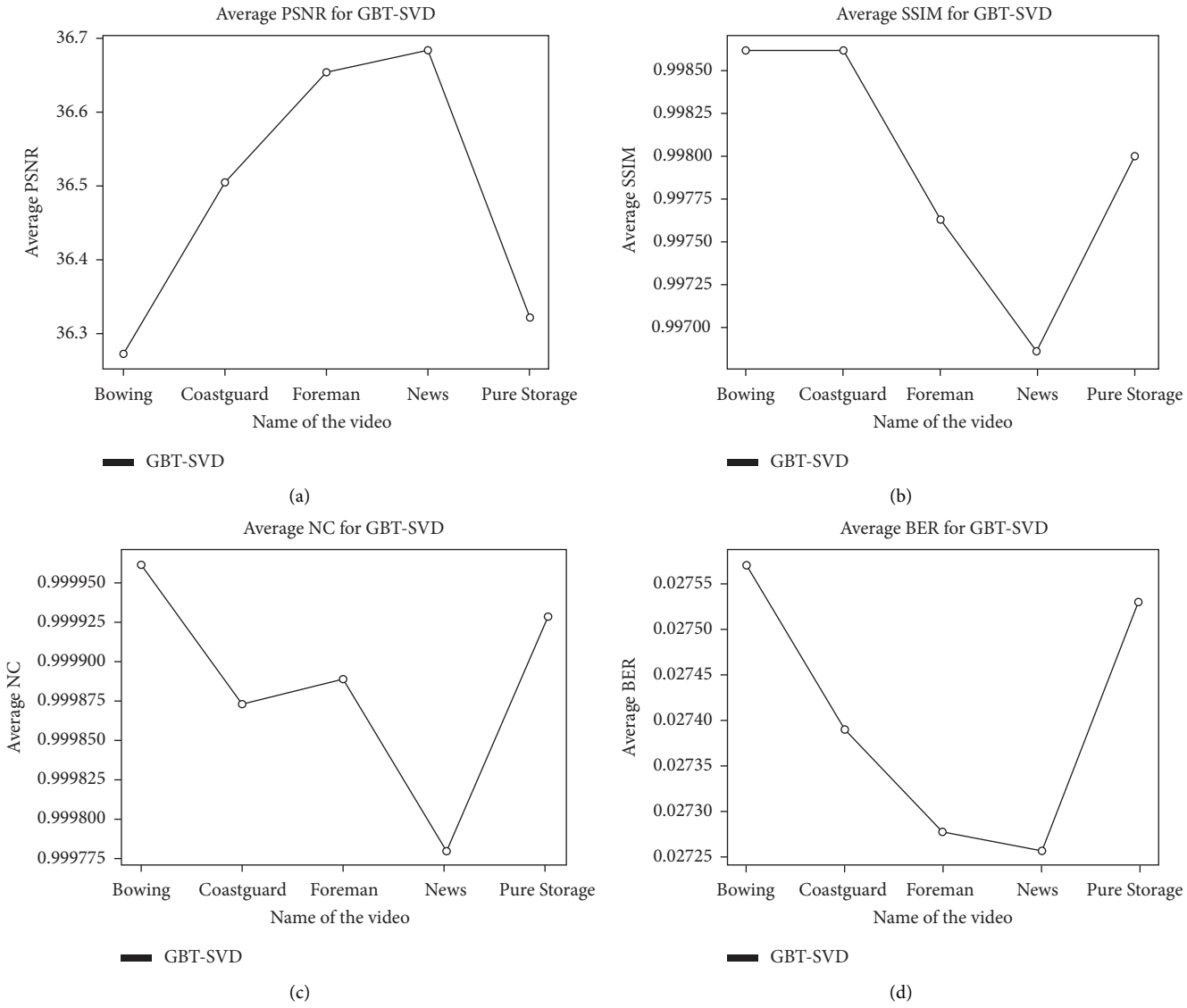


Figure 9: (a–d) Plot of PSNR, SSIM, NC, and BER w.r.t the videos taken in the proposed work for watermark 1 against no attack. (a) Average PSNR vs. no attack using watermark 1. (b) Average SSIM vs. no attack using watermark 1. (c) Average NC vs. no attack using watermark 1. (d) Average BER vs. no attack using watermark 1.

Table 4: Results of embedding time using watermark 1.

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

4.4. Gaussian Noise Attack. In Gaussian Noise attack, a random Gaussian sequence of real values {0.01} is added to all selected frames of the watermarked video using watermark 1. It can be seen from plots in Figures 11(a)–11(d) that average PSNR, NC, and SSIM decrease with increase in attack value and BER increases with increase in attack value. Figures 11(a)–11(d) compile real time testing by applying this attack of 0.01 Gaussian value; Table 5 represents results of quality parameters after Gaussian Noise attack.

4.4.1. Sharpening Attack. In Sharpening Attack, a random sequence real value {0.01} is added to all frames of the watermarked video using watermark 1. It can be seen from plots in Figures 12(a)–12(d) that average PSNR, NC, and SSIM decrease with increase in attack value and BER increases with increase in attack value. The Sharpening Attack is applied to highlight details of the image. Sharpening Attack is an attack that enhances changes in high and low frequencies of selected frames. More changes lead to more distortion in the image. It is applied

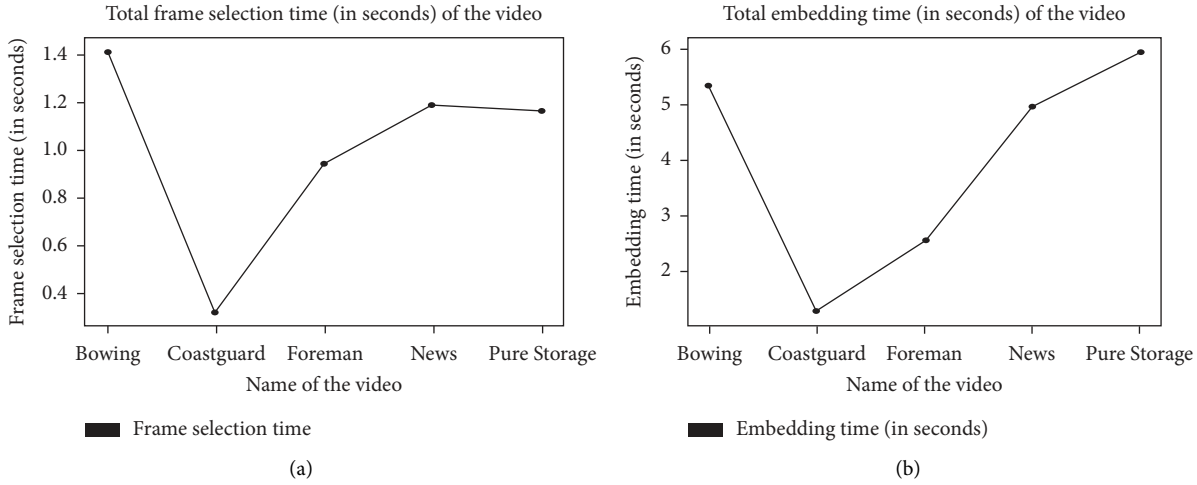


Figure 10: (a-b) Plot of total frame selection time and total embedding time (in seconds). (a) Total frame selection time (in seconds) for 5 videos. (b) Total embedding time (in seconds) for 5 videos.

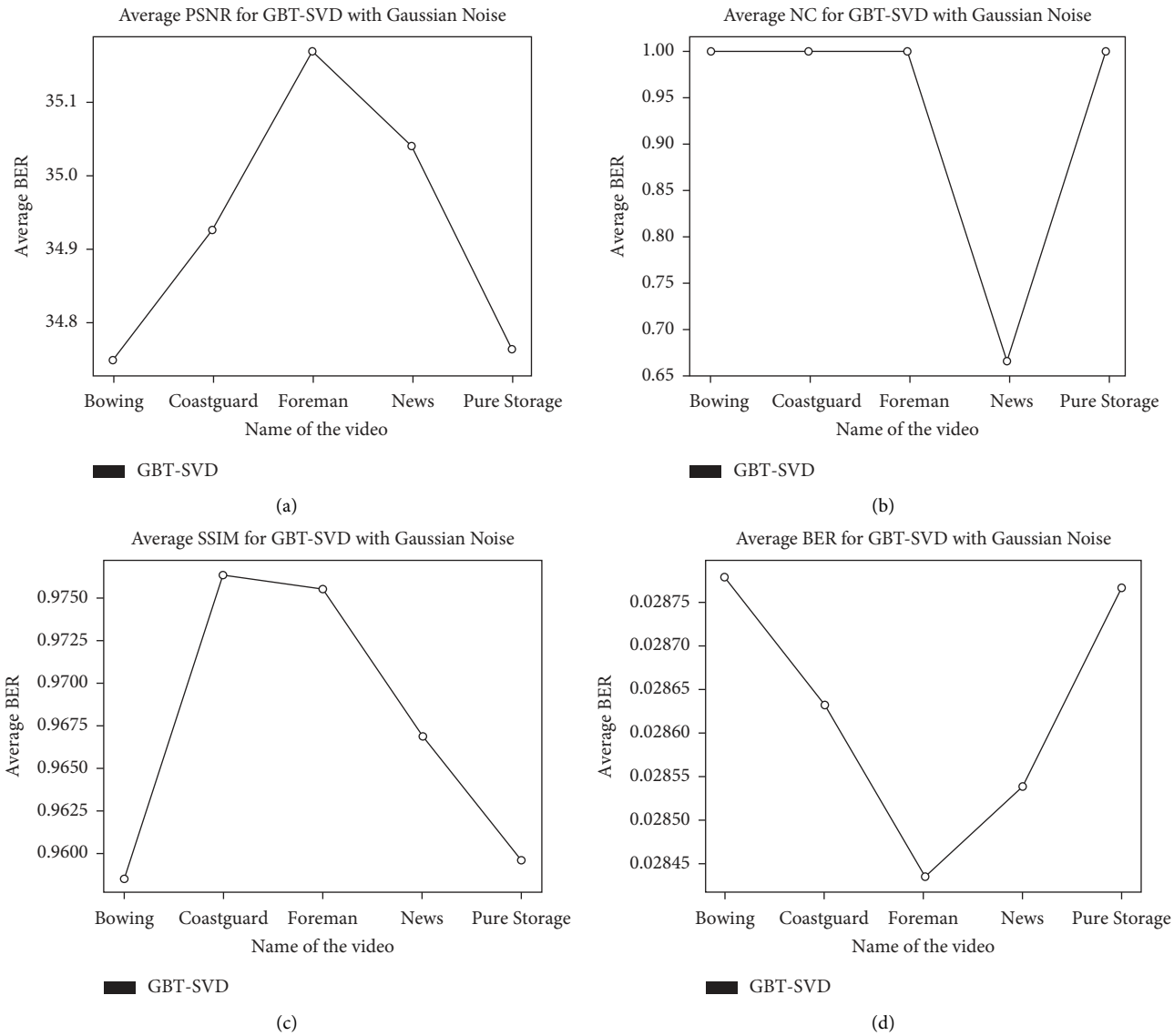


Figure 11: (a-d): Plot of PSNR, NC, SSIM, and BER w.r.t Gaussian Noise variance using watermark 1. (a) Average comparison of PSNR vs. Gaussian Noise variance. (b) Average comparison of NC vs. Gaussian Noise variance. (c) Average comparison of SSIM vs. Gaussian Noise variance. (d) Average comparison of BER vs. Gaussian Noise variance.

Table 5: Results after applying Gaussian Noise attack on watermarked frames using watermark 1 using value 0.01.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	34.9263	0.9763	0.99895	0.028632
Foreman	35.1684	0.97538	0.998965	0.028435
News	35.04007	0.966793	0.998997	0.028539
Bowing	34.74843	0.958563	0.998855	0.028778
Pure Storage	34.76392	0.959552	0.998698	0.028766

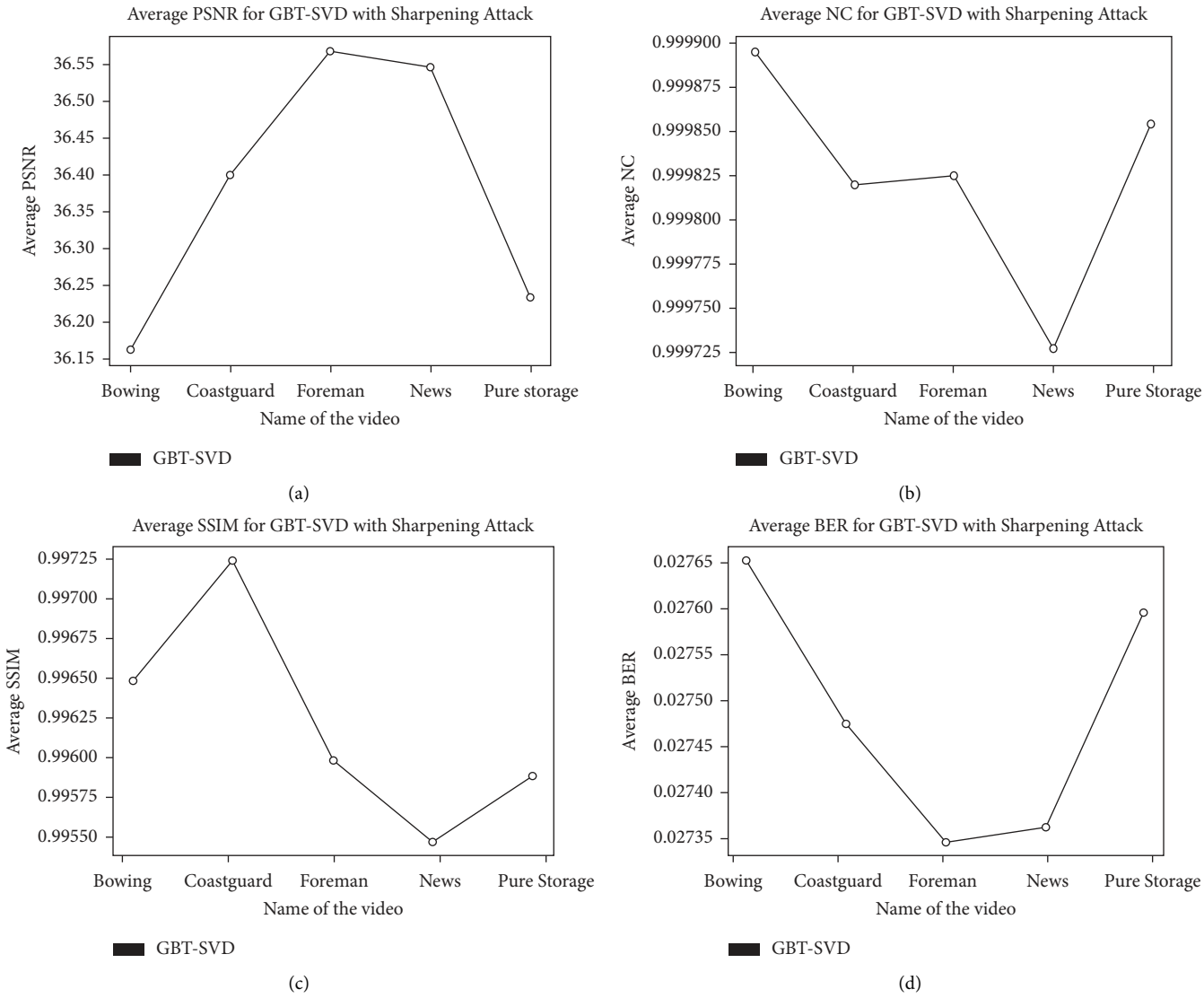


Figure 12: (a-d) Plot of PSNR, NC, SSIM, and BER w.r.t Sharpening Attack using watermark 1. (a) Average comparison of PSNR vs. Sharpening Attack variance. (b) Average comparison of NC vs. Sharpening Attack variance. (c) Average comparison of SSIM vs. Sharpening Attack variance. (d) Average comparison of BER vs. Sharpening Attack variance.

to low and high frequency bands of the image. In our research, this attack is applied to find out difference in watermarked frames with this attack and without it. The results of quality parameters after Sharpening Attack are represented in Table 6.

4.4.2. Rotation Attack. In Rotation attack, a watermarked frame is rotated with an angle of 90 using watermark 1. Higher value of Rotation attack will affect PSNR of the watermarked frame. The quality metrics of Rotation attack is affected by the higher angle in which the frame is rotated. It can be seen from plots in Figures 13(a)–13(d) that average PSNR, NC, and SSIM deteriorate with increase in attack value and BER increases with increase in attack value. The Rotation attack is carried out by rotating the watermarked frame and normal selected frame. The technique is vulnerable against Rotation attack as it does not achieve good results in that attack. The addition of optimization algorithm

Table 6: Results after applying Sharpening Attack.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	36.3996	0.99724	0.99982	0.027473
Foreman	36.56795	0.99597	0.999825	0.027347
News	36.5464	0.995467	0.999727	0.027362
Bowing	36.163	0.996473	0.999895	0.027653
Pure Storage	36.2352	0.995882	0.999854	0.027597

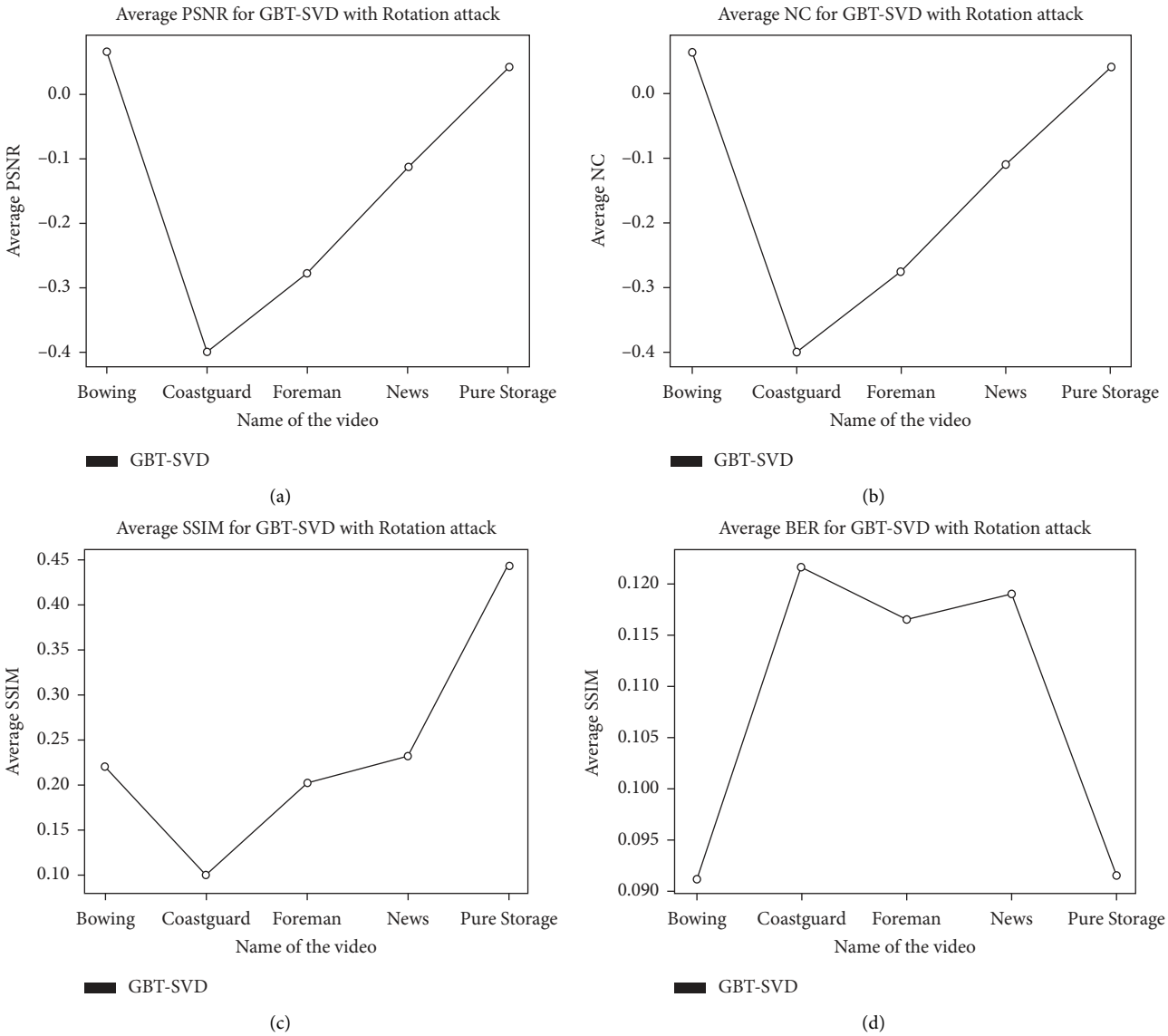


Figure 13: (a-d) Plot of PSNR, NC, SSIM, and BER against Rotation attack using watermark 1. (a) Average comparison of PSNR vs. Rotation attack variance. (b) Average comparison of NC vs. Rotation attack variance. (c) Average comparison of SSIM vs. Rotation attack variance. (d) Average comparison of BER vs. Rotation attack variance.

to find best fitness function can improve the values of quality metrics against this attack. Table 7 represents results of quality parameters after applying Rotation attack.

4.4.3. Blurring Attack. In Blurring attack, a random sequence of real values {2.05} is added to all frames of the watermarked video using watermark 1. The Blurring attack is caused by motion of an object. The more the object is moved, the lower the value of PSNR will be. It can be seen from plots in Figures 14(a)–14(d) that average PSNR, NC, and SSIM decrease with increase in attack value and BER increases with increase in attack value. In the research, we applied Blurring attack to check the motion of watermarked frame. Higher values of PSNR will indicate effectiveness of the technique. Table 8 represents results of quality parameters after applying Blurring attack.

Table 7: Results after applying Rotation attack on watermarked frames using watermark 1 using value 90.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	8.2061	0.097794	−0.39927	0.12186
Foreman	8.593	0.201262	−0.27613	0.116745
News	8.404067	0.23115	−0.1115	0.118997
Bowing	10.98838	0.220308	0.066108	0.091297
Pure Storage	11.00918	0.44313	0.041094	0.091474

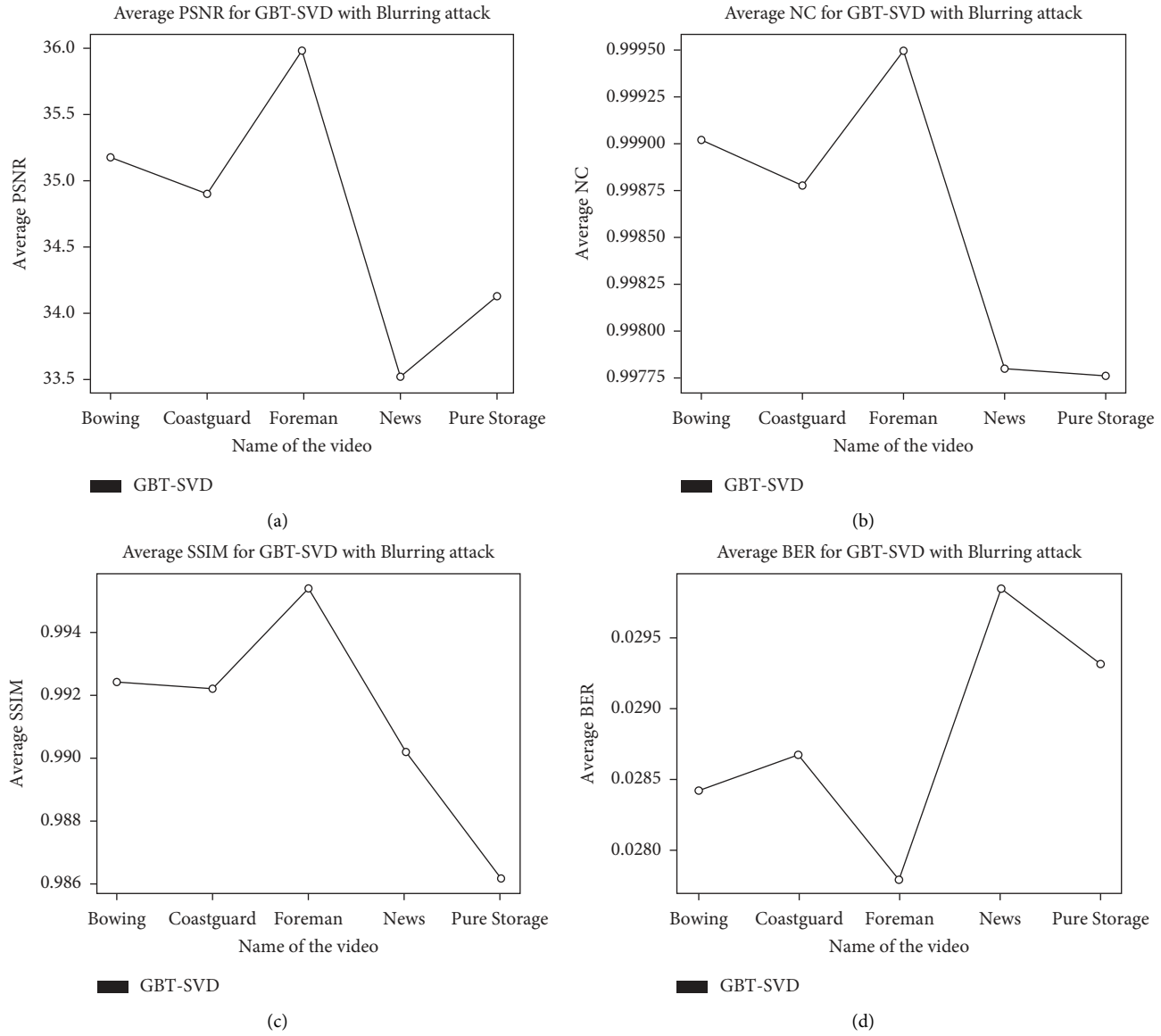


Figure 14: (a-d) Plot of PSNR, NC, SSIM, and BER w.r.t Blurring attack variance using watermark 1. (a) Average comparison of PSNR vs. Blurring attack variance. (b) Average comparison of NC vs. Blurring attack variance. (c) Average comparison of SSIM vs. Blurring attack variance. (d) Average comparison of BER vs. Blurring attack variance.

4.4.4. JPEG Compression Attack. In JPEG Compression attack, value {98} is taken and applied to all frames of watermarked video. JPEG Compression number decides how much compression attacks can be applied. JPEG Compression application on watermarked frame indicates no significant change. It can be seen from plots in Figures 15(a)–15(d) that average PSNR, NC, and SSIM decrease with decrease in value of compression attack value and BER increases with decrease in attack value. Table 9 represents results of quality parameters after applying JPEG Compression attack.

Table 8: Results after applying Blurring attack on watermarked frames using watermark 1 using value 2.05.

Video	PSNR (db)	SSIM	NC	BER
Coastguard	34.8924	0.99216	0.99878	0.02866
Foreman	35.9857	0.995365	0.9995	0.027789
News	33.5081	0.990213	0.997803	0.029844
Bowing	35.17803	0.992393	0.999025	0.028427
Pure Storage	34.1216	0.986148	0.997758	0.029309

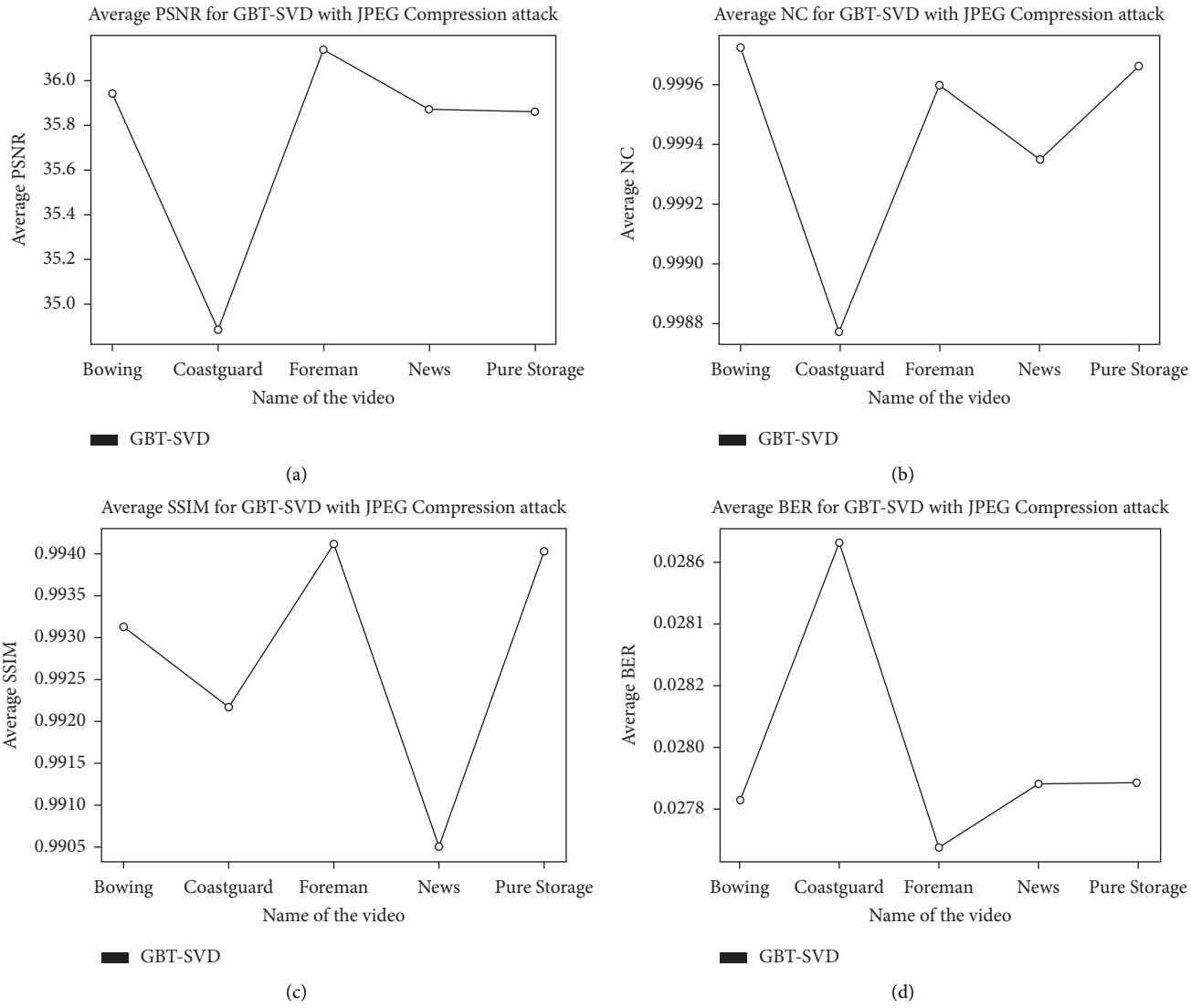


Figure 15: (a-d): Plot of PSNR, NC, SSIM, and BER w.r.t JPEG Compression attack variance using watermark 1. (a) Average comparison of PSNR vs. JPEG Compression attack variance. (b) Average comparison of NC vs. JPEG Compression attack variance. (c) Average comparison of SSIM vs. JPEG Compression attack variance. (d) Average comparison of BER vs. JPEG Compression attack variance.

Table 9: Results after JPEG attack (98 value).

Video	PSNR (db)	SSIM	NC	BER
Coastguard	34.8924	0.99216	0.99878	0.02866
Foreman	36.13615	0.99411	0.9996	0.027675
News	35.8682	0.9905	0.999357	0.02788
Bowing	35.93805	0.993125	0.999728	0.027826
Pure Storage	35.86234	0.99403	0.999662	0.027885

5. Conclusion and Future Work

We proposed a novel frame selection based watermarking technique (GBT-SVD-hyperchaotic) to address quality loss of data. Frame selection algorithm is proposed to select appropriate number of frames as addition of watermark in every frame leads to time complexity of the embedding algorithm. Frame selection is done on the basis of number of scene changes done in the video. The hybrid combination of Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption provides efficient results for watermark embedding. The proposed technique was found to be robust against many signal processing attacks, Gaussian Noise, Sharpening Attack, Rotation, Blurring, and JPEG Compression. The additional security mechanism applied in the proposed work gives added advantage over transpositional ciphers in related work. The proposed technique is fast; however, it faces the limitation of absence of optimized algorithms. The performance of the proposed technique can be improved by applying optimization algorithms like Grey Wolf Optimization that will optimize the embedding factor, thus targeting high values of PSNR.

Data Availability

The data are open and available on request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] Z. Cao and L. Wang, "A secure video watermarking technique based on hyperchaotic Lorentz system," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26089–26109, 2019.

[2] S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A survey on different video watermarking techniques and comparative analysis with reference to H. 264/AVC,"in Proceedings of the 2006 IEEE International Symposium on Consumer Electronics, St. Petersburg, Russia, pp. 1–6, 2006.

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

[4] G.-B. Huang and L. Chen, "Convex incremental extreme learning machine," *Neurocomputing*, vol. 70, no. 16–18, pp. 3056–3062, 2007.

[5] F. Tao, D. Zhao, Y. Hu, and Z. Zhou, "Resource service composition and its optimal-selection based on particle swarm optimization in manufacturing grid system," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 4, pp. 315–327, 2008.

[6] X. Wang and M. Wang, "A hyperchaos generated from Lorenz system," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 14, pp. 3751–3758, 2008.

[7] A. Al-Haj and A. Abu-Errub, "Performance optimization of discrete wavelets transform based image watermarking using genetic algorithms," journal of Computer Science, vol. 4, no. 10, pp. 834–841, 2008.

[8] C. H. Wu, Y. Zheng, W. H. Ip, C. Y. Chan, K. L. Yung, and Z. M. 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, pp. 27–36, 2011.

[9] G. Cheung, W. Kim, A. Ortega, J. Ishida, and A. Kubota, "Depth map coding using graph based transform and transform domain sparsification," in Proceedings of the 2011 IEEE 13th International Workshop on Multimedia Signal Processing, Hangzhou, China, October, 2011.

[10] T. Tabassum and S. M. M. Islam, "A digital video watermarking technique based on identical frame extraction in 3-Level DWT," in Proceedings of the 2012 15th International Conference on Computer and Information Technology (ICCIT), pp. 101–106, Chittagong, Bangladesh, 2012.

[11] M. Masoumi and S. Amiri, "A blind scene-based watermarking for video copyright protection," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 6, pp. 528–535, 2013.

[12] R. Rewani, M. Kumar, and A. Pundir, "Digital image watermarking: a survey," *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 4, pp. 1750–1753, 2013.

[13] 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, pp. 189–196, 2013.

[14] M. Kumar and R. Rewani, "Digital image watermarking using fractional fourier transform via image compression," in Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1–4, Enathi, India, 2013.

[15] P. Venugopala, H. Sarojadevi, N. Chiplunkar, and V. Bhat, "Video watermarking by adjusting the pixel values and using scene change detection," in Proceedings of the 2014 Fifth International Conference on Signal and Image Processing (ICSIP), pp. 259–264, Bangalore, India, 2014.

[16] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey Wolf optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014.

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

[18] B. Sridhar and C. Arun, "An enhanced approach in video watermarking with multiple watermarks using wavelet," *Journal of Communications Technology and Electronics*, vol. 61, no. 2, pp. 165–175, 2016.

[19] J. Hou, H. Liu, and L. Chau, "Graph-based transform for data decorrelation," in proceedings of the 2016 IEEE International Conference on Digital Signal Processing (DSP), pp. 177–180, Beijing, China, 2016.

[20] D. Kaur and S. Jindal, "A Semi Blind-DWT-SVD Video Watermarking," *Procedia Computer Science*, vol. 46, pp. 1661–1667, 2015.

[21] I. Daribo, D. Florencio, and G. Cheung, "Arbitrarily shaped motion prediction for depth video compression using arithmetic edge coding," *IEEE Transactions on Image Processing*, vol. 23, no. 11, pp. 4696–4708, 2014.

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

[23] C. Sharma, G. Singh, and G. Singh, "Efficient video watermarking technique for quality loss of data," *Indian Journal of Science and Technology*, vol. 2016, 2016.

[24] W. Wang, HY. Tan, P. Sun, Y. Pang, and B. B. Ren, "A Novel Digital Image Encryption Algorithm Based on Wavelet

Transform and Multi-Chaos," *Wireless Communication and Sensor Network*, vol. 2016, 2016.

[25] F. Seghir and A. Khababa, "A hybrid approach using genetic and fruit fly optimization algorithms for QoS-aware cloud service composition," *Journal of Intelligent Manufacturing*, vol. 2016, 2016.

[26] A. Sake and R. Tirumala, "Bi-orthogonal wavelet transform based video watermarking using optimization techniques," *Materials Today: Proceedings*, vol. 5, no. 1, pp. 1470–1477, 2018.

[27] A. Mansouri, A. Aznaveh, and F. Azar, "Blind H.264 compressed video watermarking with pattern consideration," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Texas, MA, USA, 2010.

[28] C. Sharma and A. Bagga, "Video Watermarking Scheme Based on DWT, SVD, Rail Fence for Quality Loss of Data," in Proceedings of the 2018 4th International Conference on Computing Sciences (ICCS), pp. 84–87, Jalandhar, India, 2018.

[29] A. Rajpal, A. Mishra, and R. Bala, "A novel Fuzzy selection based watermarking scheme for MPEG-4 videos using Bi-directional extreme learning machine," *Applied Soft Computing Journal*, vol. 2018, 2018.

[30] W. Wang, M. Si, Y. Pang et al., "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.

[31] M. Shabaz and C. Garg, "Clustering Yelp's sentiment data through various approaches and estimating the error rate," *Materials Today: Proceedings*, 2020.

[32] M. Kaur, D. Singh, and R. S. Uppal, "Parallel strength Pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2019.

[33] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[34] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[35] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Applied Cryptography and Noise Resistant Data Security*, vol. 1-20, 2018.

[36] H. Santoyo-Garcia, E. Fragoso-Navarro, R. Reyes-Reyes, C. Cruz-Ramos, and M. Nakano-Miyatake, "Visible watermarking technique based on human visual system for single sensor digital cameras," *Security and Communication Networks*, vol. 1–20, 2017.

[37] M. Fateh, M. Rezvani, and Y. Irani, "A new method of coding for steganography based on LSB matching revisited," *Security and Communication Networks*, vol. 1–15, 2021.

[38] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Security and Communication Networks*, vol. 1–15, 2021.

[39] S. Qin, S. Tan, F. Zhou, J. Xu, and Z. Zhang, "A verifiable steganography-based secret image sharing scheme in 5G networks," *Security and Communication Networks*, vol. 1–14, 2021.