future internet

MDPI

Article

Framework for Video Steganography Using Integer Wavelet Transform and JPEG Compression

Urmila Pilania [1], Rohit Tanwar [2,*], Mazdak Zamani [3,*] and Azizah Abdul Manaf [4]

[1] Department of CST, Manav Rachna University, Faridabad 121004, India
[2] School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[3] Department of Computer Science, New York University, 251 Mercer, New York, NY 10012, USA
[4] Department of Internet Engineering and Computer Science, LKCFES, Universiti Tuanku Abdul Rahman, Kampar 31900, Malaysia
* Correspondence: rohit.tanwar.cse@gmail.com (R.T.); mazdak.zamani@nyu.edu (M.Z.)

Abstract: In today's world of computers everyone is communicating their personal information through the web. So, the security of personal information is the main concern from the research point of view. Steganography can be used for the security purpose of personal information. Storing and forwarding of embedded personal information specifically in public places is gaining more attention day by day. In this research work, the Integer Wavelet Transform technique along with JPEG (Joint Photograph Expert Group) compression is proposed to overcome some of the issues associated with steganography techniques. Video cover files and JPEG compression improve concealing capacity because of their intrinsic properties. Integer Wavelet Transform is used to improve the imperceptibility and robustness of the proposed technique. The Imperceptibility of the proposed work is analyzed through evaluation parameters such as PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), SSIM (Structure Similarity Metric), and CC (Correlation Coefficient). Robustness is validated through some image processing attacks. Complexity is calculated in terms of concealing and retrieval time along with the amount of secret information hidden.

Keywords: steganography; text; audio; image; video; steganography attacks; stego file; integer wavelet transform; JPEG compression

check for updates

Citation: Pilania, U.; Tanwar, R.; Zamani, M.; Manaf, A.A. Framework for Video Steganography Using Integer Wavelet Transform and JPEG Compression. *Future Internet* **2022**, *14*, 254. https://doi.org/10.3390/fi14090254

Academic Editors: Nicolae Goga and Dan Garlasu

Received: 26 July 2022
Accepted: 19 August 2022
Published: 25 August 2022

1. Introduction

The internet and computer systems are gaining popularity day by day. So, in the world of digital communication, people of all age groups are transferring personal information through the web. However, the security of personal information is becoming an important issue among researchers. Steganography is the way to secure personal data in the cover file so that no one, other than the sender and receiver, is aware of its existence [1,2]. The process of steganography is shown in Figure 1. The steganography process can be carried out without a secret key. By including secret key security, of the technique is improved. With the help of a key, secret data is encrypted first and then the encrypted secret data is concealed in the cover file. In this way, it is very difficult for the hacker to detect secret information. However, combining steganography and cryptography may increase complexity of the technique. Complexity can be measured in terms of total time taken to embed the secret message. The cost of the technique may also increase because of the increase in the number of hardware devices.

Steganography techniques have some issues associated with them. Some of the issues with various steganography techniques are low concealing capacity, low graphical excellence of stego files, less robustness against attacks, the varying format of the cover file, authenticity, integrity, confidentiality, and flexibility [3]. Some of these issues can be overcome by choosing video as a cover file because of its inherent features. Dependent upon the kind of carrier file used steganography is divided into text, image, audio, and video as shown in Figure 2 [4].

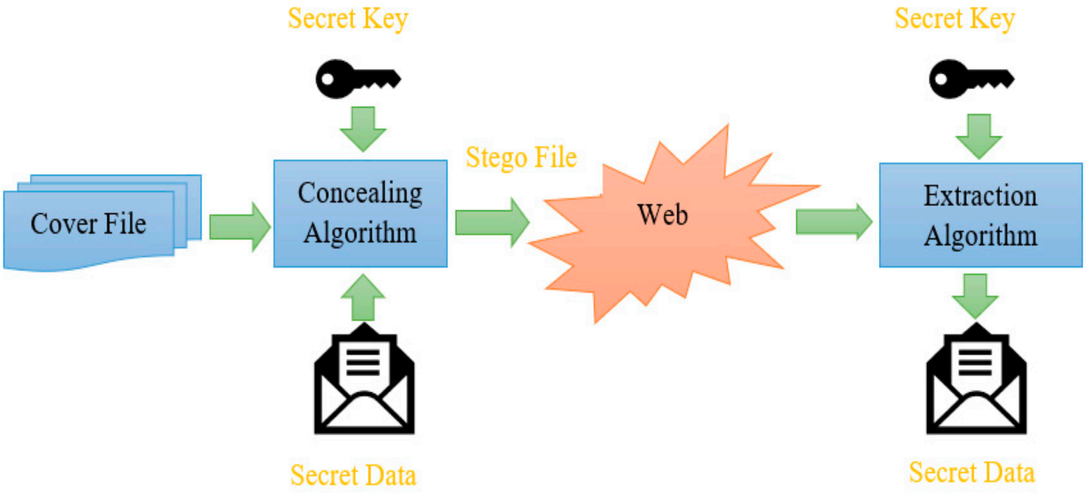


Figure 1. Steganography Process.

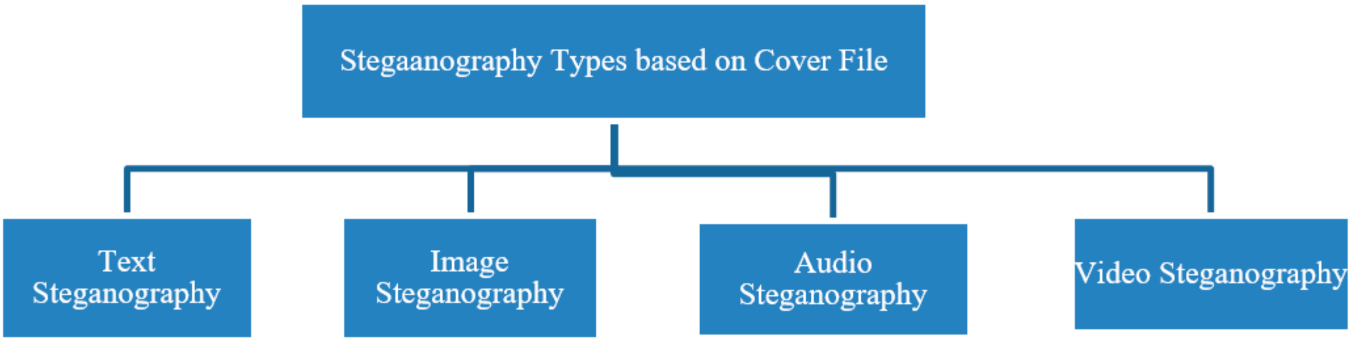


Figure 2. Steganography Types.

All these types of video files are gaining popularity day by day. Video files have their application in various fields like social sites, education, medical, business, banking, etc. Video files have a large size compared to other files like text, images, and audio. Due to the large size of the video, concealing capacity can be improved. A video file has multiple options to conceal secret information. Due to this, the security of the technique can be improved. Because of the dynamic nature of video, the chances of detection of secret information are reduced. In this way, robustness against different types of attacks can be increased [5,6].

Some of the key issues associated with the existing steganography techniques are concealing capacity, imperceptibility, and robustness. The issue of concealing capacity could be overcome by taking a video as a cover file. A video has a large size; so by providing multiple options to hide secret information, the concealing capacity can be improved. By using IWT for concealing secret information, imperceptibility, as well as robustness, can be improved. Traditional transform techniques have many disadvantages over IWT techniques. Traditional techniques work on the persistent frequency of the entire signal, but IWT decompose signals into set of wavelets. The IWT technique works in the transform domain. Transform domain techniques can analyze the signal in terms of time as well as frequency. In the time domain, a sharp spike of the signal can be identified easily. Hiding secret information in the sharp spikes does not disturb the quality of the stego file. IWT deals with integer coefficients, so requires less computational cost and time. So, IWT with video cover files can provide a proper balance between concealing capacity, imperceptibility, and robustness. JPEG compression is also helpful to enhance the concealing capacity of the technique.

This paper is organized into six sections in total. Section 2 discusses and summarizes the related work. The summary presented in Section 2 helped the authors on the proposed technique. The proposed model along with the respective algorithms is described in Section 3. Section 4 presents the experimental setup for the proposed work. In Section 5, the results are discussed and analyzed based on various evaluation parameters. The conclusion along with the future directions is presented in Section 6.

2. Literature Review

In this section, some of the existing steganography techniques are reviewed. These techniques include text, audio, image, and video steganography. A lot of work has been done on steganography techniques by researchers and academicians. However, there are some issues with these techniques and these issues need to be resolved to enhance the security of the communication system. Some of the techniques are explored with their pros and cons as follows:

Using text has some advantages, like requiring less memory space, less processing time, and less cost for printing. Along with that, the growth of the internet in almost every field of life also supports text documents. In text steganography, it is very difficult to use secret keys, although secret keys improved the security level. During the embedding of secret information rewriting, spacing, modifying line height, addition, and removal of words may result in the detection of secret information. It does not work properly on public carrier files [7]. A long time ago, text steganography was widely used by many researchers. Numerous text steganography techniques have already existed. In [8], authors proposed a novel text steganography technique in Persian and Arabic texts. A vertical displacement of points in Persian and Arabic phrases has been calculated by authors for concealing secret information. Implementation of work was done in Java language. Persian and Arabic phrases have many points in them so there exist a large number of options for concealing secret information. By doing so, the concealing capacity was improved. It was very difficult to detect hidden secret information because of the lack of availability of modern OCR (Optical Character Recognition) programs for these languages. However, secret information may get lost because of the retyping of text [9].

In this work, the Least Significant Bit Matching (LSBM) technique has been proposed for greyscale images in the spatial domain. Whenever the secret information bit does not match the Least Significant Bit (LSB) of the carrier image, then +1 or −1 is arbitrarily added to the resultant pixel value [10]. The irregularity effect is avoided due to the possibility of increasing or decreasing every altered pixel value being identical. LSBM works by matching the bits of the secret information and the carrier file, whereas LSB substitution works by substituting the LSB of the carrier file with secret data. This technique provides a large capacity as compared to the LSB technique. The visual quality of the stego file and robustness against image processing attacks is good in comparison with LSB. The LSB matching technique is more robust than the LSB substitution technique. LSB substitution technique just replaces the LSB bit of the carrier file with the secret information bit, while the LSB matching technique matches bits of carrier and secret file. Steganalysis of the LSB matching technique is very challenging and related to LSB substitution.

In the silent part of speech, secret information can be concealed which is known as the audio steganography technique. It is the simplest technique for concealing secret information with a low capacity. In this proposed work, to find the capacity of the technique, silent intervals of speech are determined and their respective length also. Determined values are reduced by x, where $0 < x < 2n$ bits and n bits represent the size of secret information that is to be concealed. During retrieval of secret information, x is calculated as mod (NewIntervalLength, 2n bits). An example is given below to understand the process of information concealing and retrieval. If value 5 is to be concealed inside the silent part of speech having size = 108, there is a need to remove 6 samples from this silent part of speech, resulting in a new length of 102 samples. For retrieving concealed information from the silent part in stego speech, a need to find mod (102, 8) = 6. These silent parts of speech remain unchanged as they generally happen in continuous sentences. This technique has good visual quality. The hidden secret message is exposed to attacks on compression. It also has a low concealing capacity [11].

In the proposed work [12], the Hash-based Least Significant Bit (HLSB) technique conceals secret information inside carrier video files having any format. Carrier video is divided into several frames, then a particular frame is selected to conceal secret information. Information about the carrier video like the number of frames, speed of frame, the height and width of the frame, etc. are retrieved from the header. The HLSB technique is used to embed secret data inside a particular frame. The size of secret information does not matter as in video there are multiple frames so secret information can be concealed in more than one frame. This technique is capable to conceal eight bits of secret information in the LSB of the RGB model. It conceals 3 bits in R, 3 bits in G, and 2 bits in B pixel of the RGB model. A 3-3-2 pixel scattering pattern is used due to the chromatic impact of the blue pixel on the human being more than that of the red and green pixel. In this way, video quality is not affected because of information concealing and a large amount of secret information can be concealed. A little change in the quality of the video is not detected by the human eyes. The location where secret information is concealed can be calculated by using the hash function as shown:

$$k = p\%n.$$

where k is the LSB bit location inside a particular pixel; p denotes the location of every concealed image pixel and n is the total number of bits of LSB [13].

In the proposed paper, the IWT steganography technique has been implemented on images. The high frequency components were used for embedding the secret message. As these coefficients represent image edges and embedding data into edges is safe compared to embedding in any other part of the image. The targeted coefficients were selected based on the intensity of edges. These selected edges were compared to the neighbouring coefficients. The input image was decomposed into blocks and IWT technique was applied on each block. The output stego generated was found to be of good visual quality. The PSNR and MSE were calculated for the evaluation of the work. The comparison of the work also has been done with some existing work for analysis of visual quality and robustness [14].

It has been concluded that a trade-off exists between embedding capacity, imperceptibility, and robustness. In the proposed work, a video steganography technique using IWT has been implemented. The IWT technique works in transform domain, so it is able to conceal the secret information in appropriate coefficients. It used a high frequency component to embed the secret data as these coefficients have a noise part of the signal. Embedding data in the noise part of the signal results in more security. The research work was implemented in MATLAB. Experimental results proved that the proposed work carry high robustness against attacks [15].

The security system is divided into two parts which are information encryption and embedding. There are many information encryption techniques in the market, but these techniques are only able to encode the secret data, their existence cannot be hidden. Information embedding techniques are able to hide the existence of secret data. In this proposed paper, an IWT-based image steganography technique has been implemented by the author. IWT transforms the high frequency components to embed the secret message. For the embedding of the secret message, the coefficients were segregated into 6 different categories by calculating value of Most Significant Bit (MSB). Coefficients lying in higher bands were used first to embed the secret data and so on. In the proposed work, a 67.7 KB secret message was embedded and then the PSNR of stego was calculated, which was found to be 54DB. Because of the IWT technique, secret message reconstruction was done efficiently [16].

From the literature review, it has been concluded that video steganography is gaining popularity. The existing techniques were compared based on the parameters mentioned in Table 1. All the parameters are properly achieved by video steganography techniques. Some of the issues related to existing steganography techniques are given as follows [17,18]:

- A relationship exists between concealing capacity, imperceptibility, and robustness.
- On changing one parameter, the other two are affected. Such as, increasing concealing capacity, the imperceptibility and the robustness of the stego file decreases.
- Text, images, and audio files are not able to store much information.
- Computational cost increases when combining multiple techniques.
- A technique can work with a specified format of cover as well as secret information only.
- Combining cryptography and steganography increase the complexity of the technique.

Table 1. Steganography Techniques based on Cover File Type [19].

Parameter	Text Steganography	Audio Steganography	Image Steganography	Video Steganography
Cover File	It hides secret information into the text	It hides secret information in the inaudible frequency	It hides secret information in images	It can hide secret information in images as well in inaudible frequency
Secret Information	Text	Text as well as inaudible frequency	Text as well as images	Text, images, inaudible frequency
Speed	Slow	Varies on the type of technique used	Fast compared to text, audio, and video steganography	In the video, steganography speed is slow compared to image steganography. The first video is converted to images and inaudible frequency and then secret information is embedded
Embedding Capacity	Low	Large compared to text steganography	Large compared to audio steganography	High concealing capacity because it has the option of hiding in images as well inaudible frequency
Robustness	Less robust	Robust compared to text	Robustness increases in image steganography	Robust because of its large size and multiple options for concealing secret information
Imperceptibility	On increasing concealing capacity imperceptibility got compromised	Carrier good visual quality compared to text steganography	An imperceptible small change in the color value of an image does not be noticed by naked human eyes	Because of the dynamic nature of video changes are not noticeable so carrier high imperceptibility
Security	Less secure	Security increases	Secure because of high imperceptibility as well robustness	It is more secure because of the dynamic and large size of video files. It also has the option for concealing secret information in audio as well as multiple images
Concealing and Retrieval Time	Less	More compared to text steganography	Need to encode and decode only a single image so takes less time	Take more time to encode and decode secret information. Secret information is concealed inside multiple images or inaudible frequency

3. Proposed Method

IWT along with the JPEG compression video steganography technique is the one that balances concealing capacity, imperceptibility, and robustness. IWT needs low power and is much more effective in terms of memory. IWT technique works on integer coefficients. With integer coefficients, calculations take less time, and chances of error are also reduced. Hardware execution of IWT is also simple due to its integer nature. To authenticate the scattering output calculates covariance (σ_{XnXm}) of sub-bands, by considering two at a time. Covariance can be expressed as in Equation (1) [20]:

$$\sigma_{X_nX_m} = (X_nX_m)^c - (X_n)^c(X_m)^c \tag{1}$$

As in Equation (1), the value of variance is found to be lowest for HH and LL sub-bands. Figure 3 shows the decomposition of input signal or video into LL and HH components [21]. Low Pass Filter (LWF) converts the input signal into LL coefficients and High Pass Filter (HPF) converts input into HH coefficients. LL coefficients are the low-frequency content and are known as an approximation. HH coefficients are high-frequency content and are known as details. LL coefficients carry the finest detail of image and HH coefficients carry noise.

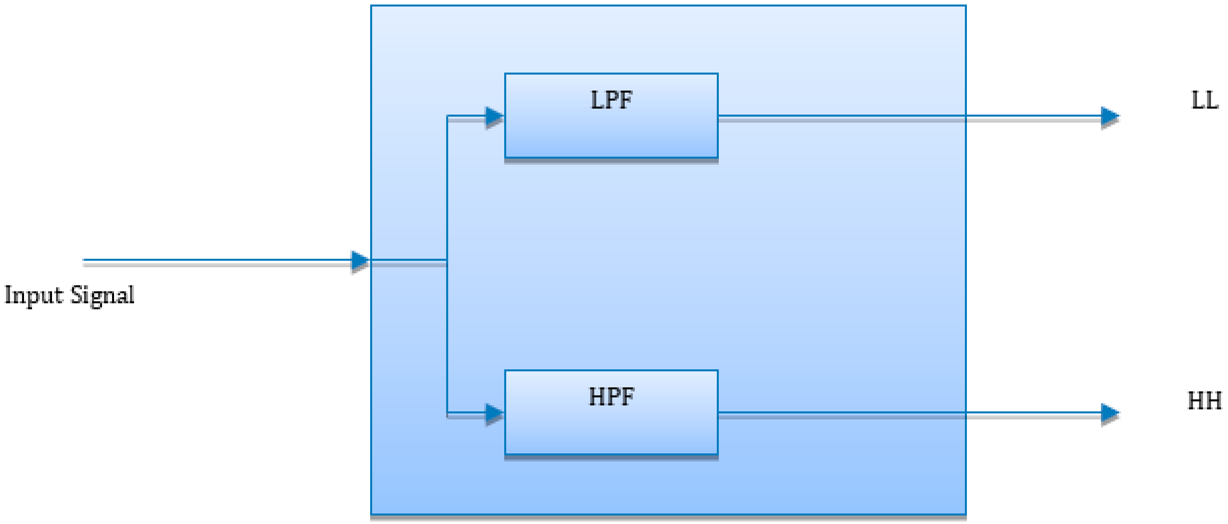


Figure 3. Approximation and Detail Coefficients.

The process of decomposing the signal is known as signal analysis. During signal analysis twice coefficients are produced so to reduce the number of coefficients decimation of coefficients is done by down sampling filter output by 2. Reduced coefficients are represented as LL * and HH *. The whole process of decimation is shown in Figure 4 as follows [19]. During decomposition only LL coefficients are considered. As LL coefficients have important information and HH coefficients have noise. Every time during decomposition, noise is removed from the information part and lastly the refined information is retrieved.

The process of decomposition of coefficients into lower resolution coefficients goes up to log2N levels. Where N is the length of the input signal. Every time LL coefficients are decomposed into LL and HH coefficients. LL coefficients give refined detail of signal and noise is eliminated from the signal in the form of HH coefficients every time due to decomposition. The decomposition tree is shown in Figure 5. In the given figure, three level decomposition of the signal is done. It can be decomposed further but up to the three level most of the noise is eliminated. So, researcher and academician generally do three levels of decomposition of the given input file or signal.

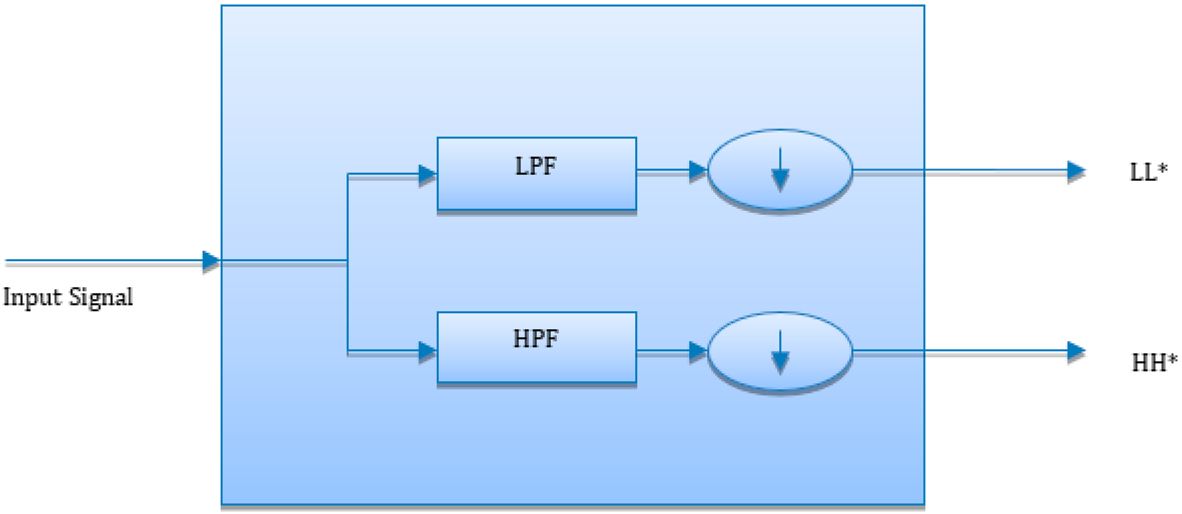


Figure 4. Signal Analysis.

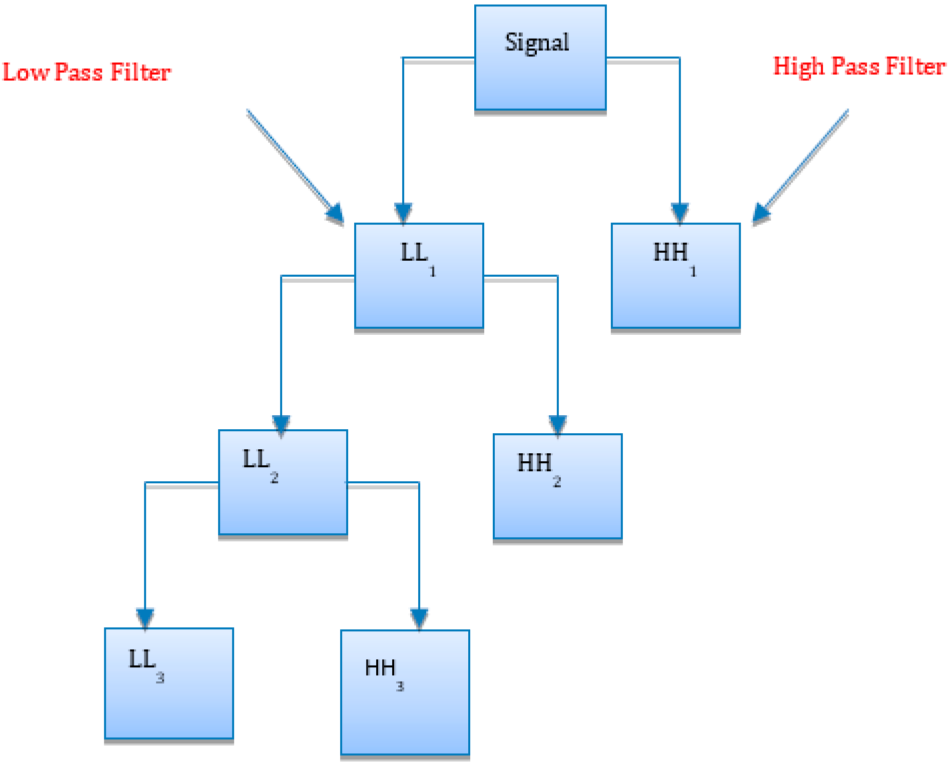


Figure 5. Wavelet Decomposition.

After a complete analysis of the input signal by using inverse IWT signals, synthesis takes place. In signal synthesis, approximation coefficients are upsampled by 2 in each step up to log2N levels. Upsampling of the signal is explained with the help of Figure 6 as follows. In signal synthesis the reduced coefficients are added back to the signal to regenerate the original signal. This process takes place at the receiver side when receiver extract the hidden secret message.

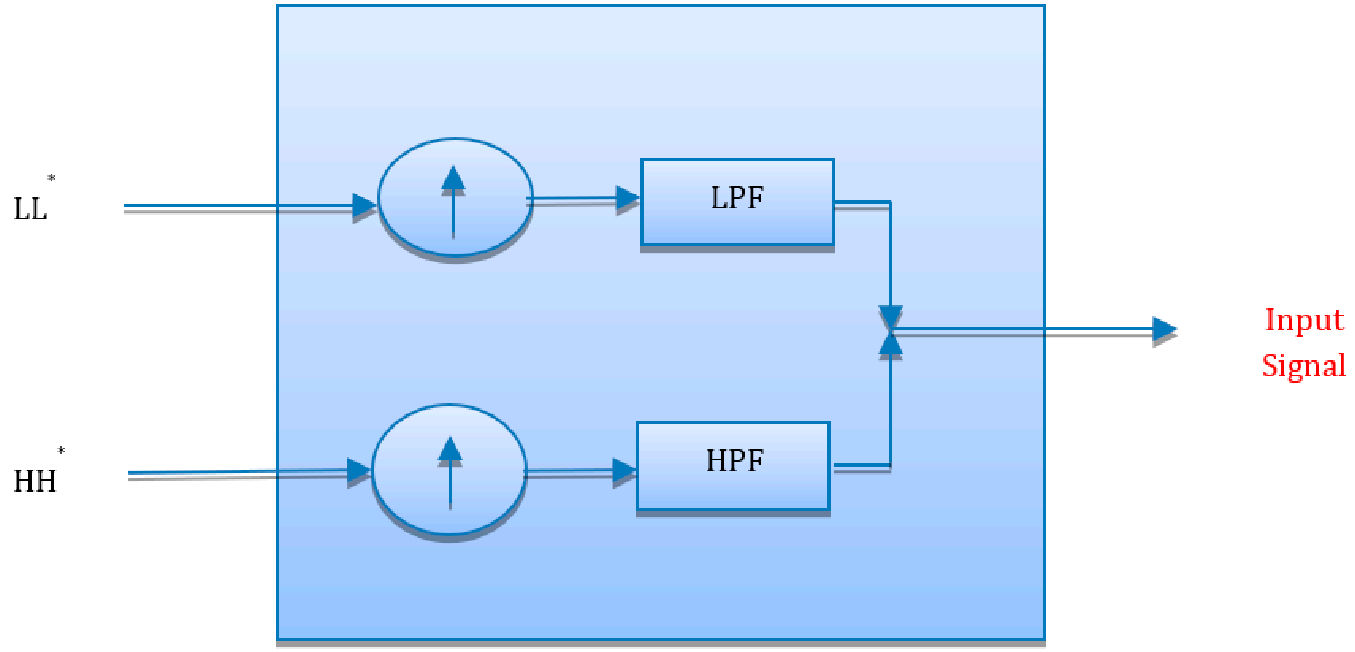


Figure 6. Signal Synthesis.

By signal synthesis, an up to log2N original signal is generated. Figure 7 shows the flow of signal reconstruction by using inverse IWT. In the complete process, almost no loss of information occurs because of the integer nature of the IWT technique. IWT reconstruct the original signal from the integer coefficients. It provides lossless reconstruction of signal due to its integer nature. Because of its simple implementation it requires less hardware resulting into low cost.

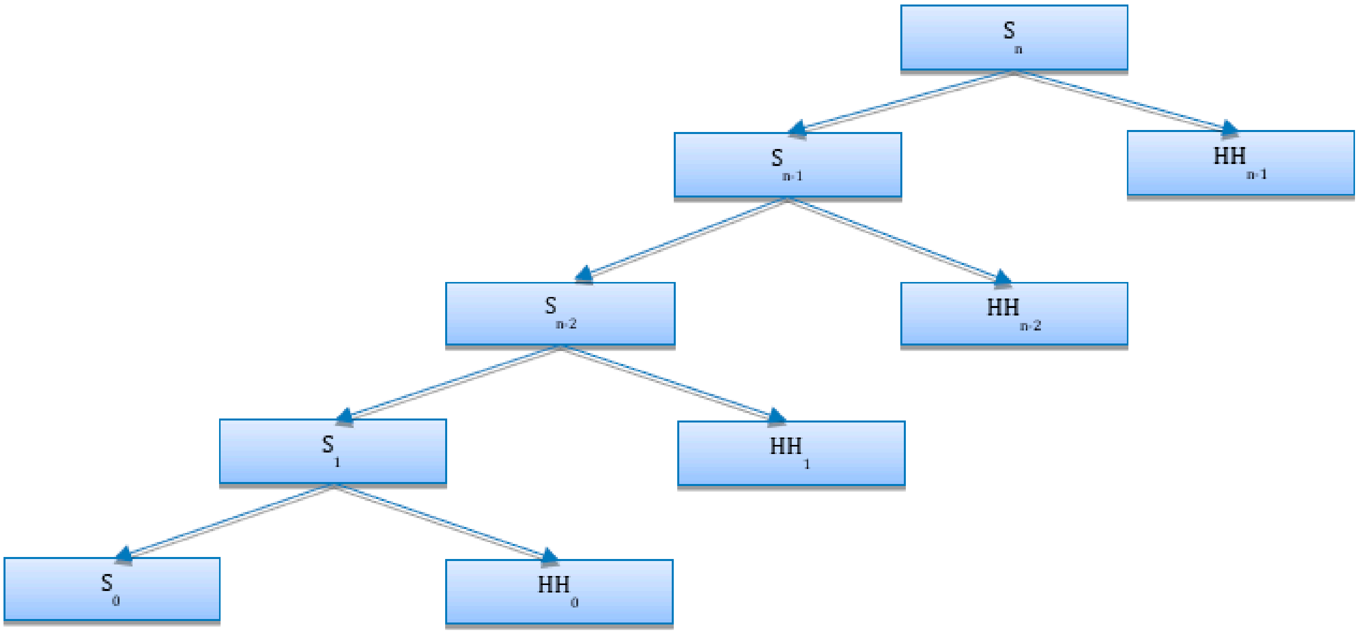


Figure 7. Signal Reconstruction.

The third technique is IWT, which helps to reduce the computational overhead. There are many conventional data hiding techniques such as DWT, DCT, LSB, MSB, and many more. However, among all these techniques IWT is chosen because of its intrinsic properties. Some of the features of IWT are listed as follows [22]:

- IWT scheme permits fast implementation of wavelet transforms with half the calculation time as compared to standard hiding techniques.
- IWT works on integer numbers so takes very less time to compute the coefficients.
- It analyzes the input signal at different frequencies with varying resolutions known as multi-resolution analysis.
- It also allows reversible IWT as compared to conventional DWT which presents errors because of floating-point processes.
- It can efficiently reconstruct the original signal because of lossless compression and its integer nature.
- It analyzes discontinuity and sharp spikes in the signal.
- It works equally in the time and frequency domains, and in the time domain discontinuities, can be analyzed easily.

Despite various traditional compression techniques such as LZW, PNG, Run-length encoding, and many more. JPEG compression is chosen because of its intrinsic features. It is the very first international standard for the compression of images. It is used widely these days and provides lossy compression. It can store and transmit information efficiently. It decomposes the image into blocks and represents it in the form of a matrix. The pixel intensity varies from 0 to 255 [23].

First of all, it converts the image into the YIQ or YUV color space. Y represents the illumination value and UV represents the color of the image. The second step is the sampling in the form of blocks of 8 × 8 or 64 × 64 and so on. Blocks are subjected to DCT transform. With DCT transform, the value of coefficients is calculated. The next step is quantization and in its actual compression takes place. The unwanted values are ignored at this step. AC and DC coefficients are calculated during the quantization process. DC coefficients carry no useful information, and these coefficients can be ignored. The process of image compression is known as encoding. For getting the original image, back process of decoding takes place. JPEG is the lossy compression so during decoding, the quality of the image may degrade to some extent. Some of the important features of JPEG compression are as follow [24,25]:

- It is an interactive visual compression process.
- It provides a multi-document interface for time enabling users to view and compare compression parameters.
- It carries a compression slider for both illumination and color value.
- It can crop unnecessary parts of the image.
- It has graphic detail quality equalizer to provide flexibility in compression.
- JPEG format is compatible with almost all image processing applications.
- It is a portable and widely used format.
- It finds the heterogeneous areas in the image and compresses those parts of the image as human eyes are extra sensitive to the variations in homogenous areas as equated to the heterogeneous area.
- It works on chrominance information in the image as the human eyes perceive changes in brightness more sharply.

Concealing and Retrieval Algorithm

The concealing and retrieval process of the secret message is shown in the Algorithm 1. IWT can decompose the given signal up to N- levels. N is the length of the given signal. Every time during decomposition IWT eliminates the noise from the signal and calculates the refined part of the signal as well. Noisy parts of the signal are used for embedding secret information. In the given algorithm, the input is taken in the form of secret image and cover video file. The file is decomposed into frame using OpenCV. Some of the suitable frames are selected to hide the secret message randomly. On the other side, JPEG compression is applied on secret image so that the concealing capacity can be improved. JPEG compression work on the chrominance information so that changes are not visible to the third person.

Algorithm 1 *IWT*

```
Input: cover_video, extract_frame, secret_image
Output: steg_video
temp_video←copy(cover_video); //copy cover video
temp_img←copy(secret_image); //copy secret image
[frm, n]←extract_frame using OpenCV(temp_video); //extract frames from video
[LL, LH, HL, HH]←JPEG Compression (temp_img); //apply JPEG compression on image
Initialize i = 1, j = 1, k = 1, count = 4;
fori = 1 to count
frame_HH[i]←IWT (frm[i]);
end for
len = column_LL × row_LL;
embed (frame_HH [], len);
i←i + count;
Do
frame_HH[i]←IWT (frm[i]);
embed(frame_HH[i], LL [j, k]);
updatei←i + 1;
if (k < max(column_LL)
update k←k + 1;
else
update j← j + 1; k = 1;
while((i ≤ n) AND(j ≤ max(row_LL)); // frames exhausted or message completely embedded
steg_video←build_video(frm); //construct video to transmit
```

IWT do the actual embedding of secret message before that secret message is decomposed into binary values. Then these values are embedded randomly into frames. The process repeats itself until the complete secret message is not embedded in cover frames. After the embedding of the complete secret message stego file is created, the stego file travels through the web to the destination.

Retrieval of the secret message is done on the receiver side. For retrieval of secret messages, the reverse process of information embedding takes place. The complete secret message is retrieved because of the integer and reversible nature of the IWT technique. IWT helps in fast calculation resulting into low cost and high robustness. JPEG compression also provides the high concealing capacity and good visual quality of stego file.

4. Experimental Setup

The proposed IWT technique is implemented in MATLAB for analysis and validation of experimental results. MATLAB is an encoding and numeric computing platform widely used by researchers to analyze information, build algorithms, and generate models. It is compatible with Windows and requires a minimum of 4 GB RAM. The image acts as secret information and the video acts as a cover for the proposed work. More than one video is taken as a cover file and Lena's image is taken as a secret image every time. Lena is a standard image, widely used in many image processing applications. The detail of the videos taken as the cover file is as follow in Table 2:

Table 2. Detail of Cover Video.

Video	Video Size in Second	Frame Rate	Aspect Ratio	Total Number of Frames	Frame Height	Frame Width	Data Rate	Bit Rate
Video 1	18	27	4:3	534	470	810	2437	2,453,551
Video 2	20	31	3:3	637	488	812	2166	2,256,343
Video 3	30	52	20:16	1910	255	349	235	225,436

All the videos have different properties such as size, frame rate, aspect ratio, the total number of frames, frame height, frame width, data rate, bit rate, etc. with the change in properties of cover video files value of performance matrices also varies. We have taken three different videos to validate our experimental results. Same secret image Lena is embedded in all the three different videos to analyse the experimental results.

Commonly used performance metrics for evaluation of research work are explained below:

PSNR: It is the performance metric used to check the excellence of the research work. It can be demarcated as the relation between the maximum possible powers of the original signal to the power of distorted noise. PSNR value is calculated in dB. PSNR value higher than 35 db represents the good visual quality of the stego file [26].

MSE: It is the amount of error present between the original and carrier file. A small difference between the original and stego file means no error is present. It can be calculated in MATLAB by using a built-in function [27]. It is calculated in dB^2.

SSIM: It is used to find the resemblance between the original and stego file. It is more efficient compared to PSNR and MSE matrices. It is the full reference metric, in other words, the measurement or prediction of image quality is based on an initial uncompressed reference. Its value varies from 0 to 1. '0' represents the poor quality of the stego file and '1' represents the excellent quality of the stego file [26].

CC: It measures the strength of the relationship between the original and the stego file. Its value varies from 0 to 1. Zero value represents the strongest relationship or no statistical change in two files. Value 1 represents a weak relationship or exposure of secret information [20,27].

5. Analysis and Discussion of Experimental Results

The experimental results are discussed on the bases on imperceptibility, robustness, complexity, cost effectiveness, and comparison with existing work. Imperceptibility means measuring the quality of stego file using different evaluation parameters. Whether the secret message can be exposed or not using some attacks, measures the robustness of the technique. We also discussed concealing capacity and total time taken by the technique. Cost effectiveness of the proposed technique is also discussed. Lastly, a comparison of the proposed work is done with some existing techniques. For comparison, we have selected two papers: one for comparing imperceptibility and robustness, and the second paper is used to compare the complexity of work in terms of time and concealing capacity.

5.1. Analysis of Imperceptibility and Robustness

The imperceptibility check is done through evaluation parameters PSNR, MSE, CC, and SSIM. By applying different attacks such as gamma correction and Gaussian attacks, the robustness of the proposed work is tested. In this section, attacks are applied on the stego image to expose the hidden secret information. Then, after the attacks, the PSNR, MSE, SSIM, and CC values are calculated for stego and original cover file which help to find the imperceptibility of the technique.

i. Gamma Correction Attack

It works on the luminance value of the input image. As luminance value of the input does affect the excellence of the image. This attack includes compression as well as expansion of input image to expose the hidden secret data. Less than 1 value of γ represents a compression of the input image. Greater than 1 value of γ represents the expansion of the input image as shown in Equation (2) [28]:

$$V_{out} = AV_{in}^{\gamma} \tag{2}$$

where V_{out} is the output image, V_{in} is the input image, A is a constant, and it is generally taken as 1.

Table 3 shows the effect of gamma correction attack on stego frame, retrieved secret image, and retrieved cover image. There is a slight variation in the quality of the cover file and stego file. Large is the difference between cover and stego file quality more are the chances of detection of secret information.

Table 3. Gamma Correction Attack.

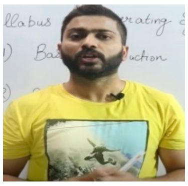
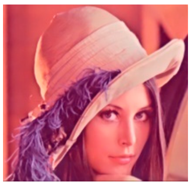
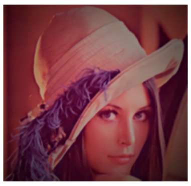
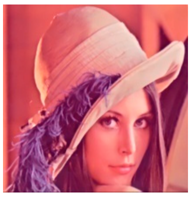
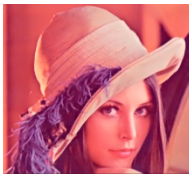
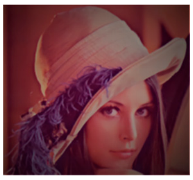
	Video Cover Frame	**Secret Image**	**Stego Frame**	**Retrieved Secret Image**	**Retrieved Cover Frame**
Gamma Correction Attack					
					
					

Table 4 expresses the value of performance metrics of the stego file for gamma correction attack. The average value of PSNR is calculated as 55.2 dB, the average value of MSE is 0.228 dB^2, the average value of SSIM is 0.77, and the average value of CC is 0.95. The lower value of MSE means less is the error present between original and stego file. Higher value of PSNR, CC and SSIM represent good quality of stego file. High value of these three parameters means a lower chance of exposure of secret message.

Table 4. Performance Metrics for Gamma Correction.

	PSNR	**MSE**	**SSIM**	**CC**
Gamma Correction Attack	52.6	0.282	0.69	0.93
	55.3	0.203	0.78	0.95
	57.7	0.189	0.86	0.97

ii Gaussian Noise Attack

It is a random variation of brightness or color information of the image. It arises during the attainment of input signal due to poor brightness, high temperature, and transmission. It can be reduced by applying the spatial filter. Equations (3) and (4) represent the Gaussian attack [27]:

$$p(z) = \frac{1}{\sqrt{2\pi\sigma}} e^{-(z-\mu)2/2\sigma^2} \tag{3}$$

$$\int_{-\infty}^{\infty} p(z)dz = 1 \tag{4}$$

where z is the gray level, μ is the mean of z, σ is the standard deviation, $\sigma 2$ is the variance, $p(z)$ is the probability density function.

Table 5 shows the effect of Gaussian noise attack on stego frame, retrieved secret image, and retrieved carrier image. Greater the alteration between the carrier and the stego image, the higher the chances of detection of secret information.

Table 5. Gaussian Noise Attack.

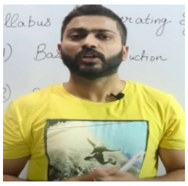
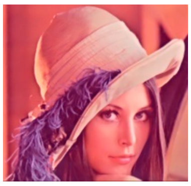
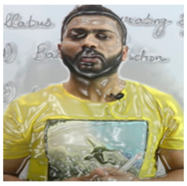
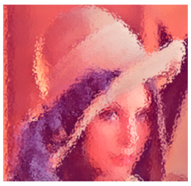
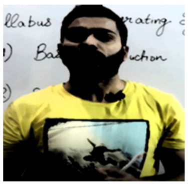
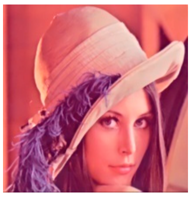
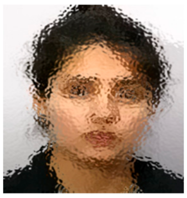
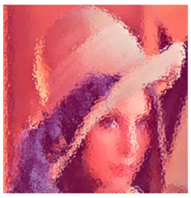
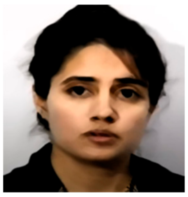
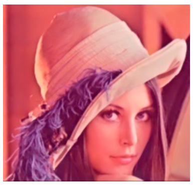
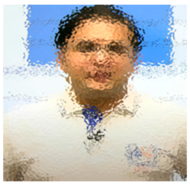
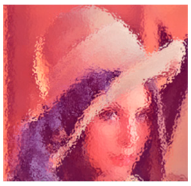
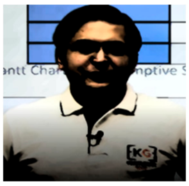
	Video Cover Frame	Secret Image	Stego Frame	Retrieved Secret Image	Retrieved Cover Frame
Gaussian Noise Attack					
					
					

Table 6 represents the value of performance metrics of the stego files Gaussian noise attack. The values of performance metrics represent the quality of research work. The average value of PSNR is calculated as 55.3 dB, the average value of MSE is 0.224 dB^2 the average value of SSIM is 0.88 and the average value of CC is 0.88. We tried Gaussian attack to expose the secret message in this part. Value of the performance metrics represent the robustness of proposed work. It has been concluded from the result that even after applying Gamma correction and Gaussian attacks, we are not able to extract the hidden secret message.

Table 6. Performance Metrics for Stego File.

	PSNR	MSE	SSIM	CC
Gaussian Noise Attack	53.3	0.301	0.81	0.82
	55.8	0.280	0.89	0.90
	57.5	0.221	0.93	0.94

5.2. Complexity Analysis

The complexity of the research work is calculated depending on the concealing and retrieval time of secret information. For complexity, we have also calculated the concealing capacity of the work. Concealing time is the quantity of time essential to hide secret data. Retrieval time is the amount of time required to retrieve the hidden secret data from the carrier file. Concealing capacity is how much data can be concealed in the cover file without the chances of exposure of secret data.

The amount of time varies with the format and type of multimedia file we are concealing. Time also varies with the format cover file. For hiding a 64 × 64 image, whose size is 20 KB, the proposed technique takes a time of 21 s. For retrieval of secret information, it has taken a time of 5 s. Concealing capacity is calculated to be 34 BPS. In the case of mp4 videos, concealing and retrieval time is found to be low as compared to any other format of video.

5.3. Cost Effectiveness

IWT scheme permits fast implementation of wavelet transforms with half calculation time as compared to standard hiding techniques. IWT works on integer numbers so takes very less time to compute the coefficients. It analyzes the input signal at different frequencies with varying resolutions, known as multi-resolution analysis. It also allows reversible IWT as compared to conventional DWT which presents errors because of floating-point processes. It can efficiently reconstruct the original signal because of lossless compression and its integer nature. It analyzes discontinuity and sharp spikes in the signal. It works equally in the time and frequency domains, and in the time domain discontinuities, can be analysed easily. It is cost efficient because of its integer nature and simpler hardware requirements.

5.4. Comparison with Existing Work

The comparison of the proposed work is done with the existing work [29]. For comparison, we have selected some parameters such as PSNR, MSE, SSIM, and CC (Concealing Capacity). These parameters help to find the trade-offs between concealing capacity, robustness, and imperceptibility.

For the proposed work, values of evaluation, parameters are found to be somewhat higher than the existing work as shown in Figure 8. PSNR for the proposed work is calculated as 61.3 and for the existing work is calculated as 54.89. The MSE of the proposed work is almost half of the existing work. SSIM is calculated as 0.98. Concealing capacity is found to be 18.79% which is very high compared to the existing work.

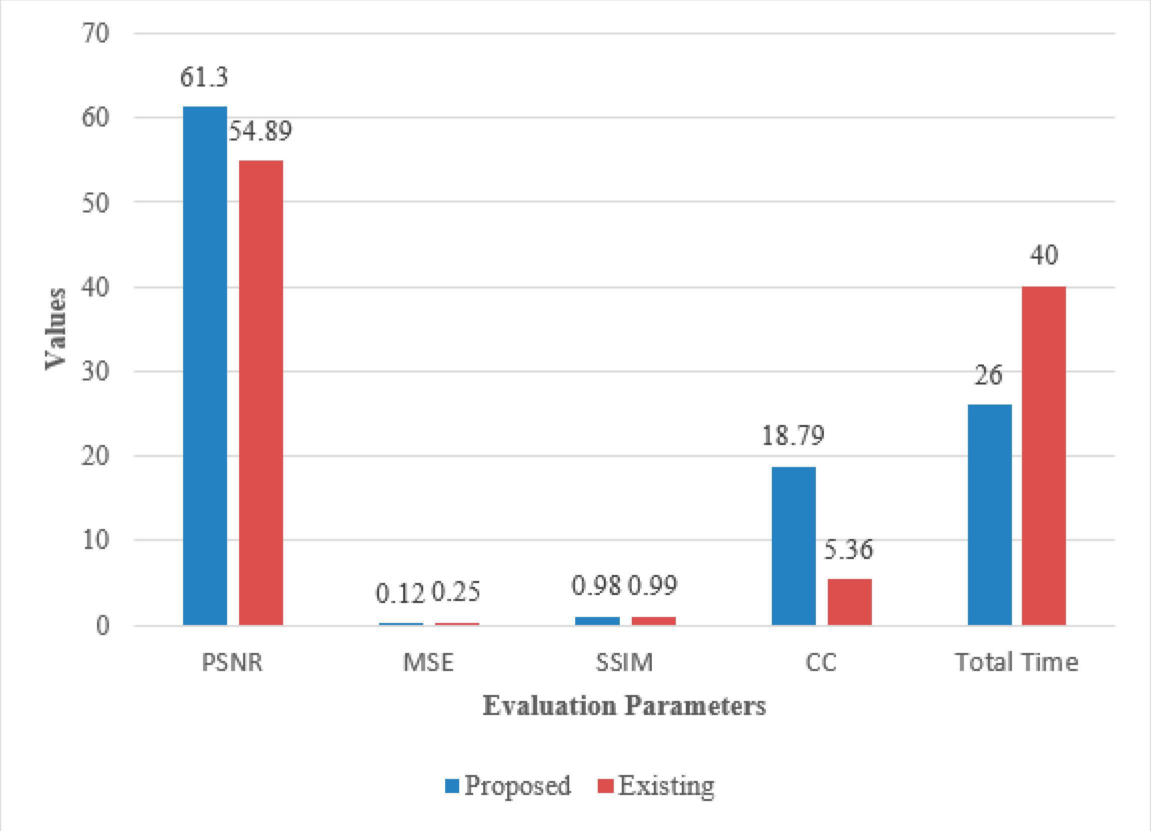


Figure 8. Comparison Chart.

In Figure 8, comparison of total time taken to conceal and retrieve the secret message is also done. Along with that size of secret message hidden is also compared with work in paper [29]. We have embedded and retrieved a secret message of size 20 KB in 26 s. Form the comparison it has been concluded that the proposed work achieved good concealing capacity in less time. It also proved the cost effectiveness of the proposed work.

6. Conclusions and Future Scope

Currently, steganography techniques are most commonly used for the security of personal information. However, these techniques have many issues associated with them. Some of the most common issues with these techniques are low concealing capacity, poor visual quality of the stego file, and robustness against attacks. IWT along with JPEG compression-based video steganography technique is used in this paper to overcome the mentioned issues. Video cover file help to improve concealing capacity whereas IWT help to improve robustness and visual quality. The robustness of the proposed work is checked through Gaussian and gamma correction attacks. SSIM, MSE, PSNR, and CC are calculated for imperceptibility check. For complexity, we calculated the concealing and retrieval time of the proposed work. Concealing capacity is calculated as 34 BPS. A comparison of the proposed work is also done with the existing work.

Due to the growth of advanced technologies, security of online transmission of information is becoming more difficult. Moreover, there are users which are not aware about new technologies. Many smart hackers are also there, who are much more aware of the advanced technologies. So, the huge gap between the skills of hackers and innocent users makes the requirement of safe online communication more aspirational as well as demanding. Still there are many issues which are associated with steganography techniques. The proposed research work could be extended with some encryption techniques, which will provide more security but at the same time complexity can be increased.

Author Contributions: Conceptualization, R.T. and U.P.; methodology, M.Z.; writing—original draft preparation, U.P.; writing—review and editing, R.T.; supervision, A.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Petitcolas, F.A.P.; Anderson, R.J.; Kuhn, M.G. Information hiding—A survey. *Proceeding IEEE* **1999**, *87*, 1062–1078. [CrossRef]
2. Maria, K.A.; Alia, M.A.; Alsarayreh, M.A.; Maria, E.A. UN-Substituted Video Steganography. *KSII Trans. Internet Inf. Syst. (TIIS)* **2020**, *14*, 382–403.
3. Jeevitha, S.; Amutha Prabha, N. A comprehensive review on steganographic techniques and implementation. *ARPN J. Eng. Appl. Sci.* **2018**, *13*, 4780–4791.
4. Amirtharajan, R.; Rayappan, J.B.B. Steganography-time to time: A review. *Res. J. Inf. Technol.* **2013**, *5*, 53–66. [CrossRef]
5. Hassaballah, M.; Hameed, M.A.; Awad, A.I.; Muhammad, K. A novel image steganography method for industrial internet of things security. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7743–7751. [CrossRef]
6. Ghazal, T.; Hasan, M.K.; Alshurideh, M.T.; Alzoubi, H.M.; Ahmad, M.; Akbar, S.S.; Akour, I.A. IoT for smart cities: Machine learning approaches in smart healthcare—A review. *Future Internet* **2021**, *13*, 218. [CrossRef]
7. Osman, B. Capacity Performance of Steganography Method in Text-Based Domain Multi-Binary Scheme Representation on Text Steganography Technique View Project Spatial Multiplexing and Multi-Mode Fiber Communication View Project. Available online: https://www.researchgate.net/publication/282279208 (accessed on 13 March 2021).
8. Shirali-Shahreza, M.H.; Shirali-Shahreza, M. A new approach to Persian/Arabic text steganography. In Proceedings of the 5th IEEE/ACIS International Conference Computer Information Science, ICIS 2006. Conjunction with 1st IEEE/ACIS, International Workshop Component-Based Software Engineering, Software Architecture Reuse, COMSAR 2006, Honolulu, HI, USA, 10–12 July 2006; Volume 2006, pp. 310–315. [CrossRef]

9. Kumar, P.M.; Shunmuganathan, K.L. Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate. *Inf. Secur. J.* **2012**, *21*, 65–70. [CrossRef]
10. Zehra, N.; Sharma, M.; Ahuja, S.; Bansal, S. Bio-Authentication Based Secure Transmission System using Steganography. *arXiv* **2010**, *8*, 318–324. Available online: http://arxiv.org/abs/1005.4264 (accessed on 29 June 2022).
11. Mishra, S.; Yadav, V.K.; Trivedi, M.C.; Shrimali, T. Audio steganography techniques: A survey. *Adv. Intell. Syst. Comput.* **2018**, *554*, 581–589. [CrossRef]
12. Muyco, S.D.; Hernandez, A.A. A modified hash based least significant bits algorithm for steganography. In Proceedings of the 2019 4th International Conference on Big Data and Computing, Guangzhou, China, 10–12 May 2019; pp. 215–220. [CrossRef]
13. Kaur, M.; Gupta, S.; Sandhu, P.S.; Kaur, J. A dynamic RGB intensity based steganography scheme. *World Acad. Sci. Eng. Technol.* **2010**, *43*, 833–836.
14. Sabeti, V.; Sobhani, M.; Hasheminejad, S.M.H. An adaptive image steganography method based on integer wavelet transform using genetic algorithm. *Comput. Electr. Eng.* **2022**, *99*, 107809. [CrossRef]
15. Pilania, U.; Tanwar, R.; Gupta, P. An ROI-based robust video steganography technique using SVD in wavelet domain. *Open Comput. Sci.* **2022**, *12*, 1–16. [CrossRef]
16. Yassin, N.I.; El Houby, E.M. Image Steganography Technique Based on Integer Wavelet Transform Using Most Significant Bit Categories. *Int. J. Intell. Eng. Syst.* **2022**, *15*, 499–508.
17. Chakraborty, R.; Roy, A. Audio Steganography—A Review. *Int. J. Trend Res. Dev.* **2019**, *6*, 144–149.
18. Yadav, S.K.; Bhogal, R.K. A video steganography in spatial, discrete wavelet transform and integer wavelet domain. In Proceedings of the 2nd International Conference Intelligence Circuits System ICICS 2018, Phagwara, India, 20–21 April 2018; pp. 265–270. [CrossRef]
19. Jambhekar, N.D.; Dhawale, C.A.; Hegadi, R. Performance analysis of digital image steganographic algorithm. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, Jaipur, India, 14–16 November 2014. [CrossRef]
20. Prabakaran, G. A High Capacity Video Steganography Based on Integer Wavelet Transform. *J. Comput. Appl.* **2015**, *5*.
21. Sukumar, A.; Subramaniyaswamy, V.; Vijayakumar, V.; Ravi, L. A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage. *Multimed. Tools Appl.* **2020**, *79*, 10825–10849. [CrossRef]
22. Valandar, M.Y.; Ayubi, M.J.B.P.; Aghazadeh, M. An integer wavelet transform image steganography method based on 3D sine chaotic map. *Multimed. Tools Appl.* **2019**, *78*, 9971–9989. [CrossRef]
23. Singh, S.; Singh, A. A Review on the Various Recent Steganography. *IJCSN Int. J. Comput. Sci. Netw.* **2013**, *2*, 2277–5420.
24. Akbar, F.C.; Purboyo, T.W.; Latuconsina, R. A Study of Text Steganography Methods. *J. Eng. Appl. Sci.* **2019**, *15*, 369–372. [CrossRef]
25. Shirali-Shahreza, M.; Shirali-Shahreza, M.H. Text Steganography in SMS. In Proceedings of the 2007 International Conference on Convergence Information Technology (ICCIT 2007), Gyeongbuk, Korea, 21–23 November 2007; pp. 2260–2265. [CrossRef]
26. Hashim, M.M.; Rahim, M.S.M.; Johi, F.A.; Taha, M.S.; Hamad, H.S. Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *Int. J. Eng. Technol.* **2018**, *7*, 3505–3514. [CrossRef]
27. Zaric, A.; Loncaric, M.; Tralic, D.; Brzica, M.; Dumic, E.; Grgic, S. Image quality assessment—Comparison of objective measures with results of the subjective test. *Proceeding Elmar Int. Symp. Electron.* **2010**, *2014*, 113–118.
28. Roy, S.; Pal, A.K. A Hybrid Domain Color Image Watermarking Based on DWT–SVD. *Iran. J. Sci. Technol. Trans. Electron. Eng.* **2019**, *43*, 201–217. [CrossRef]
29. Dalal, M.; Juneja, M. A secure and robust video steganography scheme for covert communication in H. 264/AVC. *Multimed. Tools Appl.* **2021**, *80*, 14383–14407. [CrossRef]