RESEARCH ARTICLE

SAMRIDDHI Volume 12, Special Issue 3, 2020 Print ISSN : 2229-7111 Online ISSN : 2454-5767

# Hiding Text in a Video Using Frequency Domain and Time Domain

Keerthi S. *1, Reshma Nadaf2

[1] PG Student, Dept. of E&CE, SDMCET Dharwad, Karnataka, India; e-mail : keerthis.17eee.rymec@gmail.com
[2] Asst. Prof, Dept. of E&CE, SDMCET Dharwad, Karnataka, India; e-mail : reshmanadaf27@gmail.com

## ABSTRACT

Image and video are two basic forms of transmitting information. For enhancing security, image or video encryption methods are applied for the set of image frames. Considering a video, it can be distributed in photo frames with a help of MATLAB. They are sequentially stored. For a color image or video, the frames can be either Red, Blue or Green. Watermarking technique in image or video processing issued for authentication of documents by embedding or hiding text or data in a video, image or audio file. Copyright symbols or signatures are used according to the requirement. The video Steganography is preferred over other methods because it can accommodate large size of secrete data. Discrete Wavelet Transform DWT and Pseudo-Random Encoding/Decoding algorithm is used for data insertion into a video which makes a robust technique in embedding data in video. The DWT method converts 4×4 cover image blocks in which LL, LH, HL and HH sub-band images are developed. The robustness of this technique will be tested by calculating MSE and PSNR values.

**Keywords :** Steganography, DWT algorithm, Pseudo-Random Encoding/Decoding.

*SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2020); DOI : 10.18090/samriddhi.v12iS3.30*

## INTRODUCTION

For a normal person, the ability to understand the motions of animated video shows that the movement or a change created in a running video has the small amount of pixels only that are modified and rest other pixels remain static when compared with consecutive video frames. A video is basically a combination of frames with a fixed frame rate. A standard frame rate is considered as 25 (25 frames captured in 1 sec). Digital water marking is method of hiding data within a standard video for the identification purpose. It provides unauthorized access and bares protection of copyright of the data. Robust watermarking is achieved by embedding information within digital data if necessary. Digital watermarking is of three categories: Spatial domain, transformation domain and compressed domain. For this proposed theory Spatial domain and transformation domain forms of watermarking. In this theory Transformation domain include Discrete cosine transform (DCT) and Discrete wavelet transform (DWT) is prefer for its spatial localization, frequency spread and multi- resolution characteristics. Considering the dynamics of a video internally, the stage of motion estimation is processed during the encoding and decoding internally. Hence it makes it difficult to fetch data through the image steganographic analysis techniques and a lossless coding procedure is applied. The bits of secrete

**Corresponding Author :** Keerthi S, PG Student, Dept. of E&CE, SDMCET Dharwad, Karnataka, India; e-mail : keerthis.17eee.rymec@gmail.com

**How to cite this article :** S. Keerthi, Nadaf, R. (2020). Hiding Text in a Video Using Frequency Domain and Time Domain. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 12, Special Issue (3), 157-162.*

**Source of support :** Nil

**Conflict of interest :** None

message bits is hidden in the coefficients of wavelet transform which can be even considered as motion vectors called candidate motion vectors.

The 1-D and 2-D wavelet transforms can be performed using filter banks. To obtain filter coefficients we use *wfilters* functions or input. In the least significant bit of each individual motion vector, a single bit can be hidden. The encoded data is made such that the evaluation of motion is allowed to generate motion vectors in a region only. Based on this magnitude of the vector, those candidate motion vectors are selected. Wavelet transformation with visual cryptography is preferred to improve the robustness and to provide high degree on authentication. A message bit is encoded in the form of phase angle difference. The block that is matching is restricted to detect within the selected vectors for the magnitude larger than that of predefined threshold. For reversible method, at the decoder the candidate motion vectors dependent on the cause of the motion vector quality. This paper is arranged systematically as follows: Section 2 describes the related works. Section 3 describes proposed methods. Section 4 describes experimental results for video steganography.

## Related Work

Hiding text in a image, audio and video is under research. Many work is under process relative to this. Some of work is presented below.

Sinha Sanjana, [1] describes that the Digital watermarking is a method considered for copyright protection of digital applications. In this paper a relative approach for watermarking digital video is analyzed. A hybrid digital watermarking scheme based on DWT and Principle Component Analysis (PCA) is proposed.

Chen.B et.al.,[2] presents a classification of embedding methods called Quantization index modulation QIM that provides good rate distortion robustness. It shows that compensated distortion QIM is an specific embedding strategy that can be used against some important classes of international attacks.

Memon N [3] describes some of the specific image related steganography techniques are analyzed and it shows that an observer in fact distinguishes between image carrying a hidden data and image which do not carry. It derives a near form expression of the probability of discovery and fake alarm in the number of bits that are hidden.

M Memon et.al., He and Luo, Masoumi and Amiri, Tong [4-7] identifies the new method of digital watermarking approach for protection of copyright of video, based on wavelet transform. The motion part of the video is found by scene changing analysis, and then apply 3-D wavelet transform over detection motion parts, 10 sub-bands wavelet coefficients are provided [8-9].

H Zhang et,al.,[10] describes that the Geometric distortions are common and effective attacks for many other watermarking methods. For this paper, a new watermark form which allows watermark detection and extraction on the basis of affine transformation attacks [11-13].

Gil-ei-lee et.al.,[14] describes the idea of this proposed paper is that the algorithm is watermark embedding which can be much robust than traditional LSB technique. It makes the random coordinate secure of cover image to enhance the robustness of the watermark image.

M.Hy et.al.,[15] proposed method utilizes the pixel value of the digital original image to gray-scale watermark image in the 1st phase. In second phase a binary watermark image can be later retrieved through the just procedure-permuted gray-scale watermark from the 1st phase.

In real time algorithm, the complete original video is segmented in to number of images using particular MATLAB code. After processing the video by MATLAB module the video gets divided into frames of same size. The text data that has to be inserted into images is partitioned into groups of two bits each. Only two pixels per image is modified and we divide text data in two bits. Each character of text is represented as ASCII value so that each character occupies 1byte or 8bits in an image. The image which has two pixels modified, only the last two character bits in text data to be inserted is represented by ASCII value in line. Later each character represented into groups of 8 bits is subdivided into two bits. Hence we have 4 groups for each character in the text data.

Few watermarking techniques are considered to resist attacks that might be performed against it. In spatial domain, Least Significant bit-LSB of the chosen pixel in the image are flipped. An improvement in this technique is done by pseudo random with number generator which chooses particular pixel to embed data using seed or key. LSB is vulnerable on having to LSBs exchanged with constant values. Threshold based watermarking is less effective when compared to LSB technique based on its schemes.

DCT based schemes are lossy compression. DFT scheme avoids attacks such as rotating, removal and sheering. DWT schemes are more robust against addition in digital data. Histogram technique is used to obtain reversible watermarking performance. For block based watermarking scheme watermark signals must embedded in the maximum coefficients of PCA blocks in LH and HL sub-bands. Or on shot segmentation and block classifications in which watermark should be embedded into AC coefficients 4×4 DCT in compression domain (Figure 1).

From an existing method summary of lossy video compression is considered to define notations and evaluation metrics. A frame is used to encode using regular image compression technique similar to JPEG but with different quantization table and step at the encoder and hence decoder can reconstruct it independently. The intra frame (I- frame) is taken as a reference frame for an encoding a group of forward motion compensated prediction(P) or bi-directionally predicted(B) frames. The commonly used standard MPEG-2, the video is arranged into bunch of pictures and its own frames can be encoded in the particular sequence.

## Proposed Method

### Discrete wavelet transform (Frequency domain)

A wavelet based watermarking in which the watermark is supposed to be embedded on the selected wavelet of the luminance of the image frame. If gray image is considered the image value will be 1. If it's of color image then the image value will be 3 (red=1,green=2,blue=3) as shown in fig. 2. The wavelet transformation is applied in the form of DWT-technique. The behavior of continuous wavelet transform analysis is by Filter banks. The decomposition of a signal is done by the high-pass filter and low-pass filter. The wavelet decomposition is done by considering rows first and then columns. For example consider A × B image. First filter out each row and down-sample the image to obtain two A × (B/2) images. Next filter out each column and sub-sample the filter output to get for (A/2) × (B/2) images of the original image. The output image derived by low-pass filtering of rows and columns are called as LL image. For high-pass row filtering and low-pass filtering column are called HL image. For low- pass filtering row and high-pass filtering column is called LH image and for high-pass filtering of rows and columns are called as HH filtering. In this technique HH band is a desirable sub-band.

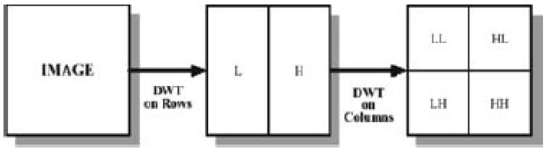


**Figure 1:** DWT block diagram a) original image b) output image on applying one-dimension on row input c) output image after applying one-dimension on column input

Wavelet transform is a multi-resolution tool used for palm print image analysis in different decomposition levels. To extract fine lines of palm print Level-1 palm print decomposition is used. Greater the decomposition level value, coarser the palm fine lines will be (wrinkles and principle lines). To obtain the discontinuity between the two pixels *Haar transformation* is used. The data is en-coded as a portion where the estimation is allowed to generate only vectors in that specific region. The motion estimation-stage is processed during the encoding and decoding internally. A message bit is en-coded as phase angle difference. The block that is matching is restricted to fetch within the selected vectors for the magnitude lager than its predefined threshold.

### Embedding process and Extraction process

Frequency domain technique mainly uses Discrete Wavelet Transformation i.e DWT for data embedding. In this technique for inserting process a cover frame from the video is selected. HH sub-band is selected to hide data over other sub-bands (LL,LH,HL) since identifying hidden data by the intuition of cryptanalyst will be difficult.

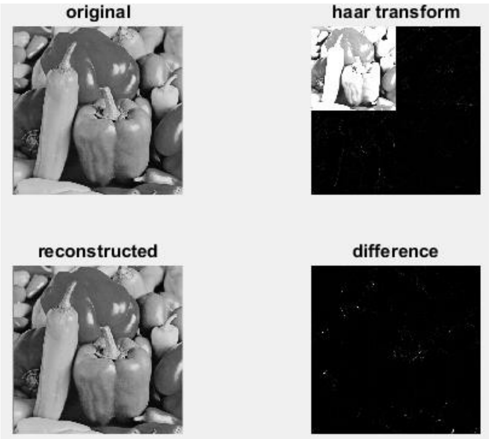


**Figure 2:** a) original gray image, b) applying haar transformation on the gray image c) output image (reconstructed) having secrete text hidden in it, d) the difference between original and constructed image (with secrete text) of HH sub-band

The small difference found in the constructed image after the transformation will be referred as internal Noise in obvious conditions which results in integrity of the data.

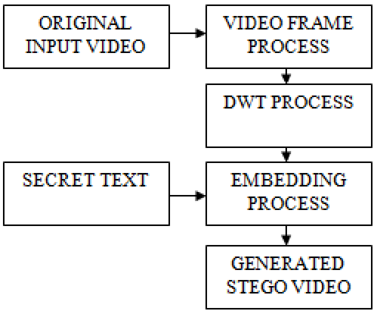


**Figure 3:** Block diagram of embedding text in a video frame

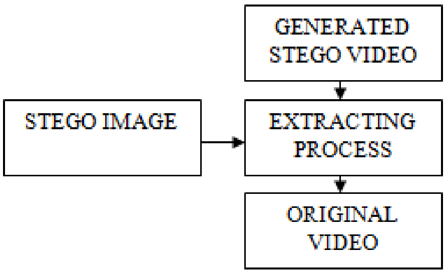


**Figure 4** : Block diagram of extracting the hidden data from the stego video frame

***DWT Algorithm* :**

Step 1: Read input video
Step 2: Convert video into its frames
Step 3: Select the cover frame
Step 4: Apply DWT process for that frame
Step 5: embed secret message (text)
Step 6: Write a stego-frame
Step 7: Reconstruct video

**Pseudo-Random Encoding/Decoding (Time Domain)**

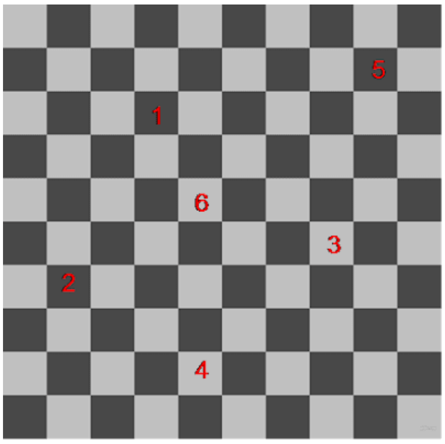


**Figure 5:** Pseudo-Random encoding example

Pseudo-Random generator is initialized with no starting point set. There is no set pattern in message data being encoded/decoded based on random pixel locations determined by random number generator. There are several advantages following;

a) no set encoding/decoding patterns for histogram analysis to detect,

b) Recovery rate is quick i.e, predefined encoding pattern implemented usually with more efficiency.

c) size of the message will become difficult to estimate.

One disadvantage with this technique is that detecting of message can be done using varying sized windows and localized histogram analysis.

**Pseudo-Random algorithm**

Step 1: Read input video
Step 2: Convert video into its frames
Step 3: Select the cover frame
Step 4: Apply Pseudo-Random process for that frame
Step 5: Embed secrete message (text)
Step 6: Write a stego-frame
Step 7: Reconstruct video

## Experimental Results for Video Stegnography

### Mean Square Error (MSE)

It is defined as the square of error between cover frame and the stego frame. The distortion in that frame is measured by MSE.

$$MSE=abs((1/(vidH\times vidW))\times(sum(sum(Yorg - Yout))))$$

Here, vidH = video frame height
Here, vidW = video frame width
Yorg = selected Y frame of original Video
Yout = selected Y frame of output video

### *Peak Signal to Noise Ratio*

It is the maximum signal to noise in stego frame.

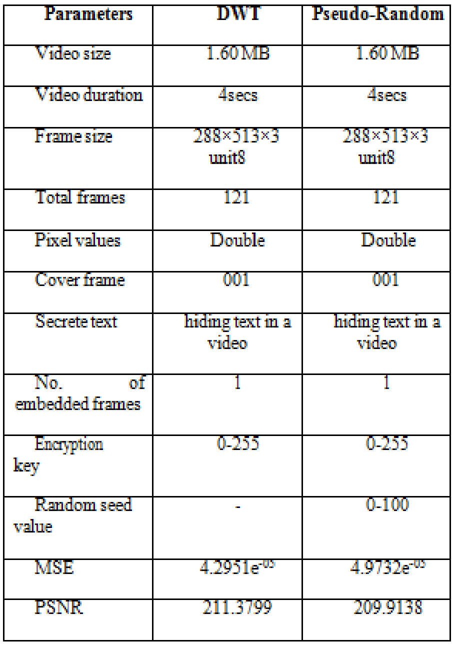
$$PSNR = 10\times log((255\times 255)/MSE)$$

### Results

The algorithm performed in this proposed theory is considered effective over other algorithm only when the PSNR range is greater between them. By comparing the MSE and PSNR values, DWT algorithm is more effective than Pseudo- random algorithm.

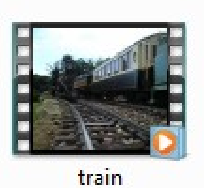
*Comparison between two Domains Example A*

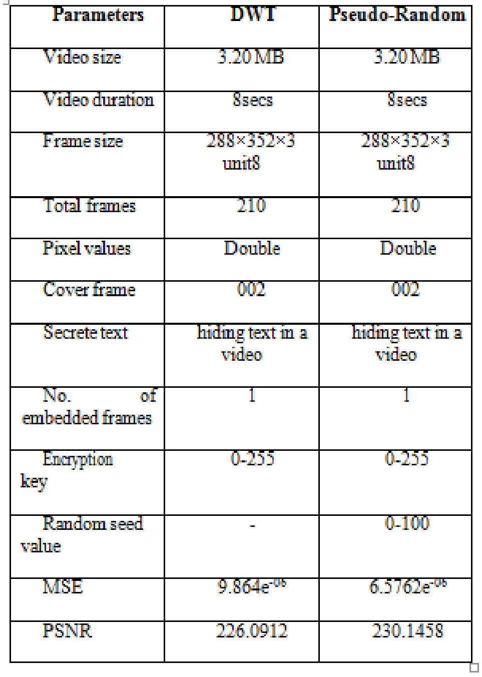
Shuttle Video : 00:00:04.



| Parameters | DWT | Pseudo-Random |
|---|---|---|
| Video size | 1.60 MB | 1.60 MB |
| Video duration | 4secs | 4secs |
| Frame size | 288×513×3 unit8 | 288×513×3 unit8 |
| Total frames | 121 | 121 |
| Pixel values | Double | Double |
| Cover frame | 001 | 001 |
| Secrete text | hiding text in a video | hiding text in a video |
| No. of embedded frames | 1 | 1 |
| Encryption key | 0-255 | 0-255 |
| Random seed value | - | 0-100 |
| MSE | $4.2951e^{-05}$ | $4.9732e^{-05}$ |
| PSNR | 211.3799 | 209.9138 |

*Comparison between two Domains (Example B) Train Video : 00:00:08*





| Parameters | DWT | Pseudo-Random |
|---|---|---|
| Video size | 3.20 MB | 3.20 MB |
| Video duration | 8secs | 8secs |
| Frame size | 288×352×3 unit8 | 288×352×3 unit8 |
| Total frames | 210 | 210 |
| Pixel values | Double | Double |
| Cover frame | 002 | 002 |
| Secrete text | hiding text in a video | hiding text in a video |
| No. of embedded frames | 1 | 1 |
| Encryption key | 0-255 | 0-255 |
| Random seed value | - | 0-100 |
| MSE | $9.864e^{-06}$ | $6.5762e^{-06}$ |
| PSNR | 226.0912 | 230.1458 |

## CONCLUSION

In this proposed theory, Discrete wavelet Transform (DWT) of Frequency Domain and Pseudo-Random of Time Domain based Algorithms are performed which results in showing no difference between the original video and embedded video in both the techniques. Video steganography is more preferred than Image steganography because, detecting embedded image frame from the bunch of video frames is more difficult. These methods can be used for Video, Audio or text files and the data can be transferred more securely. From this procedure, the Elapsed time of Pseudo-Random is less than DWT resulting in fast execution. One extra step for performing pseudo- random technique is that we have to feed a "seed" value. Seed value given as the starting point for the pseudo-random generator to perform encryption and decryption. Generator considers its own logical calculations for embedding each character of the text into the pixels of a cover frame. and in DWT technique, image is embedded as column allocation logic. If *Histogram Analysis* is implemented, data security is more in DWT than Pseudo-Random technique since the PSNR value of DWT technique is more than PSNR value of Pseudo-random technique. Hence performing steganography in Frequency domain is more efficient than performing in Time domain techniques for secure data transmission. By improving these methods, we can obtain video files without any noise distractions.

## REFERENCES

[1] Sinha Sanjana "Digital video watermarking using DWT and principle component analysis" international journal of wisdom based computing, vol-1,no-2,7-12,aug-2011.

[2] Chen.B and G.W.Wornell "quantization index modulation for digital water marking and information embedding of multimedia, J.VLSI signal process,vol-27,pp.7-12,2001.

[3] Memon N "Analysis of LSB based image stegnographic techniques' in IEEE proc.ICIP Oct 2001.

[4] He.X and Luo.Z, A novel stegnographic Algorithm based on motion vector phase, in proc. int. conf. comp. sc.and software Eng.2008,pp.822-825.

[5] Masoumi M. and Amiri.S 'A blind scene based watermarking for video copyright protection' AEU-int.J.Electron.commun.,vol-67.no.6.pp.528-535, june-2013.

[6] Tong M "New video mark scheme resistant to super strong cropping attack" J.inf.secur.,vol- 3,no.2, pp.138-148 2012.

[7] Memon M., Avcibus and Sankur B "stygnalasis using image quality metrics, IEEE trans IP,vol-12 pp.221-229, Feb 2003.

[8] Murat Tekalp A "digital video processing' Prentice Hall Signal processing series.

[9] Midasala V. Bhavanam N. and Naveen Kumar G S "image hiding in a video based DWT and LSB algorithm" ICPVS 2014.

[10] Zhang H. et,al "Affine Legendre Moment invariants for image watermarking Robust to Geometric Distortions" IEEE transactions to image processing, Vol 20, no.8, 2010, pp.2189- 2199.

[11] Ruanaidh J.J.K.O, Pun T., 'Rotation scale and translation invariant spread spectrum digital watermarking, signal process, vol.66, no.03, pp 303-317, 1998.

[12] Pereira S., Pun T., 'robust template matching for affine resistant image watermarking' IEEE Trans, Image process, vol.9, no.06, pp. 1123-1129, june 2000.

[13] Shu. H.Z., Zhuo J., Han G.N., Luo L.M., Lcoatrieux J., 'image reconstruction from limited range projections using orthogonal moments' Pattern recog. Vol.40, no.2. pp-670-680. 2017.

[14] Gil-ei-lee, Eun-Jun-Yoon, Kee-Young-Yu 'A new LSB based watermarking scheme with random mapping function' 978-0-7695-3427-5/08, 2008 IEEE DOI 10.1109/UMC.2008.33.

[15] Hy M., Luo D. and Chang M. 'Dual wrapped digital watermarking scheme for image copyright protection, computers and security' 26:319-330 oct-2006.