Securing Data: A Study on Different Transform Domain Techniques

SAUGATA DUTTA
Research Scholar, Galgotias University,
Greater Noida, Uttar Pradesh, INDIA

KAVITA SAINI
Associate Professor, Galgotias University,
Greater Noida, Uttar Pradesh, INDIA

Abstract: Steganography is a technology which is utilized in securing information through hiding data over another data which can be stored or passed over public network without a clue that secret data is hidden in the cover medium. This article focus on securing and hiding the data through transform domain techniques used in Image, Audio and Video steganography. The review study throws light on the algorithm and properties of transform domain techniques and its benefits to utilize in securing data. Parameters such as imperceptibility, capacity and robustness are evaluated for discrete cosine transform (DCT) and discrete wavelet transform (DWT).

Key-words—Steganography; Discrete cosine transform; Discrete Fourier Transform; Discrete Wavelet Transform; Network security; Secure Communication

Received: August 26, 2020 . Revised: November 16, 2020. Accepted: January 15, 2021.
Published: January 22, 2021.

1. Introduction

Steganography is a technique of hiding information into some medium such that the information can be passed on to the intended recipients without a clue to the public. The technique of steganography is nothing new, this had been used since ancient times. The first recorded used of this term was in 1499 by Johannes Trithemius, which was a book "Steganographia" on cryptography and steganography hidden as a book on magic [1]. There were other different techniques on steganography such as using invisible ink, wax tablet, microdots etc. In Modern times, with the inception computer age, the techniques of steganography had changed as against the earlier.

There is a difference between cryptography and steganography wherein cryptography, it is understood that the information is protected by some algorithm as sent over the communication channel where as in steganography the information is hidden in a cover medium and passed on to the communication channel without a clue for the existence of the hidden data. Steganography is of different types such as text, image, audio and video. These techniques includes, spatial domain techniques where the data is hidden with the strength of the pixel. As the data is embedded, the value of the pixel is changed. In Spread Spectrum Technique, data is hidden in the frequency with a wide bandwidth. In Statistical technique, the property of the cover is changed to hide the data. In Transform domain technique, data is hidden in the frequency domain. In Distortion technique, the signal is distorted to hide the data. When data is hidden by marking an image, it is known as masking and filtering technique. This paper studies about transform domain techniques used primarily. It discusses in details about the transform domain techniques and algorithm used. Firstly, we will start with the general algorithm and flow chart of simple steganography data hiding terminology.

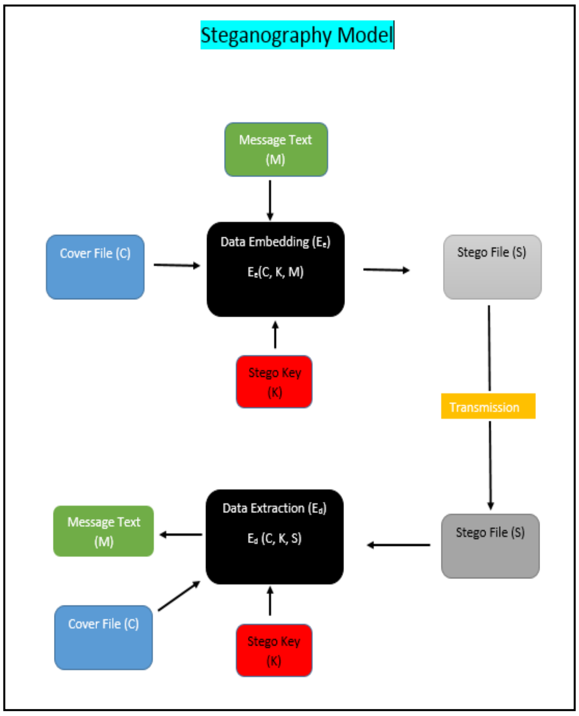

Figure 1: Basic steganography model

In steganography data embedding is done by hiding the Message text (M) with the Cover file (C) and Stego Key (K) generating a Stego file (S). The Stego file (S) is then transmitted through some communication channel at the destination end. Message Text (M) is then extracted at the destination end after a data extraction algorithm (D) performed in the Stego file (S).

Let the embedding process be "e" and "d" as an extraction process. The representation of embedding and extraction of data is as follows:

$\mathbf{E_e (C, K, M) \rightarrow S}$

$\mathbf{E_d(C, K, S)} \approx \mathrm{M}$

2. Review Litreature

Diptasree Debnath et al. explores image steganography techniques founded on Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) where numerous images can be hidden with increased quality and greater capacity. The exploration results also points its capability of withstanding various steganalysis attacks. [2].

Farah Qasim Ahmed Alyousuf et al. presents image steganography techniques used with Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) where it analyses various performances metrics which primarily uses Least Significant Bit (LSB) in spatial domain while in transform domain it uses differentiated between DCT and DWT. The result of the paper shows spatial domain technique is a better tool for embedding due to its performance and better capacity [3].

Srushti S Yadahalli et al. compares both Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT) method in image steganography evaluating various significant parameters. The result shows that DWT is less vulnerable to attacks and distortion including better performance [4].

Meenu Suresh et al. proposes algorithm for video steganography using single level discrete wavelet transform which decomposes frames into RGB channels. Data is grouped in three data matrices and data is embedded in each matrices. Diagonal, approximation and embedded coefficients are used for reconstruction of stego video. The result yields better security and video quality [5].

M. K. Oudah et al. explores the improvement in steganography technique using Discrete Wavelet Transform (DWT) which separates the signal to frequency components. The message is hidden in suitable frequency bands and the result shows High Peak Signal to Noise Ratio (PSNR) when increasing the DWT level and has better imperceptibility performance [6].

Laxminarayan Gahalod et al. surveyed a 3-level DWT image watermarking technique using Alpha blending Technique where the watermark is embedded into the cover image which can be recovered with the extraction technique. The Observation states that the watermark image quality depends on the scaling factor whereas extracted watermark is not dependent of the scaling factor. It also shows that the recovered watermark and images are better for 3-level DWT as compared against the 1-level DWT and 2-level DWT [7].

Amir Massoud Bidgoli et al. Proposed improved Capacity, Security and Robustness parameters in color image steganography with a Joint and Integrated method based on Discrete Wavelet Transform (DWT). As a first step the secret message is processed with format homogenization, compression and eliminating redundancies by using the Huffman and differential algorithms. Cover image is chosen and DWT is applied on the blue channel as against the red because red plane is more human eye sensitive. Complimentary algorithm is used to embed the hidden message in the HH sub-band. The PSNR values are higher as compared to other techniques and achieved the three parameters of Robustness, Capacity and Security [8].

Latifah Uswatun Hasanah et al. reviewed the audio data concealment and advantage of steganography where a file can be transferred from source to destination end without raising any suspicion while secret message embedded into it. It is found that the technique is better and efficient for information hiding. Media that has been inserted a secret message will not resize the file significantly [9]

Tanusree Podder et al. proposed algorithms that hides the key which increases the stego image quality as against hiding the secret image. The PSNR values are high which depicts that the stego image is of high quality. Through the Block Matching technique secret image is extracted from the stego image with the help of the key without hiding any information on it [10].

3. Transform Domain Techniques

This is a technique which transforms the pixel from time domain to frequency domain. An Image in a digital form is basically a collection of pixels. The edge pixels are known to have high frequency whereas non edge pixels are known to be low frequency pixels. There are various techniques in transform domain such as IWT (Integer Wavelet Transform), Haar Transform, Discrete Curvelet Transform (DCVT), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform). Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) are commonly used. As Spatial domain techniques changes bits in the pixel value while hiding data but there is a difference between transform domain technique and spatial domain technique. Transform domain technique is more robust and better than spatial domain as it hides data on those parts where it is not effected by cropping, compression and some other forms of image processing techniques.

4. Mathematical Prefaces of Transform Domain Techniques

4.1 Discrete Fourier Transform (DFT)

A French Mathematician named Joseph Fourier in early 1800 introduced continuous time periodic signals known as Fourier series. The Signal can be broken into weighted sum of complex exponentials. The frequency content of the signal is represented by this weighted sum known as the spectrum. A signal spectrum becomes continuous when the signal becomes non periodic and the period becomes infinite. In Fourier transform, an image is decomposed into orthogonal function where the spatial intensity is transformed to frequency domain. For a two dimensional fourier transform, let f(x,y) – Spatial domain image and let F(u,v) – Frequency domain transformed image. A 2D DFT general equation is as follows:

$$F(u,v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\exp\left[-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right],$$

Where u = 0, 1, 2..., M-1 and v = 0, 1, 2.., N-1

Figure 2: General 2D DFT Equation [11]

The inverse DFT can be represented as

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)\exp\left[j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right],$$

Where x= 0,1,2...., M-1 and y=0,1,2... N-1

Figure 3: General 2D DFT Inverse Equation [11]

4.2 Discrete Cosine Transform (DCT):

The Fourier transform was originally used on heat conduction but later gain usage in various applications and became a base for other transformation like DCT. Images and videos compression algorithm uses DCT to transform into frequency domain and data compression is done through quantization. Image is divided into parts or sub-bands. DCT transformation (2D), let f(x,y) - Spatial domain image and F(u,v) - Frequency domain image. A 2D DCT general equation is as follows:

$$F(u,v)=C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{(2x+1)u\pi}{2N}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right),$$

where if $u=v=0$, $C(u)=C(v)=\sqrt{\frac{1}{N}}$; otherwise, $C(u)=C(v)=\sqrt{\frac{2}{N}}$.

The inverse DCT can be represented as

$$f(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}C(u)C(v)F(u,v)\cos\left(\frac{(2x+1)u\pi}{2N}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right).$$

Figure 4: General 2D DCT and Inverse Equation [11]

For Expressing 2D DCT there is a more convenient method through matrix F=MfM^T and the inverse DCT is f=M^{T}FM where F and f are denoted as 8 x 8 matrix. The coefficients referenced are abundancy of all cosine waves which are utilized to create the original signal in the opposite process. These transformation properties are found to be inherited to Fourier cosine transform.

$$M=\begin{bmatrix}
\frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} \\
\frac{1}{2}\cos\frac{1}{16}\pi & \frac{1}{2}\cos\frac{3}{16}\pi & \frac{1}{2}\cos\frac{5}{16}\pi & \frac{1}{2}\cos\frac{7}{16}\pi & \frac{1}{2}\cos\frac{9}{16}\pi & \frac{1}{2}\cos\frac{11}{16}\pi & \frac{1}{2}\cos\frac{13}{16}\pi & \frac{1}{2}\cos\frac{15}{16}\pi \\
\frac{1}{2}\cos\frac{2}{16}\pi & \frac{1}{2}\cos\frac{6}{16}\pi & \frac{1}{2}\cos\frac{10}{16}\pi & \frac{1}{2}\cos\frac{14}{16}\pi & \frac{1}{2}\cos\frac{18}{16}\pi & \frac{1}{2}\cos\frac{22}{16}\pi & \frac{1}{2}\cos\frac{26}{16}\pi & \frac{1}{2}\cos\frac{30}{16}\pi \\
\frac{1}{2}\cos\frac{3}{16}\pi & \frac{1}{2}\cos\frac{9}{16}\pi & \frac{1}{2}\cos\frac{15}{16}\pi & \frac{1}{2}\cos\frac{21}{16}\pi & \frac{1}{2}\cos\frac{27}{16}\pi & \frac{1}{2}\cos\frac{33}{16}\pi & \frac{1}{2}\cos\frac{39}{16}\pi & \frac{1}{2}\cos\frac{45}{16}\pi \\
\frac{1}{2}\cos\frac{4}{16}\pi & \frac{1}{2}\cos\frac{12}{16}\pi & \frac{1}{2}\cos\frac{20}{16}\pi & \frac{1}{2}\cos\frac{28}{16}\pi & \frac{1}{2}\cos\frac{36}{16}\pi & \frac{1}{2}\cos\frac{44}{16}\pi & \frac{1}{2}\cos\frac{52}{16}\pi & \frac{1}{2}\cos\frac{60}{16}\pi \\
\frac{1}{2}\cos\frac{5}{16}\pi & \frac{1}{2}\cos\frac{15}{16}\pi & \frac{1}{2}\cos\frac{25}{16}\pi & \frac{1}{2}\cos\frac{35}{16}\pi & \frac{1}{2}\cos\frac{45}{16}\pi & \frac{1}{2}\cos\frac{55}{16}\pi & \frac{1}{2}\cos\frac{65}{16}\pi & \frac{1}{2}\cos\frac{75}{16}\pi \\
\frac{1}{2}\cos\frac{6}{16}\pi & \frac{1}{2}\cos\frac{18}{16}\pi & \frac{1}{2}\cos\frac{30}{16}\pi & \frac{1}{2}\cos\frac{42}{16}\pi & \frac{1}{2}\cos\frac{54}{16}\pi & \frac{1}{2}\cos\frac{66}{16}\pi & \frac{1}{2}\cos\frac{78}{16}\pi & \frac{1}{2}\cos\frac{90}{16}\pi \\
\frac{1}{2}\cos\frac{7}{16}\pi & \frac{1}{2}\cos\frac{21}{16}\pi & \frac{1}{2}\cos\frac{35}{16}\pi & \frac{1}{2}\cos\frac{49}{16}\pi & \frac{1}{2}\cos\frac{63}{16}\pi & \frac{1}{2}\cos\frac{77}{16}\pi & \frac{1}{2}\cos\frac{91}{16}\pi & \frac{1}{2}\cos\frac{105}{16}\pi
\end{bmatrix}.$$

Figure 5: General 2D DCT Inverse Equation [11]

4.3 Discrete Wavelet Transform (DWT):

DWT is a way to transform from spatial to frequency domain. DWT is used in JPEG 2000 compression which is very popular. Wavelets are basically functions that integrate to zero waving below and above the x axis. For Signal and image processing, wavelets are used as the basic function like sines and cosines in Fourier transform. These functions are gained by spreading and decoding mother wavelet ψ (x) by amount s and **τ**.

$$\Psi_{\tau,s}(x)=\left\{\psi\left(\frac{x-\tau}{s}\right),(\tau,s)\in R\times R^{+}\right\}.$$

Figure 6: Mother Wavelet [11]

Wavelet transform is localized in time and frequency allowed by translation and dilation. Wavelet basis functions in a more compact way can represent spikes and discontinuation. Continuous Wavelet Transform (CWT) is denoted as

$$cwt_{\psi}(\tau,s)=\frac{1}{\sqrt{|s|}}\int x(t)\Psi^{*}_{\tau,s}(t)dt,$$

where $\Psi^{*}_{\tau,s}$ is the complex conjugate of $\Psi_{\tau,s}$ and $x(t)$ is the input signal defined in the time domain.

Figure 7: Continuous Wavelet Transform (CWT)

For Inverse CWT is define, here *C* Ψ is a constant.

$$x(t)=\frac{1}{C^{2}_{\psi}}\int_{s}\int_{\tau}cwt_{\psi}(\tau,s)\frac{1}{s^{2}}\Psi_{\tau,s}(t)d\tau ds,$$

Figure 8: Inverse Continuous Wavelet Transform (CWT)

For a 2D signal, with the combination of 1D wavelet transform the 2D wavelet can be decomposed. In each of the dimensions of the image 1D transform can be applied separately. When using the quadrature mirror filters and image can be decomposed into wavelet coefficients. The images are divided into sub images when filters H and G are applied. G$_r$I contains high pass frequency information and H$_r$I contains low pass frequency information. Four sub images are obtained when filters are applied into column of two images. Sub images HcHrI (low-low), GcHrI (high-low), HcGrI (low-high) and GcGrI (high-high) stores information passes. Figure 9 shows the decomposition process. This process is followed repeatedly until the size of the sub image is reached to 1 x 1. It may not be essential for all conceivable decomposition until the size arrives at 1 x 1 as only a couple levels are adequate in light of the fact that as the greater part of features of the object can be extracted from them.

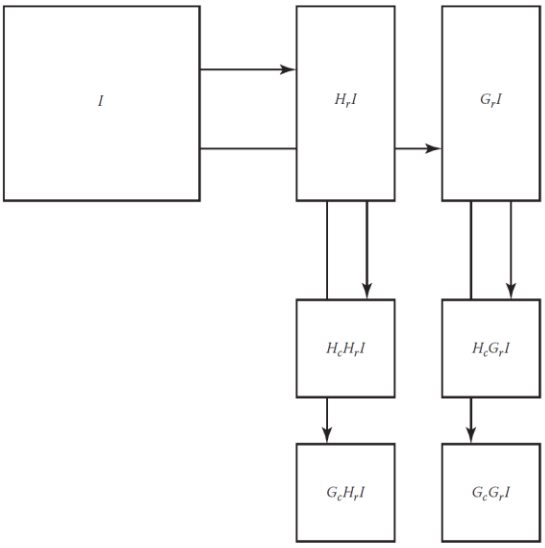

Figure 9: Wavelet decomposition of an image

5. Image Steganography in Transform Domain Technique

DCT and DWT are commonly used Image Transform domain technique. In DCT orthogonal transformation occurs for a signal into elementary frequency components. Image pixels are transformed from spatial to frequency domain using DCT techniques where error rate is less, compression ratio is high and more robust in terms of data loss. In DCT Image Steganography the image is separated into 8 x 8 blocks where two dimensional DCT is applied and selected coefficients is used for data hiding in the LSB of each DCT coefficients. The lower and higher frequency coefficients are in the upper left and lower right positions in the block.

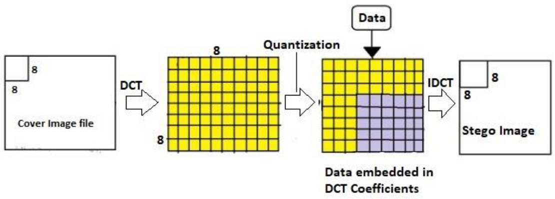

Figure 10: Data embedding using DCT

DWT processes non stationary signals and wavelets which are small waves and of shorter duration with varying frequency. Translation and Dilation of mother wavelets creates wavelets. Discrete wavelet transform (DWT) when used with image steganography for embedding text uses Haar DWT (HDWT). In 2D-HDWT there are two operations which is horizontal and vertical. As an initial step pixels are scanned from left to right horizontally where additions and subtractions are performed in corresponding pixels and the sum and difference are stored on left and right respectively. This process is repeated unless all pixels are reached. The pixels sum is represented as low frequency while the difference is represented as high frequency.

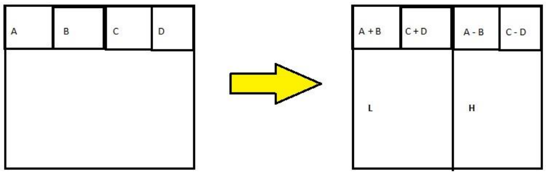

Figure 11: 2d-HDWT horizontal operations

Similarly, pixels are scanned from top to bottom vertically where additions and subtractions are performed in corresponding pixels and then sum and differences are stores in top and bottom respectively.

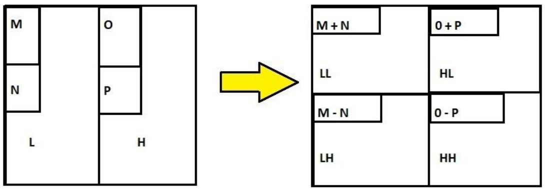

Figure 12: 2d-HDWT vertical operations

In this way four sub-bands are achieved as LL, HL, LH and HH. The LL contains harsh depiction of the image and it is gotten by low pass filtration in rows and columns. HH sub-band is obtained by both direction high pass filtration and have high frequency components. The HL and LH are the outcome of low pass filtration in one direction and high pass filtration in other direction.

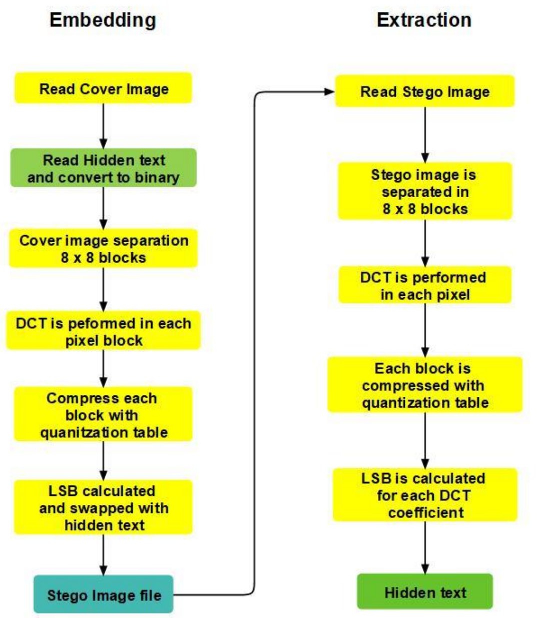
Embedding
Extraction
Read Cover Image
Read Hidden text and convert to binary
Cover image separation 8 x 8 blocks
DCT is peformed in each pixel block
Compress each block with quanitzation table
LSB calculated and swapped with hidden text
Stego Image file
Read Stego Image
Stego image is separated in 8 x 8 blocks
DCT is performed in each pixel
Each block is compressed with quantization table
LSB is calculated for each DCT coefficient
Hidden text

Figure 13: DCT based Image steganography flow

5.1 Algorithm of Image Steganography for text message embedding in DCT:

1. First Cover Image is read
2. Hidden message is read
3. Binary conversion of hidden message.
4. Cover Image is separated into 8 x 8 pixel blocks.
5. For each Pixel block DCT is performed.
6. Quantization table is used to compress each block.
7. LSB is calculated of each DCT coefficients and swapped with the hidden message.
8. Stego image is produced.

5.2 Algorithm of Image steganography for text message extraction in DCT:

1. First Stego image is read
2. Then next, through 8 x 8 block of pixels stego image is separated.
3. Then in each Pixel block DCT is performed.
4. Now after this step, quantization table is used to compress each block.
5. For each DC coefficient LSB is computed.
6. Convert each bits into character and retrieve the hidden message.

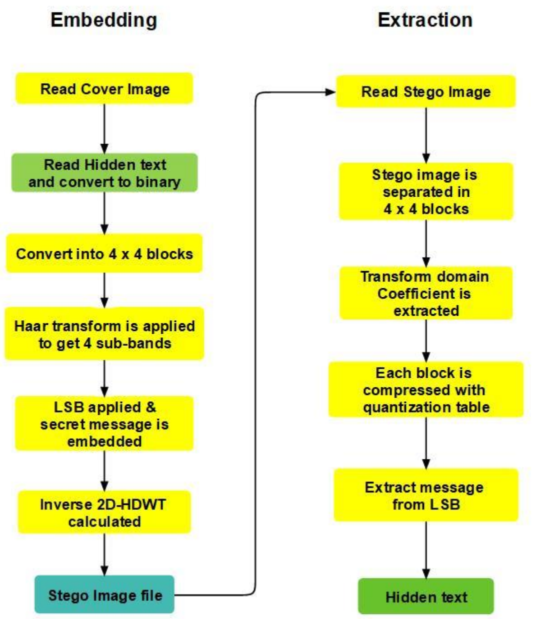
Embedding
Extraction
Read Cover Image
Read Hidden text and convert to binary
Convert into 4 x 4 blocks
Haar transform is applied to get 4 sub-bands
LSB applied & secret message is embedded
Inverse 2D-HDWT calculated
Stego Image file
Read Stego Image
Stego image is separated in 4 x 4 blocks
Transform domain Coefficient is extracted
Each block is compressed with quantization table
Extract message from LSB
Hidden text

Figure 14: DWT based Image steganography flow

5.3 Algorithm of Image steganography for text message embedding in DWT:

1. Cover Image is read.
2. The hidden message is read
3. Binary conversion of hidden message.
4. Convert the cover image into 4 x 4 blocks.
5. 2D-Haar transform is applied to get 4 sub-bands LL, HL, LH & HH.

6. LSB of each sub-band is changed and secret hidden message is embedded into it.
7. Inverse 2D-HDWT (Haar Discrete Wavelet Transform) is calculated for each 4 x 4 block.
8. Stego image is produced.

5.4 Algorithm of Image steganography for text message extraction in DWT:

1. The Stego image is read.
2. Stego image is divided into 4 x 4 blocks
3. Transform domain coefficient is extracted by using 2D Haar Discrete Wavelet Transform (HDWT) for each block.
4. Extract message from LSB in each pixel
5. Hidden message is extracted

6. Audio Steganography in Transform Domain technique

Audio steganography uses cover audio files which acts as a carrier to hide secret message. Using transform domain technique carrier audio file is transformed to from time to frequency domain. Audio steganography is tough against common signal processing attacks which includes filtering, noise addition, re-mastering and cropping. Using Discrete Cosine Transform (DCT), time domain is changed to frequency domain. DCT audio signal can work on one dimensional and two dimensional signals of audio. As a basic function, DCT uses cosine function of numerous wave numbers and work on real signals and spectral coefficients. DCT of a 1D or 2D sequence and reconstructing the original signal from its DCT coefficients is known as inverse DCT (IDCT). Low frequency signals are DC and high frequency signals are AC. Discrete Wavelet Transform (DWT) is a very common method for processing of image and compression of image. The audio signal is decomposed into components of approximation and detail coefficients (cA & cD) respectively by using wavelet transform. The approximation is known to be low frequency components as against the details coefficients which are higher frequency. The audio signal can be reconstructed with the help of approximation coefficients.

The process flow chart to embed and extract text message through DCT based audio steganography is mentioned below.

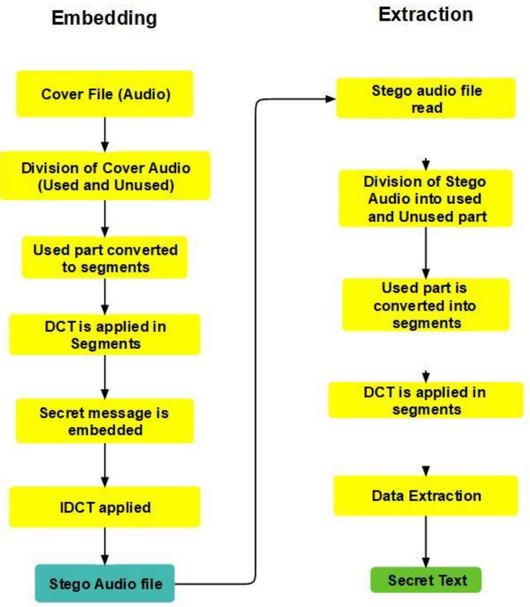
Embedding
Extraction
Cover File (Audio)
Division of Cover Audio (Used and Unused)
Used part converted to segments
DCT is applied in Segments
Secret message is embedded
IDCT applied
Stego Audio file
Stego audio file read
Division of Stego Audio into used and Unused part
Used part is converted into segments
DCT is applied in segments
Data Extraction
Secret Text

Figure 15: DCT based Audio steganography flow

6.1 DCT Based Audio Steganography to embed text message:

1. Cover audio file is read.
2. The cover signal is divided into two parts used and unused part respectively
3. The used part is utilized for data hiding and is converted into segments identical size of hidden message
4. DCT is applied on segments. Each segment has DC signal and AC signal
5. Secret message is implanted in contrast of two samples in a segment.
6. IDCT reconstructs the stego signal in virtue of changed AC samples and Unchanged DC samples
7. Stego audio file is constructed

6.2 DCT Based Audio Steganography to extract text message:

1. Stego audio file is read.
2. The stego signal is separated into two parts Used and Unused parts.
3. The used part is separated into segments equivalent to the size of the hidden message bit.
4. DCT is applied on each segment wherein each segment represents DC and AC signals
5. Data recovery is done in comparing two samples of segment.
6. Hidden message is extracted

The process flow chart to embed and extract text message through DWT based audio steganography is mentioned below.

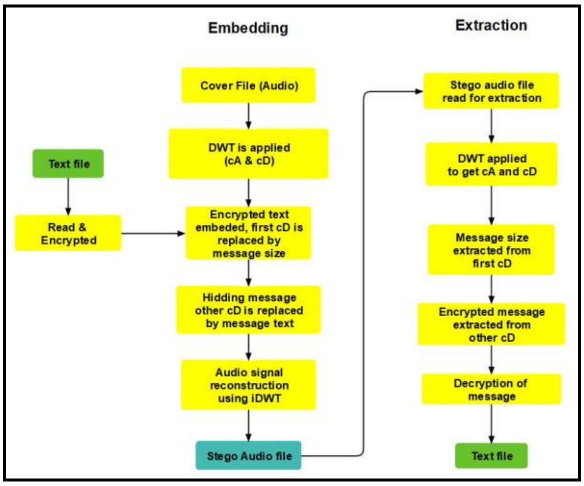
Embedding
Extraction
Text file
Read & Encrypted
Cover File (Audio)
DWT is applied (cA & cD)
Encrypted text embeded, first cD is replaced by message size
Hidding message other cD is replaced by message text
Audio signal reconstruction using iDWT
Stego Audio file
Stego audio file read for extraction
DWT applied to get cA and cD
Message size extracted from first cD
Encrypted message extracted from other cD
Decryption of message
Text file

Figure 16: DWT based Audio steganography flow

6.3 DWT Based Audio Steganography to embed text message:

1. Cover audio file is chosen and read to get the details for frequency and samples.
2. DWT matrix is applied on cover audio files which provides the approximation coefficients (cA) and detail coefficients (cD).
3. Text file is read and encrypted with size calculated in binary.
4. Encrypted text is embedded, where the size of the secret message is rooted because the encryption and decryption of the secret text is based on message size. Here the first cD coefficient is replaced by the size.
5. Hiding the actual message where the other cD coefficients is substituted by the encrypted message.
6. Stego Audio Signal is reconstructed using inverse DWT (IDWT) of approximate coefficient (cA) and detail coefficient (cD).

6.4 DWT Based Audio Steganography to extract text message:

1. Stego audio file is read to get the details for frequency and samples.
2. DWT is applied to get cA and cD
3. Message size can be acquired from the first cD coefficient.
4. Considering as much coefficients as the size of the encrypted message characters from the second cD coefficient.
5. Decryption of the secret text and writing to a file.

7. Video Steganography in Transform Domain Technique

Video steganography uses video files to hide secret message. Video steganography in transform domain transforms pixel from spatial domain to frequency domain. In easy language, a video is basically a collection of moving visual images. Hence a digital image is a collection of pixels which has low and high frequency components. The edge pixels or border pixels are high frequency pixels and non-border pixels are low frequency pixels. The embedding process rest on DCT coefficients in Discrete Cosine Transform (DCT). The DCT coefficients stores the hidden text message on Least Significant Bit (LSB) of cover video. If the DCT coefficient is greater than a benchmarked value the image is separated into low, medium and high frequency components. DCT is used widely in TV signals, radio signals, image and speech. Discrete Wavelength Transform (DWT) operates on horizontal and vertical wavelets and are sampled discretely. The image is divided into four sub-band coefficients. DWT coefficients are LL (low-low frequency – left top), HL (High-low frequency – right top), LH (Low-high frequency – left bottom) and HH (High-High frequency – right bottom).

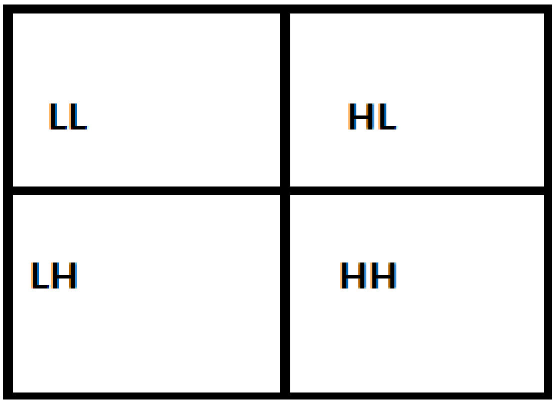

Figure 17: Sub-bands 2D-DWT

As a first step in horizontal direction pixels are scanned left to right. Calculations is performed like additions and subtractions on pixels which are adjacent. The sum are stored on left and on right variations are stored. This operation is repeated until all rows are processed.

The process flow chart to embed and extract text message through DCT based video steganography is mentioned below.

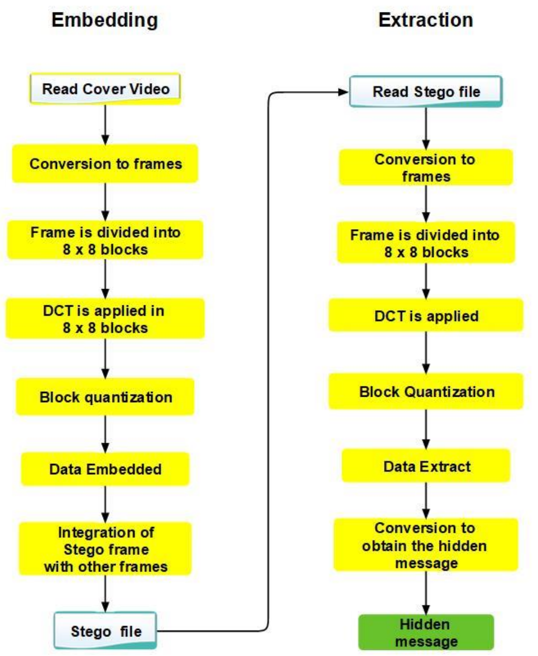

Figure 18: DCT based video steganography flow

7.1 Algorithm of video steganography for text message embedding using DCT:

1. Cover video is selected
2. Frames are extracted
3. Frames for hiding information is selected
4. Read hidden text
5. Frame is divided into 8 x 8 blocks
6. DCT is applied in 8 x 8 blocks which is also called Block DCT
7. Blocks are compressed with quantization table
8. LSB is computed from each Block DCT coefficient and replaced with the hidden text bits.
9. Integrate the stego frames with others frames and reconstruct the video
10. Stego video is constructed.

7.2 Algorithm of video steganography for text message extracting using DCT:

2. Stego video is selected
3. Stego video is converted into frames or images
4. Frames are converted into 8 x 8 blocks.
5. DCT is applied into these blocks.
6. Through quantization table, blocks are compressed
7. LSB is computed for DCT coefficient
8. Retrieve the hidden text by converting every bits.

The process flow chart to embed and extract text message through DWT based video steganography is mentioned below.

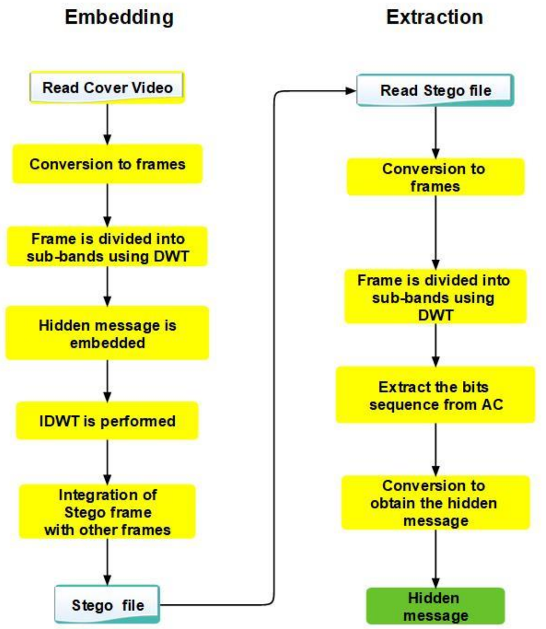
Embedding
Read Cover Video
Conversion to frames
Frame is divided into sub-bands using DWT
Hidden message is embedded
IDWT is performed
Integration of Stego frame with other frames
Stego file
Extraction
Read Stego file
Conversion to frames
Frame is divided into sub-bands using DWT
Extract the bits sequence from AC
Conversion to obtain the hidden message
Hidden message

Figure 19: DWT based Video steganography flow

7.3 Algorithm of video steganography for text message embedding using DWT:

1. Cover video is selected
2. Cover video is converted into frames or images.
3. Cover image/frame is selected.
4. The frame is divided into sub-bands using DWT.
5. The hidden message is embedded to the approximation sub band.
6. IDWT is applied for conversion to stego frame.
7. Stego frame is integrated with other frames for the final stego video.

7.4 Algorithm of video steganography for text message extraction using DWT:

1. Stego video is selected.
2. Stego video is converted into frames or images.
3. Stego image/frame is selected.
4. The frame is divided into sub-bands using DWT.

5. Extract the bits sequence from the approximation band (AC)
6. Binary bits sequence is converted for retrieving the secret text.
7. Hidden message is extracted

8. Result and Analysis

Parameters such as imperceptibility, capacity, and robustness are evaluated.

(a) Imperceptibility: It refers the stego file quality post embedding the secret text. This is a significant factor in steganography wherein if the stego file doesn’t retain its quality, it can be suspected to have hidden information.

(b) Capacity: It refers to the size of the secret message that can be embedded in the carrier or cover file.

(c) Robustness: It refers to withstand manipulation of the stego file such that the embedded secret information can be retrieved after various attacks like scaling, cropping, compression, rotation, blurring, noise adding, filtering and re-mastering.

DWT	**Features**	**Image**	**Audio**	**Video**
	Imperceptibility	Medium	Low	Low
	Capacity	Low	Medium	High
	Robustness	High	High	High
DCT	**Features**	**Image**	**Audio**	**Video**
	Imperceptibility	Medium	Medium	Medium
	Capacity	Low	Medium	Medium
	Robustness	Medium	Medium	Medium

Table 1: Qualitative analysis

9. Conclusion

Transform domain techniques like DCT and DWT are used widely in TV and radio waves, images, video and audio files and has better performance in context to embedding of data and robustness. It is more robust in contradiction to image and signal processing attacks like scaling, cropping, compression, rotation, blurring, noise adding, filtering and re-mastering as compared to spatial domain technique which can be detectable. The data can be securely hidden and transferred over the public network utilizing this technique. However, DCT has less data embedding capacity and robustness in comparison to DWT. The purpose of this study shows that steganography technology when implemented using transformation domain techniques can be a boon in security systems. The benefits of using this techniques will help in develop a framework for covert communication and storing of data secretly. It can help greatly in digital watermarking technology, copyright and holograms. The benefits not limited to data secrecy but can also be used in metadata and secured authentication framework system.

Acknowledgements

My sincere thanks to my professor and guide who has supported me enormously for accomplishing.

References:

[1] Taha, M. S., Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering*, 2019, 518, 052003.

[2] Debnath, D., Ghosh, E., & Banik, B. G. Multi-Image Hiding Blind Robust RGB Steganography in Transform Domain. *International Journal of Web-Based Learning and Teaching Technologies (IJWLTT)*, 15(1), 2020, 24-52.

[3] Qasim Ahmed Alyousuf, F., Din, R., & Qasim, A. Analysis review on spatial and transform domain technique in digital steganography. *Bulletin of Electrical Engineering and Informatics*, 9(2), 2020, 573–581.

[4] S. S. Yadahalli, S. Rege and R. Sonkusare, "Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques," *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, COIMBATORE, India, 2020, pp. 1325-1330.

[5] M. Suresh and I. S. Sam, "Single level Discrete Wavelet Transform based Video Steganography on Horizontal and Vertical coefficients," *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, Chennai, India, 2020, pp. 1-4.

[6] M. K. Oudah,A. N. Abed, R. S. Khudhair and S. M. Kaleefah“Improvement of Image Steganography Using Discrete Wavelet Transform, “*Engineering and Technology Journal*, Vol. 38, Part A, No. 1, 2020, pp. 83-87.

[7] Gahalod, Laxminarayan., and Gupta, Kumar, Sanjeev., “A Review on Digital Image Watermarking using 3-level Discrete Wavelet Transform”, *IJSRSET*, 4, 1, 2018, pp. 930-936.

[8] Bidgoli, Massoud, Amir., and Behrang, Sara., “A New Hybriod Method for Colored Image Steganography based on DWT”, *Journal of Advances in Computer Research* 9, 3, 2018, pp. 71-86.

[9] Hasanah, Uswatun, Latifah., Purboyo, Waluyo, Tito., and Saputra, Erfa, Randy., “A Review of Mp3 Steganography Methods”, *International Journal of Applied Engineering Research*, 13, 2, 2018, pp. 1128-1133.

[10] Podder, Tanusree., Kar, Purbani., and Kumari, Lalita., “An Approach to Hide Information using wavelet based method”, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3, 1, 2018, pp. 800-804.

[11] Shih, Y. Frank., “Digital Watermarking and Steganography: Fundamentals and Techniques”, 2017.