Stable High Capacity Video Steganography in Wavelet Domain

[1]Urmila Pilania, [2*]Rohit Tanwar, [3]Prinima Gupta

[1]Research Scholar, Department of Computer Science & Technology, Manav Rachna University, Faridabad, Haryana, India.
urmila@mru.edu.in

[2]Assistant Professor, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India.
r.tanwar@ddn.upes.ac.in (ORCID: 0000-0002-9087-6019)
*Corresponding Author

[3]Associate Professor, Department of Computer Science & Technology, Manav Rachna University, Faridabad, Haryana, India.
prinima@mru.edu.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: Video Steganography provides a secure way of communication by embedding the secret message inside video frames. Supported by a real-time environment, a significant growth in choosing video as a cover file has been noticed in the last decade. Large concealing capacity, more robustness to attacks, and indistinguishability of cover video and stego video are of major concern for any video steganography technique. In this paper, a novel technique has been proposed to achieve the above-mentioned objectives. Implementation of video steganography in the transform domain inherently contributes to improved robustness. We have embedded an image inside a chosen video file using the Lifting Scheme based on the Haar Wavelet Transform. To achieve increased concealing capacity, the Singular Value Decomposition technique has been applied before the actual embedding task. The proposed work is implemented using the MATLAB environment. The suggested method is then tested and analyzed for its robustness, capacity, and imperceptibility. It is concluded that proposed technique is robust against general video processing attacks, like low-pass filtering, scaling, rotation, transformation, and histogram equalization attacks. Additionally, the values for Peak Signal to Noise Ratio, Mean Square Error, Structure Similarity Index Matrix, and Correlation Coefficients were calculated and analyzed as a performance measure of the method.

Keywords: Video steganography, singular value decomposition, lifting scheme, haar wavelet transform, low-pass filtering and histogram equalization.

1. Introduction

In the world of information technology, the data is generated as well as communicated from one point to another at a faster rate. As a counterpart of the advancement in communication technology, the transfer of multimedia information is susceptible to many attacks, like Man-in-Middle attack, Impersonation, Phishing, etc.. The preferred approach to protect the secret information while traveling through the public channel is to hide its presence. Steganography is a technique of facilitating secret communication in a way that third party, except the host and receiver, knows that there exists some secret information inside the transmitted media. The media used to conceal the secret information is known as a cover file. Depending upon the type of cover file chosen for embedding, steganography is divided into various categories like Text steganography, Audio steganography, Image steganography, Video steganography, etc. Due to the large size and real-time availability, video steganography is gaining popularity to transmit secret information (Mudusu et al., 2018). The video steganography process is described in Figure 1.

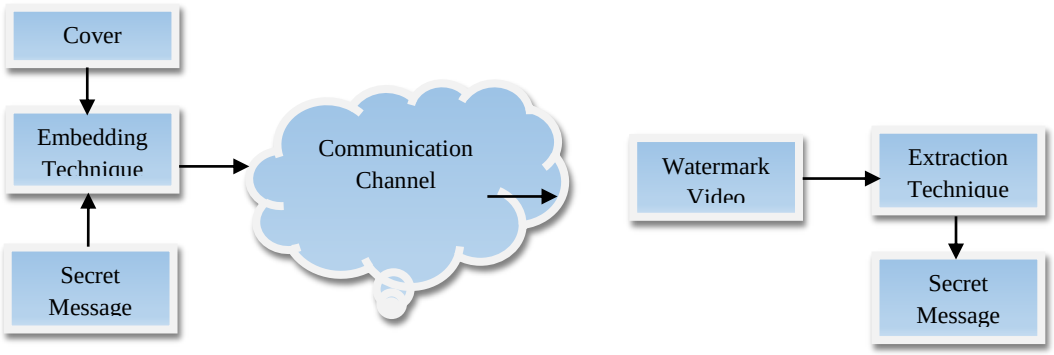


Figure 1. Video Steganography Process

Another categorization of steganography is based on the domain; (i) Spatial Domain and (ii) Transform domain. The spatial domain substitutes secret information directly on the least significant bits of the cover file. Embedding as well as extraction of secret information is simple in this domain. It has less complexity, high embedding capacity, and less robustness to intentional and unintentional attacks. During embedding of secret information, it adds distortion in the cover file that directly affects statistical properties of the cover file. Whereas, the transform domain deals with the rate of pixel change. It embeds secret information in the region that is less exposed to cropping, compression, scaling, and image processing (Raftari & Moghadam, 2012). These techniques can handle different file formats. Transform domain techniques, like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), and Haar Wavelet Transform are very complex and yields great robustness at a cost of embedding capacity. Thus, the objective to get high robustness motivates the researchers to work in the transform domain. Less computation time and more robustness favored the use of the Lifting Scheme (LS) based on Haar Wavelet Transform. Singular Value Decomposition (SVD) technique provides required compression thereby contributing to improved embedding capacity.

The paper is organized into various sections. Section-II describes the related work done in the field of video and image steganography in various domains with varying attempts by the researchers to achieve the required objectives. Based on the observations from the literature reviewed, a problem is identified and formulated in Section-III. In Section-IV, a methodology is proposed to resolve the stated problem and describe proposed algorithms for embedding as well as the extraction process. Section-V describes the implementation background and discussion of the results obtained. The work is concluded and the scope for future work is stated in Section-VI.

2. Litrature Survey

Different researchers worked on the related problems to hide a message with a video or image. In this section, the relevant literature of the past *20* years is studied and described.

The author of (Banik & Banik, 2020) paper, reviewed many video steganography techniques categorized in different domains. After discussing various techniques of different domains their imperceptibility, robustness against image processing attacks, embedding capacity, video pre-processing, and secret information pre-processing were analyzed. Along with that advantages and disadvantages of every steganography technique were mentioned. The author has provided recommendations and future research trends for the steganography techniques also. However, in this work the researchers proposed Red Green Blue (RGB) intensity-based steganography technique for embedding secret information. In order to enhance the embedding capacity, four LSBs of carrier file were used to embed the secret bits. The resulted technique had more embedding capacity and security than the existing '*2*' LSB techniques. This technique also overcame the problem of sequential manner embedding. The image pixels suitable for embedding were selected using a stego key. Moving ahead the researchers in (R. K. Singh & Shaw, 2018) combined dual watermarking with cryptography technique to provide a higher security level. LSB and DCT techniques were used for embedding the secret information. The watermark image was converted to QR Code by applying encryption. In this way, the robustness of the proposed technique got increased. The technique not only offered dual level security to secret information but the authentication of original information also.

DWT finds it's one of the prime applications in Digital Signal Processing (DSP). Lifting Scheme (LS) was introduced in (Joshi et al., 2015) the work in three-parent wavelets that are Haar wavelet, Daubechies and Cohen-Daubechies-Feauveau wavelet. Haar wavelet was applied to project the elementary architecture of DWT. Daubechies filters and Cohen-Daubechies-Feauveau bi-orthogonal wavelet filters were also deliberated for DWT construction. Later on, the comparison of the basic architecture of DWT with this constructed architecture concluded that the lifting scheme is capable to provide less power consumption because of its simple architecture. Extending the concept further, the researchers in (S. Singh et al., 2016) proposed an image steganography technique using Singular Value Decomposition (SVD) and IWT that used chaotic sequence for clambering logo. The proposed technique improved robustness against various image processing attacks such as cropping, scaling, rotation, gaussian, filtering, noise, etc. Results of the proposed technique were compared to

DCT and Reversible Discrete Wavelet Transform (RDWT) based techniques. Experimental results showed the good visual quality of the output file, more robustness, and high embedding capacity.

Utilizing the inherent benefits of IWT, the author presented (Xuan, Zhu, et al., 2002) an optimal distortion less image steganography technique. IWT is capable of converting a watermark image into an original image without distortion. The proposed techniques embedded secret information into middle multiple bit-planes of IWT componenets of medium and high-frequency sub-bands. The proposed technique was capable to hide a large amount of secret message as compared to the existing distortion-less steganography techniques. It also provided a better level of imperceptibility compared to existing techniques. The author also used an image histogram for avoiding the probable overflow of greyscales. Similarly, in this work (Muhuri et al., 2020) a steganography technique was proposed that embed secret information in integer wavelet coefficients of the image. Author combined steganography with an optimum pixel adjustment process for enhancing the embedding capacity of the proposed technique compared to existing techniques. A secret key was used for the selection of random bits that provided additional security to the proposed system. The error difference was also reduced among original integer wavelet coefficient values and revised values by using an optimum pixel adjustment process. Extending the concept the author (Gupta & Parmar, 2017) proposed a hybrid IWT-SVD technique. The results were compared with similar other techniques to validate the performance of the planned one. The proposed technique was a consequent motivation from the challenges associated with steganography techniques i.e. robustness, embedding capacity, and imperceptibility. The results showed that the excellence of the stego image and the retrieved image are reliant on the scaling factor. The proposed technique had a good value of Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NCC) equated to the standing DWT-SVD techniques. Moreover, the NCC values of the proposed work vary at different scaling factors. The work (Thanikaiselvan & Arulmozhivarman, 2013) attained large embedding capacity, high imperceptibility, and robustness measured in terms of PSNR, Mean Square Error (MSE), and Steganalysis. High imperceptibility was verified through a good PSNR value. Robustness was attained by hiding secret bits randomly in cover file. Additionally, the authors used reversible integer Haar wavelet transform for randomly embedding of secret information in R, G, and B planes separately. Graph theory was used for selecting random bits coefficients. Three secret keys were used; one for the embedding of secret information, the second for extraction of secret information, and the third for selection of random coefficients respectively. Experimental results showed that what was claimed as large embedding capacity, high imperceptibility, and robustness against attacks has been achieved as well.

On the other hand, researchers in their work (Kakde et al., 2015) suggested the usage of integer wavelet as a decorrelation phase for optimal context-based lossless audio encoding. First of all, the unique wideband audio signals were divided into wavelet subbands. After that, the integer-valued coefficients were obtained that could be transmitted by applying the optimal context-based lossless audio encoding technique. On the other side, an equally capable decoder was used to rebuild and efficiently restore the audio waveform. Additionally, many methods of encoding the integer wavelet coefficients and compared results with those gained in full band context optimal encoding. Steganography is the process of embedding secret bits inside the carrier file were explored. In this paper (Churin et al., 2013), video steganography technique was proposed hiding secretmessage in a video file. For embedding secret image the intensity features composed with lifting based multi-level wavelet transform was applied. Initially, the secret message and carrier video file were transformed by applying lifting based multi-level wavelet transform. After that locations having the same values in the secret image and cover video were calculated. These locations were used to embed the secret image. The proposed technique was found to have a good PSNR value as equated to the existing techniques.

The author in their work (Bruno Razafindradina & Mohamed Karim, 2013) proposed an optimized robust watermarking method using edge insertion. The proposed technique was robust against different attacks except for rotation. Rotation greater than *0.25* angle resulted in the detection of embedded secret information. Specifically, the proposed technique provided better robustness against Joint Photographic Experts Group (JPEG) compression. However, the robustness can be enhanced by adjusting block H, but it impacted the visual quality of the output file accordingly. Similarly, hiding capacity can be improved by deleting rows to half, but in this case, robustness will get decreased. In other work (Cheddad et al., 2009), the author proposed image steganography to hide secret information in the skin portion of the image. The initial task was to find the skin

portion in a color space generating a skin model then process these portions for embedding the secret information. Almost all the existing techniques of image detection have a challenge of decorrelation of luminance. Some of these techniques conclude that luminance can be ignored as it is the least contributing color element to skin color detection. The proposed technique overcame the above-mentioned challenges by proving that luminance is valuable in the detection of skin and non-skin portions. It was found that embedding of secret information in the selected skin portion was robust against image processing attacks.

3. Problem Forumation Bachground

After the literature survey, it has been found that maintaining a proper balance of imperceptibility, robustness, visual quality of watermark, and embedding capacity are some of the major challenges of steganography techniques. If the system tries to embed large amounts of secret data then it affects the statistical properties of the cover file leading to suspicion by the third party. If the system tries to increase robustness against various attacks then embedding capacity gets comprised and the method becomes more complex with high computational requirements.

3.1 Problem Statement

The problem statement is to develop a video steganography technique that embeds a large amount of image data while maintaining robustness along with the good visual quality of the watermark with limited computational requirements.

Steganography in the wavelet domain inherently provides high robustness along with the good visual quality of watermark but that comes at the cost of reduced capacity and more computational needs. In the below sections, the Lifting scheme based Haar wavelet transform has been explored along with SVD to rationalize their suitability in resolving the above-mentioned problem statement.

3.2. Lifting Scheme based Haar Wavelet Transform

Wim Sweldens innovated Lifting Scheme for building bi-orthogonal wavelets. It is the simplest and well-organized technique to compute the wavelet transform. LS is independent as compared to Fourier Transform and capable to realize reversible integer wavelet transform. In the wavelet transform, two sorts of coefficients are acquired; scaling and wavelet. Scaling coefficients can be picked up by aggregating two nearest samples whereas scaling coefficients speak to a coarse estimation of discourse flag and captures information at different frequencies (Joshi et al., 2015). Wavelet coefficients can be obtained by the subtraction of two adjacent samples and then these subtracted results are divided by '*2*'. Haar coefficients have all details of the speech signal and capture information at different locations (Li et al., 2018). The commands used for the implementation of the lifting scheme in MATLAB are mentioned in Figure 2. The lifting scheme is explained in (Roy & Pal, 2019) and the RGB colour model is explained in (Sanjida. (nd). Digital Image Processing tutorial-3, n.d.).

[CA, CH, CV, CD]=IWT(X, Wname); // CA computes the approximation coefficients of image, and details coefficients of image are: CH gives horizontal, CV vertical, CD diagonal details of given image, obtained by a wavelet decomposition of input image X. 'Wname' is a string containing the wavelet name.

[XAR, XHR, XVR, XDR]= IWT(X(:, ;, 1), 'LS'); // For Red component in level 1 integer wavelet transformation XAR gives approximation coefficient, XHR gives horizontal detail, XVR gives vertical detail and XDR gives diagonal details of image.

[XAG, XHG, XVG, XDG]= IWT(X(:, ;, 2), 'LS'); // For Green component in level 1 integer wavelet transformation XAR gives approximation coefficient, XHR gives horizontal detail, XVR gives vertical detail and XDR gives diagonal details of image.

[XAB, XHB, XVB, XDB]= IWT(X(:, ;, 3), 'LS'); // For Blue component in level 1 integer wavelet transformation XAR gives approximation coefficient, XHR gives horizontal detail, XVR gives vertical detail and XDR gives diagonal details of image. To increase robustness IWT can be implemented in multiple levels based on the value of approximation coefficient.

Figure 2. MATLAB commands for Lifting Scheme (Sumit, n.d.)

- **Algorithm for Lifting Scheme**

*Step1***:** Split the given information into even and odd sets.

Step2: Predict odd sets from even sets; this step gives a guarantee of polynomial deletion in high pass.

Step3: Updates even set with wavelet co-efficient for determining scaling function, which guarantees the appearance of a moment in low pass.

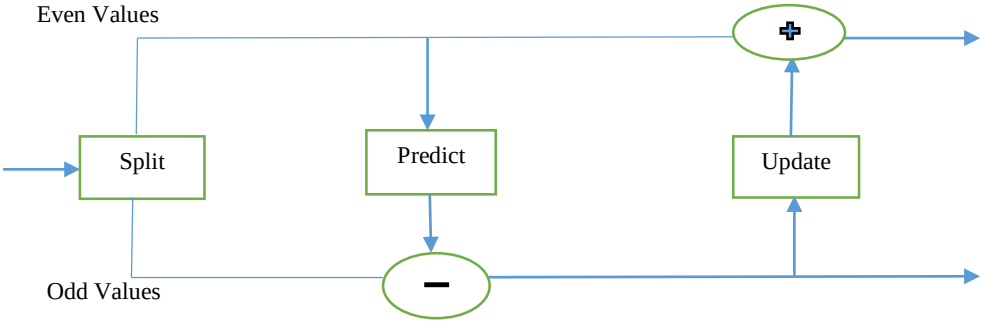


Figure 3. Forward wavelet transform Lifting Scheme (Churin et al., 2013)

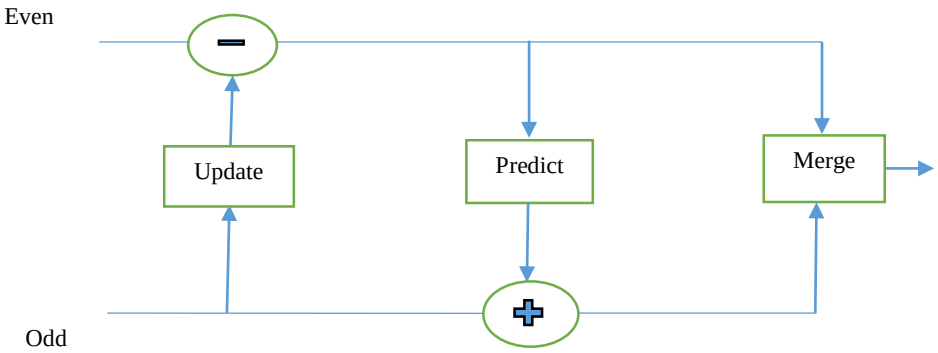


Figure 4. Inverse Wavelet Transforms Lifting Scheme

Transforming forward haar will replace A and B value with average and difference shown in equation 1:

$$a = \frac{A+B}{2}, \quad d = \frac{B-A}{2} \qquad (1)$$

Inverse haar transformation is used to calculate sample A and B's original value shown in equation 2:

$$A = \frac{a-d}{2}, \quad B = \frac{a+d}{2} \qquad (2)$$

LS allows quick execution of wavelet transforms with half computation as compared to conventional DWT. Additionally, LS is well-organized for actual short power applications and permits the in-place computation of wavelet transform that is why no secondary storage is required and the unique signal can be changed by its wavelet transform. It permits reversible integer wavelet transform as compared to the usual system which introduces error because of floating operations. Ideal reform is possible for lossless compression and could be applied for uneven sampling (Xuan, Chen, et al., 2002). Figure 3 and Figure 4 show the concept of the lifting scheme.

3.3. Singular Value Decomposition

SVD is similar to the Fourier or wavelet transformations, the only difference is that in Fourier and wavelet dimensions are infinite, but in SVD dimensions are finite. One of the applications of SVD is finding patterns in

data (Zeng, 2007). SVD finds a line that represents the data with the first left singular vector. It finds another line of data that is most close to the information. If dimensions are higher-order then the process of finding a line of data continuously does the same thing. SVD also brings smoothness to the data. This technique continuously decreases the singular values of smooth functions. As almost every real-life functions are smooth so compression algorithm is required which is also done by SVD (Thanki & Borisagar, 2018).

SVD in technical terms for matrix A of order m×n is: $U\Sigma V^T$

Where U is left singular orthogonal matrix having order m×m,

Σ is singular values diagonal matrix carrying m rows and n column and

V^T is a right singular orthogonal matrix having n×n order.

By applying SVD on *256×256* image compression can be done up to *49.45%*. First, SVD has been applied to the input image and it is converted into *64×64* blocks. The commands used for the implementation of SVD in MATLAB are specified in Figure 5.

```
inputimage=imread("Image"); // Read the image
[U, S, V]=svd(inputimage); // SVD of given image
blocksize=64;
outputimage=U(:,1:blocksize)*S(1:blocksize,1:blocksize)*V^T(1:blocksize,:); // Image is divided into block of size 64
```

Figure 5. MATLAB commands for SVD

4. Proposed Work and Methodology

An appropriate method of video steganography that is capable of balancing between information embedding capacity and robustness while maintaining video quality is required. It should be robust against attacks to be used in practical security strategies. To achieve higher security, a combination of steganography techniques with some other appropriate methods is suggested. However, the cover file could be taken as text, image, audio, or video file but among all these, video is becoming more popular. Usually, a video file has a great embedding capacity to hide the secret data because of its large size. Videos are dynamic in nature, so the chances of getting suspicious about the presence of secret information are less as compared to still images and audio. For embedding, the video cover file is first decomposed into several frames having images and audio information; then the secret information is embedded in multiple image or audio frames.

In the proposed work, Haar based Lifting scheme with the SVD method is used to resolve the problem statement as explained using a flowchart in Figure 6 and corresponding algorithm in Figure 7. This technique has a smaller amount of power utilization & more area-efficiency as compared to the DWT technique (S. Singh et al., 2016). The lifting scheme is easy to plan in hardware due to compact computations. Based on domain structures new wavelet can be derived from the original wavelets. Even samples are used to create odd samples & then through prediction and update blocks filters are replaced. The lifting method also allows a reversible integer wavelet transform. Integer numbers can be easily stored and processed as compared to real numbers.

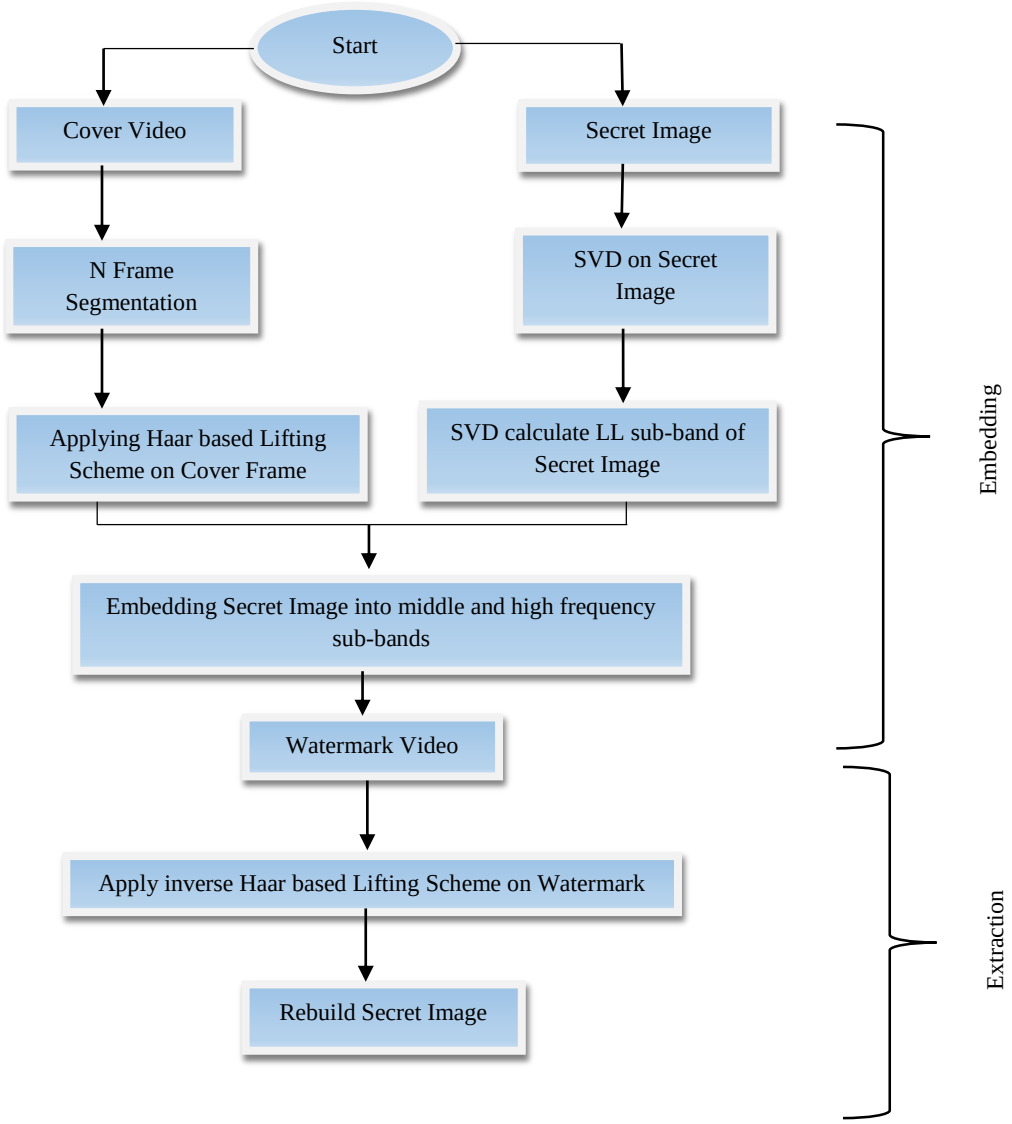


Figure 6. Embedding and Extraction Process

```
Algorithm: Lifting_scheme_Haar_wavelet_SVD
Input: Cover_video, secret_image
Output: extract_img
1.  temp_video←copy(cover_video); //copy cover video
2.  temp_img←copy(secret_image);  //copy secret image
3.  [frm, n]←extract_frame(temp_video);//extract frames from video
4.  [LL, LH, HL, HH]←SVD(temp_img); //apply SVD on image
5.  Initialize i=1, j=1, k, count;
6.      Do
7.          if (j+count)>max(LL)  //LL component have max data
8.              count←max(LL)-j;  //avoid overflow
9.          else
10.             continue;
11.         k←j+count;
12.         temp_frame←lifting_scheme_HAAR(frm[i]);
13.         bits_to_embed←LL[j ,k];
14.         embed(temp_frame ,bits_to_embed);
15.         update i←i+1;
16.         update j←k+1;
17.         while((i≤n) AND (j<max(LL)); //all frames used or complete message
        embedding
18.  steg_video←build_video(frm); //construct video to transmit
19.  temp_ext_img←inverse_ lifting_scheme_HAAR(steg_video); //apply inverse
operation to extract data
20.  extract_img←build_img(temp_ext_img);  //reconstruct secret data
21.  return(extract_img);
```

Figure 7. Proposed Algorithm

LS provides perfect restoration, nonlinear transforms and permits competent lossless compression. SVD allows enhanced perceptual excellence of created watermark file with better robustness against image processing attacks. In this work, a video has been taken as the cover file and the secret information as an image. In the embedding process, we have chosen a random frame from the video and converted the chosen frame into four sub-bands (HH, LH, LL, HL). On the secret image, the SVD technique is applied to find a valuable part of the secret message. Then by haar based lifting scheme, the secret message is hided in middle and high-frequency sub-bands to get the watermark video as output. This output video is tested against different 2D attacks for

robustness. In the extraction process, the inverse haar based lifting scheme is applied to watermark video to get the secret image. The quality of the extracted image is tested and analyzed using various evaluation parameters.

5. Implementation Details and Results Discussion

The proposed method has been implemented in MATLAB 2017 on Windows 10 platform. MATLAB processes still images and creates a simulation of videos easily. Video files of any size and any type can be used for processing in MATLAB. One of the advantages of MATLAB is that it can call external libraries for image processing.

Video file acts as a cover file and a secret message is taken in the form of an image of size 512×512. After that, it is divided into frames of size 64×64. Embedding of secret information is done in multiple random frames of the video file so that attackers will not be able to find where secret information is embedded. This makes the mischievous extraction of data more difficult.

Quantitative measurement matrices based on mathematical and computational algorithms to find the precision of the perceived image are Embedding capacity, PSNR, MSE, Structure Similarity Index Matrix (SSIM), and Corelation Coefficient (CC). These quantitative measurement matrics are calculated based on the comparison of the extracted image to the original image (Velmurugan & Hemavathi, 2019).

5.1. Embedding Capacity (EC)

Embedding means amount of secret information concealed in carrier file. (Sudir, P., & Ravishankar, M., 2015). Equation 3 represents the embedding capacity in terms of kilobytes.

$$Embedding\ Capacity = \left(\frac{Secret\ file\ size}{Cover\ file\ size}\right) \quad (3)$$

5.2. Peak Signal to Noise Ration (PSNR)

Imperceptibility means a person must not be able to differentiate between the original and the watermark video. These days many steganalysis techniques are very intelligent to notice slight modifications in cover files. High imperceptibility motivates researchers to develop steganalysis resistant video steganography techniques. We have used PSNR to measure the imperceptibility of our work which is a well-known metric and can be calculated by equation 4:

$$10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad (4)$$

Where R is the range of pixel values(R=*255* for RGB images). If the PSNR is greater than 35 dB, in that case, our visual system wouldn't be capable to distinguish between the cover image and watermark image progressively (Pramanik et al., 2020).

5.3. Mean Square Error (MSE)

The minimum value of MSE means that the original image and watermark image both have the same quality. Lower the value of MSE more robust is the steganography technique. The error can be calculated by equation 5:

$$\frac{\sum_M^N [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (5)$$

I_1 and I_2 are the original and watermark image having M rows and N columns, respectively.

5.4. Structure Similarity Index Matrix (SSIM)

The SSIM is a metric that represents a degradation in a cover file because of processing like information compression, loss of information during the transfer from source to sink. SSIM matric values vary between *0* to *1*, value *1* represents the perfect match between the extracted watermark and original image. SSIM focus on the calculation of three conditions, specifically luminance, contrast, and structure of sample. The general list is the multiplication of the above conditions as shown in equation 6 (Zaric et al., 2010):

$$SSIM(x,y) = \left[l(x,y)^{\alpha} \cdot c(x,y)^{\beta} \cdot s(x,y)^{\gamma}\right] \quad (6)$$

$$l(x,y) = Luminance\ of\ samples\ x\ and\ y,$$
$$c(x,y) = Contrast\ of\ samples, and$$
$$s(x,y) = Structure\ of\ samples$$
$$\alpha, \beta, \gamma\ denote\ the\ relative\ importance\ of\ each\ component$$

5.5. Correlation Coffiecient (CC)

The CC matric represents the relationship between the cover file and the watermark. The value of CC matric varies between *-1.0* and *1.0*. A value large than *1.0* and less than *-1.0* represents an error between the cover file and watermark. Correlation co-efficient 'r' estimates excellence and course of a direct relation among two factors scheduled scatter plot as shown in equation 7:

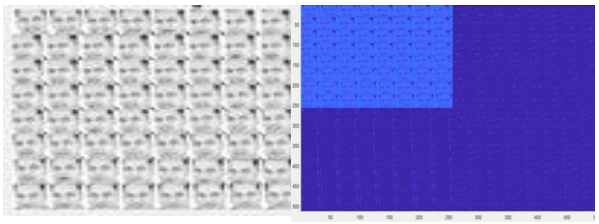
$$r_{xy} = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2 \sum(Y_i - \bar{Y})^2}} \quad (7)$$

Where:

r_{xy} - correlation coefficient for variable x and y
X_i - value of variable X in sample
x□ - average of X-variables
Y_i - value of variable Y in sample
$\bar{y}$ - average of Y-variables

For the embedding process, the Haar wavelet function has been applied on the cover video file to calculate four sub-bands LL, LH, HL, and HH as shown in Figure 8. HH sub-band has more noise so for embedding secret information HH band has been used. Now, the secret image is divided into four sub-bands with SVD and the LL sub-band has the most useful information. So, the LL sub-band of the secret image is embedded inside the HH sub-band of the video cover file to get the output as a watermarked video.

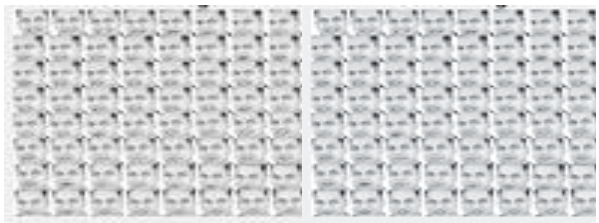
For the extraction process, the secret image is extracted from the watermark video file by applying the inverse Haar wavelet transform. Then the watermark video has been tested for robustness against different attacks e.g. low-pass filtering, scaling, rotation, transformation, and histogram equalization as shown in Figures 9, 10, 11, 12, and 13 respectively.



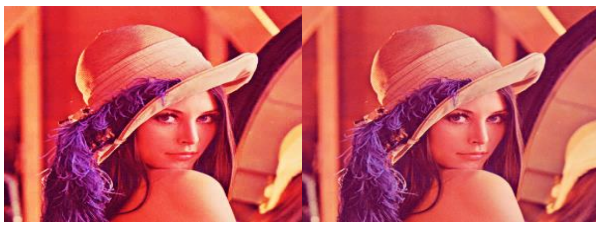
i) ii)

iii) iv)

Figure 8. i) Video cover file in 64×64 Frames, ii) Haar Wavelet Function with Lifting Scheme, iii) SVD on the Secret Image, iv) Extracted Watermark

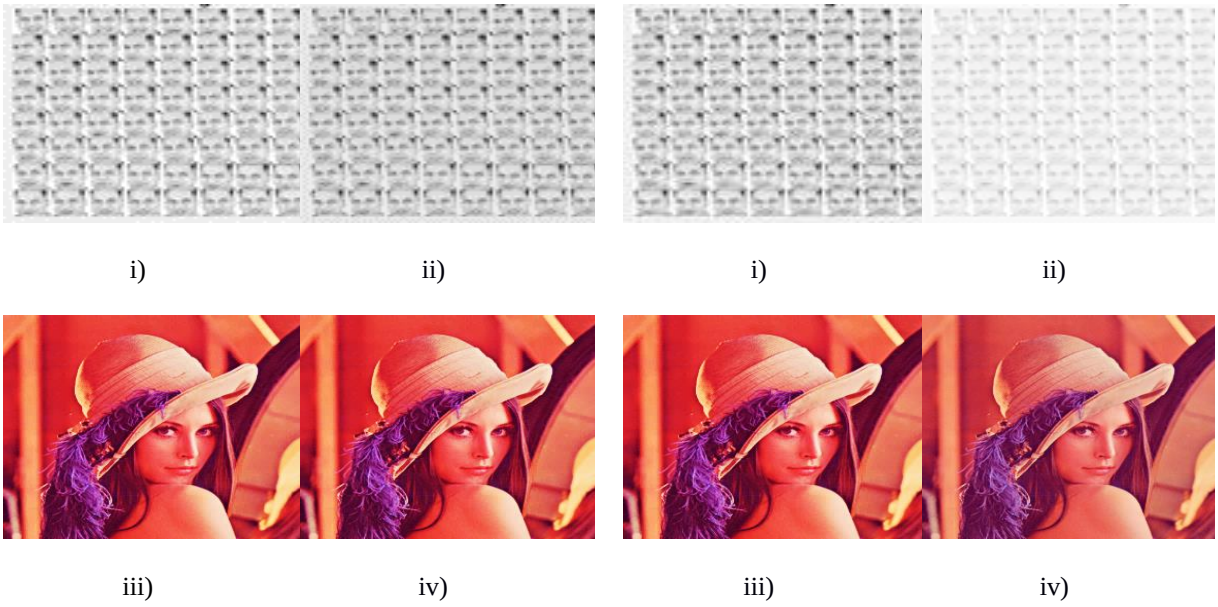


i) ii)



iii) iv)

Figure 9. i) Cover Image, ii) Watermarked Image, iii) Original Secret Image, iv) Recovered Watermark with Low Pass Filter

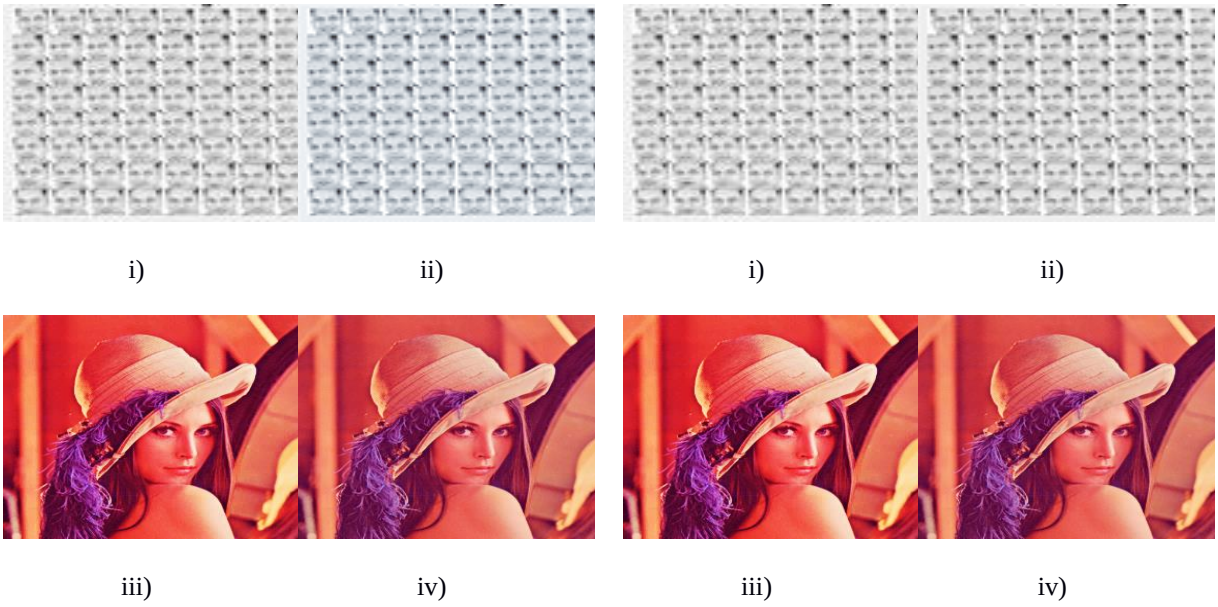


i) ii) iii) iv)

Figure 10. i) Cover Image, ii) Watermarked Image, iii) Original Secret Image, iv) Recovered Watermark with Scaling

i) ii) iii) iv)

Figure 11. i) Cover Image, ii) Watermarked Image, iii) Original Secret Image, iv) Recovered Watermark with 2D Rotation Transformation



i) ii) iii) iv)

Figure 12. i) Cover Image, ii) Watermarked Image, iii) Original Secret Image, iv) Recovered Watermark with 2D Translation

i) ii) iii) iv)

Figure 13. i) Cover Image, ii) Watermarked image, iii) Original Secret Image, iv) Recovered Watermark with Histogram Equalization

5.6. Low Pass Filtering (LPF)

Filters are used to smoothen and sharpen images by removing very high and very small frequency components. LPF removes high-frequency component & keep low-frequency components. LPF includes ideal low pass, Butterworth, and Gaussian filter (Sivasubramanian & Konganathan, 2020). The transformation function in an ideal LPF is specified below in equation 8. LPF attack is used to the generated watermark to check the robustness of the proposed technique.

$$H(U,V) = \begin{cases} 1, D(U,V) \leq D_0 \\ 0, D(U,V) \leq D_0 \end{cases} \quad (8)$$

Where, D_0: Non-negative integer

5.7. Scaling

Scaling implies resizing (increasing or decreasing) object or entity size (Ariatmanto & Ernawan, 2020). The proposed technique has been tried against scaling attack to demonstrate the strength of the watermark. First, scale the given watermark frame to enlarge it and then scale it back to the original size. Equation 9 below shows the scaling task:

Before scaling: P(X,Y); After scaling: P'(X', Y')

$$X' = X.S_x \qquad Y' = Y.S_y \tag{9}$$

5.8. Rotation

Rotation means rotating an object or entity about an angle either in a clockwise or anticlockwise direction (S. Singh et al., 2016). The watermark has been tried against the rotation process for checking the robustness of the proposed technique. Rotation can be obtained with the help of equation 10:

$$X_{new} = X_{old} \text{x} \cos\theta - Y_{old} \text{ x } \sin\theta; \quad Y_{new} = X_{old} \text{ x } \sin\theta + X_{old} \text{ x } \cos\theta \tag{10}$$

5.9. Translation

Translation means moving an object or entity from one position to another position . The proposed technique has been tested for robustness against translation attacks by changing the coordinates of the watermark. Translation can be done as shown below in equation 11:

Image coordinates before translation: P(X, Y)

Image coordinates after translation: P'(X', Y')

$$X' = X + t_{x'} \qquad Y' = Y + t_{y'} \tag{11}$$

5.10. Histogram Equalization

It is the frequency distribution of a digital object or entity. The histogram of an object or entity is a discrete function shown in equation 12 (Hashim et al., 2018). For testing the robustness of the proposed technique histogram attack also has been tested on a watermark.

$$H(r_k) = n_k \tag{12}$$

where r_k is k^{th} intensity value and n_k is no. of pixels in digital image carrying intensity r_k.

Embedding capacity, PSNR, MSE, SSIM, and CC parameters for the watermark frame have been computed under Low pass filtering, Scaling, Rotation, Translation, and Histogram equalization attacks for quantitative analysis of the proposed technique. The results are shown in Table 1 along with their graphs for embedding capacity, PSNR, MSE, SSIM, and CC matrices.

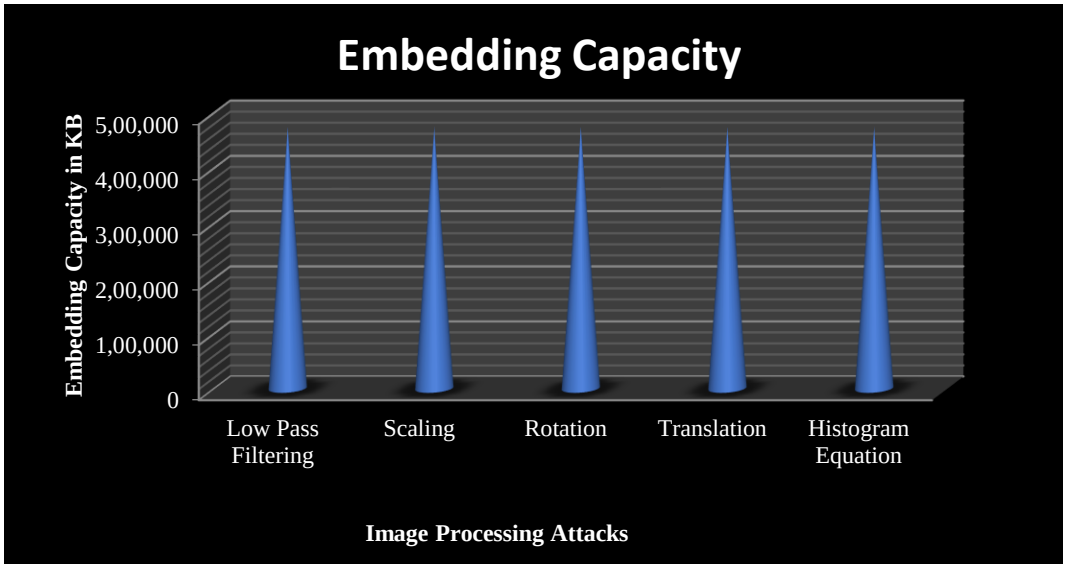


Figure 14. Embedding Capacity with 2D attacks

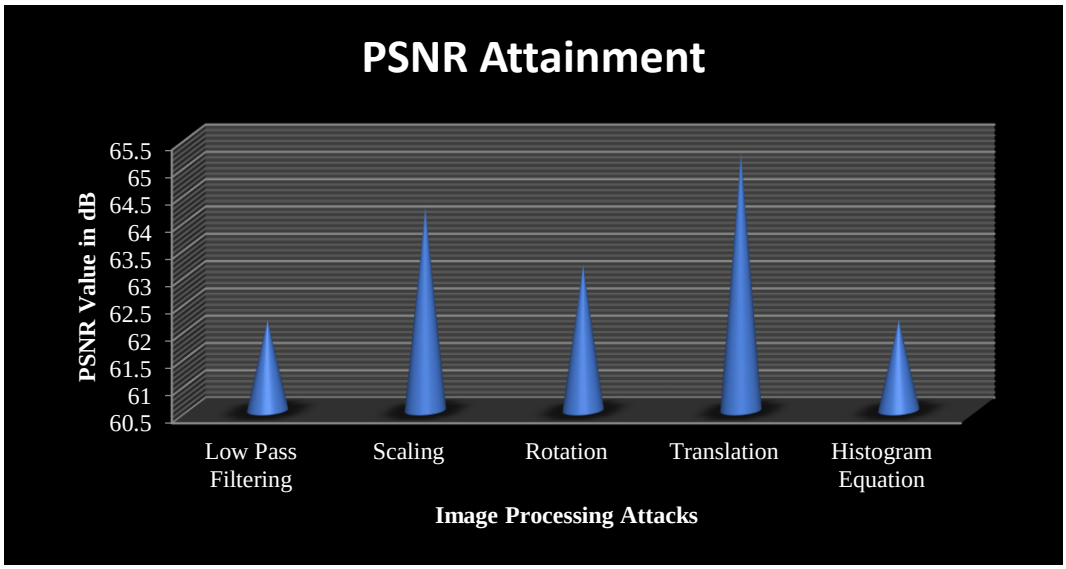


Figure 15. PSNR value with 2D attacks

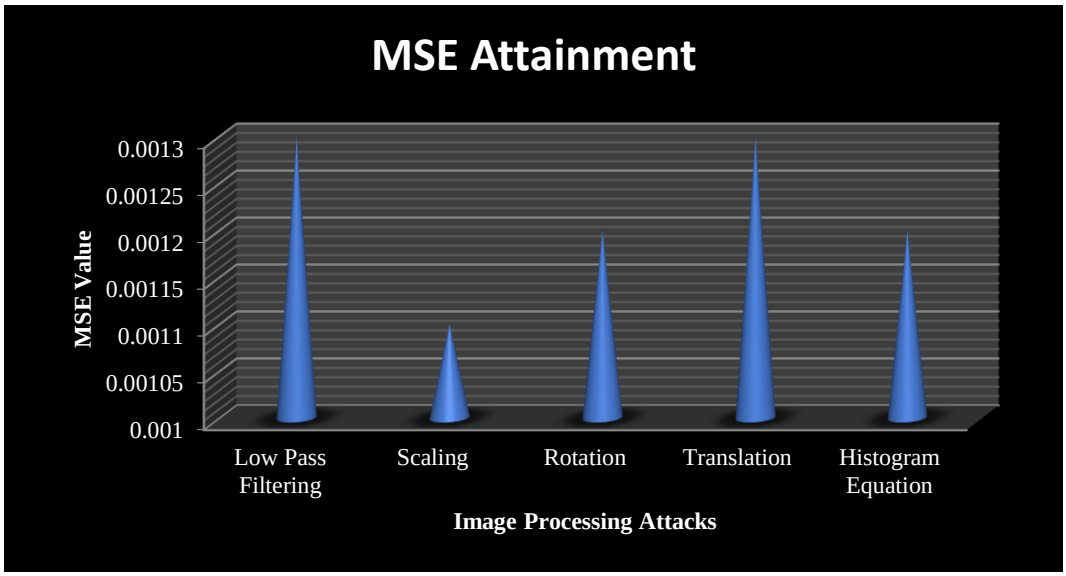


Figure 16. MSE value with 2D attacks

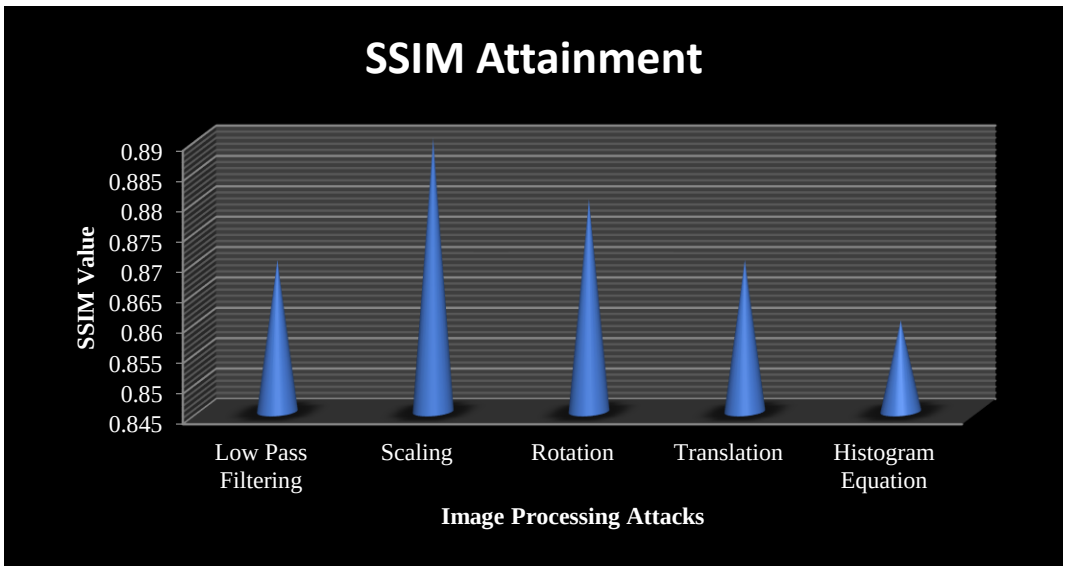


Figure 17. SSIM value with 2D attacks

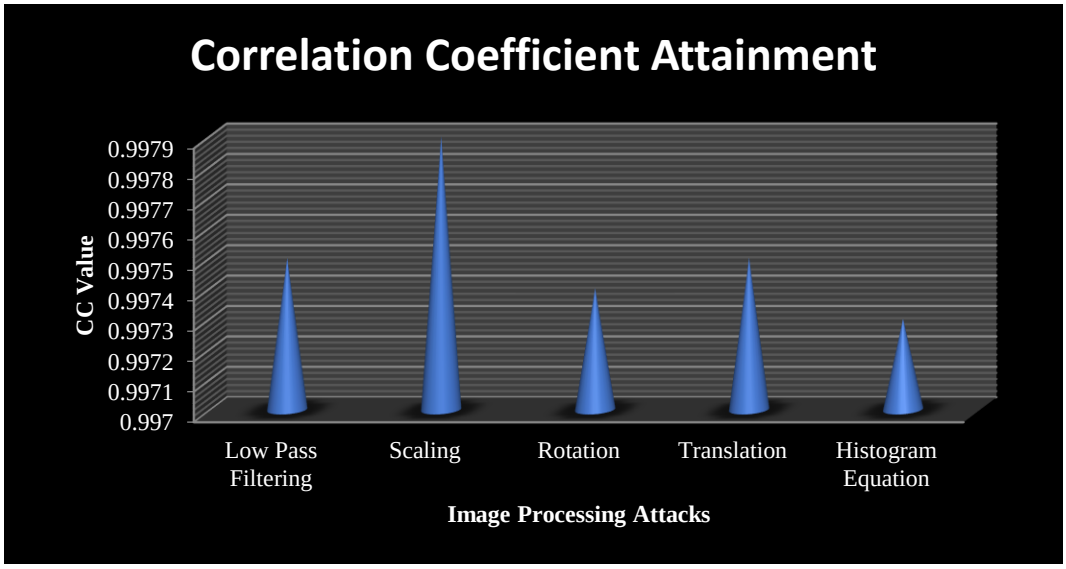


Figure 18. CC value with 2D attacks

Table 1. Value of performance matrices with different attacks on Watermark

Attacks	***Test Image (Watermark)***				
	Embedding Capacity (KB)	*PSNR*	*MSE*	*SSIM*	*CC*
Low Pass Filtering	*4,74,136*	*62.156*	*0.0013*	*0.87*	*0.9975*
Scaling	*4,74,136*	*64.23*	*0.0011*	*0.89*	*0.9979*
Rotation	*4,74,136*	*63.17*	*0.0012*	*0.88*	*0.9974*
Translation	*4,73,136*	*65.22*	*0.0013*	*0.87*	*0.9975*
Histogram Equation	*4,74,136*	*62.156*	*0.0012*	*0.86*	*0.9973*

The experimental results are visualized and analyzed against various image processing attacks. Figures 14,15,16,17,18 represent embedding capacity, PSNR, MSE, SSIM, CC values respectively for the stego image against image processing attacks like low pass filtering, scaling, rotation, translation, and histogram equation. In order to visualize properly, we have chosen a random frame of the original video and then the corresponding frame from the stego video file. The embedding capacity achieved (474136 KB) is satisfactory. It is calculated by dividing the size of the cover file by that of the secret message. PSNR is measured after applying different attacks and it ranges from *62* dB to *65* dB. The values achieved are much more than the standard value (*30* dB) which is considered as a symbol of good visual quality. The value of MSE is ranging from *0.0011* to *0.0013* even after the application of different attacks. It shows that the similarity between the original and extracted data remains maintained after attacks as well. In terms of the SSIM metric, the value is ranging from *0.86* to *0.89* which is within *10%* variance of the standard value of SSIM. This shows that the original frame and stego frame are structurally close. The correlation coefficient attains values ranging from *0.9973* to *0.9979* which shows the acceptability of the proposed method. Based on the analysis of the values attained for all these parameters, it can be said that the proposed technique has achieved the objective of large embedding capacity while maintaining robustness along with the good visual quality of the watermark.

6. Conclusion and Future Scope

The work done comprises the embedding of the secret image inside a video cover file. In order to resolve the well-known trade-off between achieving high embedding capacity along with robustness, the Haar wavelet transform based lifting scheme along with the SVD technique has been used. SVD has provided good robustness against image processing attacks by modifying singular values of the watermark. Additionally, SVD also provided image compression thereby contributing to improved embedding capacity. The use of Haar based lifting scheme helped to achieve a good reconstruction of the watermark, increasing smoothness, and decreasing aliasing effects. The performance of the proposed method is analyzed using the standard digital signal processing parameters like PSNR, MSE, SSIM, and CC. The attainment of these parameters ultimately evaluates the achievement of steganography objective; robustness, imperceptibility, embedding capacity, and quality of watermark video. Experimental results show that the proposed method achieved *63.386* dB and *0.00122* as an average PSNR and MSE respectively. This is a symbol of good robustness. Additionally, the attainment of the *0.874* average value for SSIM supports the achievement of requirement robustness. On the other hand, the embedding capacity calculated comes to be *474136* KB that can be considered satisfactory. The proposed method is capable of providing more robustness and good quality of watermark video while maintaining high embedding capacity. The method is found to be resistant against low-pass filtering, scaling, rotation, translation, and histogram equalization attacks. Additionally, the method demands less computational power thereby increasing the performance in terms of execution time.

Considering the entire cover video during embedding secret information may result in a poor quality of the stego file. Rather finding a specific region and focusing on that specific part of the cover video for embedding provides better results in terms of imperceptibility and robustness. Because of this, the first challenge for the attacker would be to find out the specific portion where secret information could have been embedded like the face or body of humans, cars, and other objects similarly.

References

1. Ariatmanto, D., & Ernawan, F. (2020). An improved robust image watermarking by using different embedding strengths. *Multimedia Tools and Applications*, *79*(17–18), 12041–12067. https://doi.org/10.1007/s11042-019-08338-x
2. Banik, B. G., & Banik, A. (2020). Robust, imperceptible and blind video steganography using RGB secret, maximum likelihood estimation and Fibonacci encryption. *International Journal of Electronic Security and Digital Forensics*, *12*(2), 174–199. https://doi.org/10.1504/IJESDF.2020.106310
3. Bruno Razafindradina, H., & Mohamed Karim, A. (2013). Blind and Robust Images Watermarking Based on Wavelet and Edge Insertion. *International Journal on Cryptography and Information Security*, *3*(3), 23–30. https://doi.org/10.5121/ijcis.2013.3303
4. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2009). A skin tone detection algorithm for an adaptive approach to steganography. *Signal Processing*, *89*(12), 2465–2478. https://doi.org/10.1016/j.sigpro.2009.04.022
5. Churin, K., Preechasuk, J., & Chantrapornchai, C. (2013). Exploring video steganography for hiding images based on similar lifting wavelet coefficients. *Communications in Computer and Information Science*, *409*, 35–46. https://doi.org/10.1007/978-3-319-03783-7_4
6. Gupta, P., & Parmar, G. (2017). Image watermarking using IWT-SVD and its comparative analysis with DWT-SVD. *2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017, July*, 527–531. https://doi.org/10.1109/COMPTELIX.2017.8004026
7. Hashim, M. M., Rahim, M. S. M., Johi, F. A., Taha, M. S., & Hamad, H. S. (2018). Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *International Journal of Engineering and Technology(UAE)*, *7*(4), 3505–3514. https://doi.org/10.14419/ijet.v7i4.17294
8. Joshi, S., Arindom, R., Dikshit, T., Anish, B., Deep, A. G., & Pallav, P. (2015). Lifting-based discrete wavelet transform for real-time signal detection. *Indian Journal of Science and Technology*, *8*(12), 83–89. https://doi.org/10.17485/ijst/2015/v8i
9. Kakde, Y., Gonnade, P., & Dahiwale, P. (2015). *Audio-Video steganography*.
10. Li, P., Benezeth, Y., Nakamura, K., Gomez, R., Li, C., & Yang, F. (2018). Comparison of region of interest segmentation methods for video-based heart rate measurements. *Proceedings - 2018 IEEE 18th International Conference on Bioinformatics and Bioengineering, BIBE 2018*, 143–146. https://doi.org/10.1109/BIBE.2018.00034
11. Mudusu, R., Nagesh, A., & Sadanandam, M. (2018). Enhancing Data Security Using Audio-Video

Steganography. *International Journal of Engineering & Technology*, *7*(2.20), 276. https://doi.org/10.14419/ijet.v7i2.20.14777

12. Muhuri, P. K., Ashraf, Z., & Goel, S. (2020). A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization. *Applied Soft Computing Journal*, *92*, 106257. https://doi.org/10.1016/j.asoc.2020.106257
13. Pramanik, S., Bandyopadhyay, S. K., & Ghosh, R. (2020). Signature Image Hiding in Color Image using Steganography and Cryptography based on Digital Signature Concepts. *2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 - Conference Proceedings*, *Icimia*, 665–669. https://doi.org/10.1109/ICIMIA48430.2020.9074957
14. Raftari, N., & Moghadam, A. M. E. (2012). Digital image steganography based on Integer Wavelet Transform and assignment algorithm. *Proceedings - 6th Asia International Conference on Mathematical Modelling and Computer Simulation, AMS 2012*, 87–92. https://doi.org/10.1109/AMS.2012.15
15. Roy, S., & Pal, A. K. (2019). A Hybrid Domain Color Image Watermarking Based on DWT–SVD. *Iranian Journal of Science and Technology - Transactions of Electrical Engineering*, *43*(2), 201–217. https://doi.org/10.1007/s40998-018-0109-x
16. Sanjida. (nd). Digital Image Processing tutorial-3. (n.d.). *URL: https://www.youtube.com/watch?v=c2VMpu0Q4UU*. Created on March 17, 2020, Accessed on May 30, 2020.
17. Singh, R. K., & Shaw, D. K. (2018). A hybrid concept of cryptography and dual watermarking (LSB-DCT) for data security. *International Journal of Information Security and Privacy*, *12*(1), 1–12. https://doi.org/10.4018/IJISP.2018010101
18. Singh, S., Singh, R., & Siddiqui, T. J. (2016). Singular value decomposition based image steganography using integer wavelet transform. *Advances in Intelligent Systems and Computing*, *425*, 593–601. https://doi.org/10.1007/978-3-319-28658-7_50
19. Sivasubramanian, N., & Konganathan, G. (2020). A novel semi fragile watermarking technique for tamper detection and recovery using IWT and DCT. *Computing*. https://doi.org/10.1007/s00607-020-00797-7
20. Sumit, S. P. S. using wavelet transform proj. with source code. (n.d.). *URL: https://www.youtube.com/watch?v=jmBWkMJ2iYo&t=159s*. Created on Sept 11, 2017, Accessed on May 27, 2020.
21. Thanikaiselvan, V., & Arulmozhivarman, P. (2013). High security image steganography using IWT and graph theory. *IEEE ICSIPA 2013 - IEEE International Conference on Signal and Image Processing Applications*, 337–342. https://doi.org/10.1109/ICSIPA.2013.6708029
22. Thanki, R. M., & Borisagar, K. R. (2018). Securing multiple biometric data using SVD and Curvelet-based watermarking. *International Journal of Information Security and Privacy*, *12*(4), 35–53. https://doi.org/10.4018/IJISP.2018100103
23. Velmurugan, K. J., & Hemavathi, S. (2019). Video Steganography by Neural Networks Using Hash Function. *5th International Conference on Science Technology Engineering and Mathematics, ICONSTEM 2019*, *1*(2017), 55–58. https://doi.org/10.1109/ICONSTEM.2019.8918877
24. Xuan, G., Chen, J., Zhu, J., Shi, Y. Q., Ni, Z., & Su, W. (2002). Lossless data hiding based on integer wavelet transform. *Proceedings of 2002 IEEE Workshop on Multimedia Signal Processing, MMSP 2002*, *January*, 312–315. https://doi.org/10.1109/MMSP.2002.1203308
25. Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z., & Su, W. (2002). Distortionless data hiding based on integer wavelet transform. *Electronics Letters*, *38*(25), 1646–1648. https://doi.org/10.1049/el:20021131
26. Zaric, A., Loncaric, M., Tralic, D., Brzica, M., Dumic, E., & Grgic, S. (2010). Image quality assessment - Comparison of objective measures with results of subjective test. *Proceedings Elmar - International Symposium Electronics in Marine*, *October 2014*, 113–118.
27. Zeng, G. (2007). Facial recognition with singular value decomposition. *Advances and Innovations in Systems, Computing Sciences and Software Engineering*, *480*, 145–148. https://doi.org/10.1007/978-1-4020-6264-3_26