# COMPUTERIZED VIDEO STEGANOGRAPHY USING MULTIPLE ALGORITHEMS

**Talakal Sowmya[1], Latha B M[2], Usha Devi[3]**

[1]MTech(D.E), P.G Scholar, Dept of ECE, GMIT, Davangere ,Karnataka, India
[2]Assistant professor, Dept of ECE, GMIT, Davangere, Karnataka, India
[3]Professor, Head of Dept of TCE, JNNCE, Shimoga, Karnataka, India

***Abstract*: Computerized watermarking have been utilized for keeping up copyright data of the advanced media for 10 years. Advanced watermarking is a strategy utilized for inserting copyright data in the media records. The media document could be a picture, a sound, a video, or content. Steganography have been utilized as a part of the Digital watermarking application. Steganography has turned out to be more essential because of the exponential development of correspondence of potential PC data on the web. Steganography contrasts from cryptography, with the end goal that cryptography shrouds the substance of mystery message, while, steganography is about concealing the message in media successfully. This exploration article gives an outline of steganography, its applications, and distinction from cryptography. This paper explains the execution of the Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).**

**This paper introduces the distinctive video steganography procedures. It gives an audit on different accessible calculations. Notwithstanding it, concentrate on Combined Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) Technique and furthermore LSB with adjustments Technique. and likewise DWT**

***Keywords*: Least Significant Bit (LSB), Discrete Cosine Change (DCT), discrete wavelet transforms (DWT), Watermarking, Video, Copyright Protection**

## 1. INTRODUCTION

One of the current copyright protection methods that has recently received considerable attention is Watermarking. The multimedia can be anything for example, it can be text, audio, video and their compositions as well. Conventional watermarks are generally found on valuable paper documents like our check, stock certificates and cash.[1] These conventional watermarks can be viewed by a certain angle or through certain illumination. They cannot be easily removed without leaving an evidence of being tampered. Some watermarks can be visible to indicate ownership of Digital images/video using translucent logos generally used by some television broadcast station superimposed on their transmitted videos. These are plain in view and they do not provide any form of equivalent physical properties other than the actual pixel values to modify . In this case if any pixel values are changed, the content changes as well.[8] A balanced should be maintained so that the watermark imposed can be clearly visible but at the same time difficult to remove. Another concern for visible watermark is that it shouldn't cause any kind of visual distractions. Invisible watermarks are different from visible watermarks, although their objectives are the same to provide copyright protection. Visible watermarks can be used to help prevent any form of piracy by showing ownership semi-transparently on top of images
Various areas where watermarking can be applied:

- Audio
- Video
- Documents
- Images

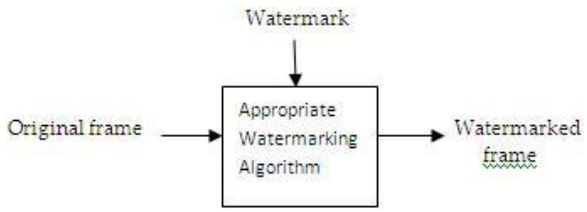



**Fig- 1:** Basic watermarking block diagram

### 2.1 Visible Watermarking

Watermarks are applied to images only. These watermarks can be seen and they cannot be removed by just cutting out the watermark. They are protected from statistical analysis.[5] The only disadvantage of visible watermark is it degrades the image quality . It is not possible to detect them by dedicated programs or devices.

### 2.2 Invisible Watermarking

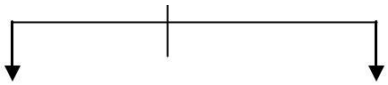
These watermarks are not visible and they can be removed only by the authorized user. They are used by authors and content protectors as they help in protecting the content from being copied.

### 2.3 Partially Visible Watermark

The partially visible watermark is a combination of a visible watermark and an invisible watermark. First a visible watermark is inserted in the host image and then an invisible watermark is added to the already visible-watermarked image.

## 3. WATERMARKING DOMAINS

**Watermarking Domains**



**Spatial Domain** **Frequency Domain**

### 3.1 Spatial Domain

In this technique the watermark embedding is achieved by modifying directly pixel values of host image . Most commonly used method in this technique is the least significant bit (LSB) method.[9] In this technique the least significant bit (LSB) of each pixel in host image is modified so as to embed the secret message. This can help resist only some attacks. In this, the watermark is embedded into the original image in spatial domain ,dividing the original image into different sizes of block and by adjusting the brightness of the block according to the watermark embedded.[4] The methods proposed are robust enough against some operations of image processing , like median filter, scaling and rotation; they are however less robust to cropping attack as the bits of watermark are embedded in the whole image therefore some data may be lost in cropping.

### 3.2 Frequency Domain

In this technique, host image is initially converted into frequency domain by using the method of transformation like the discrete wavelet transforms (DWT),discrete cosine transforms (DCT) or discrete Fourier transforms (DFT) .[7] The transform domain coefficients are then modified using the watermark. The inverse transform is applied to obtain the
image watermarked finally. Due to complicated calculations done by the forward and inverse transforms, these methods are more complex and have higher computational costs compared to spatial domain methods. Transformation domain methods however are more robust enough against attacks compared to spatial domain methods.

Commonly used Transform domain methods: -DCT - Discrete Cosine Transform
-DWT - Discrete Wavelet Transform
-DFT- Discrete Fourier Transform

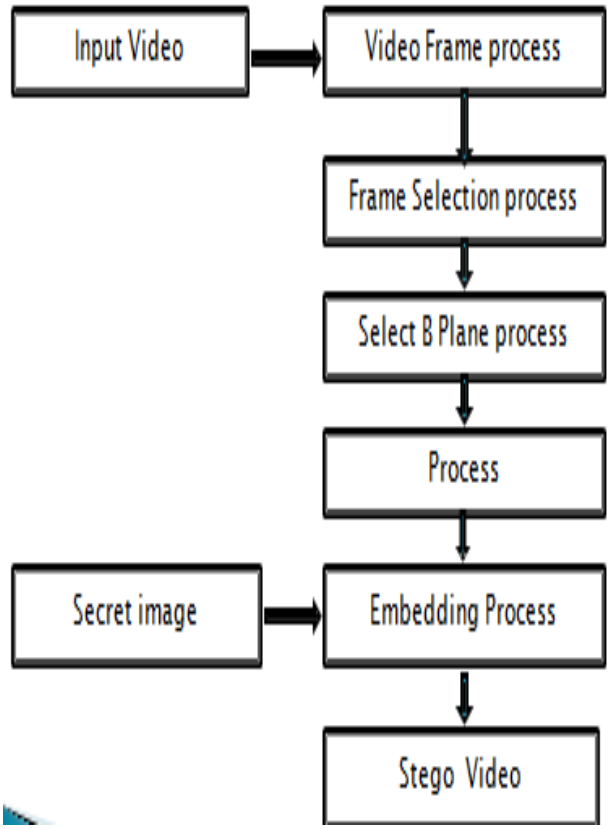


Fig 2:Block diagram for Embedding

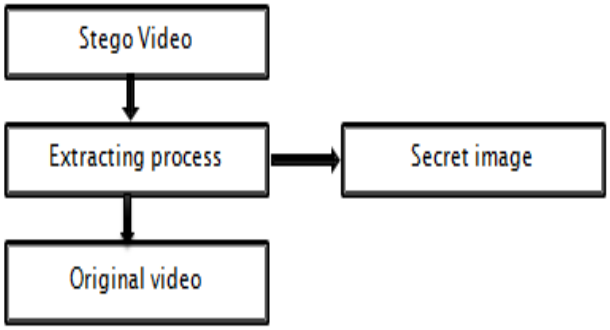


Fig:3: Block diagram for extraction

## 4. COMBINED MODIFIED LSB AND DCT WATERMARKING TECHNIQUE.

General LSB technique is used because it is used from so many years & it is well trusted. This technique gives the ease of use & simplicity of coding with precise results.[12] This technique provides the result in both visible & invisible form (As per the requirement). With some modifications it is good to incorporate this technique for video watermarking.

How the water mark is inserted using LSB technique.

- First the video is divided in number of frames using MATLAB function in bmp file format(bmp file format is uncompressed file format & this format restores the binary data in much safe way).
- Then the number which we need to encrypt (as a key) is converted in binary form.
- This key number is then placed in message at LSB position.
- Then for each frame, message is watermarked at respective LSB position.

- At end all frames are again combined and video is formed with uncompressed file format to restore the data integrity.
- While extracting we get the exact message image and the key encrypted into the message image.

**Limitations:**

- Only 256x256 size video with such size image is good.
- Gray colour image & video are better. In Discrete cosine transform there is a conversion of a sequence of data points in the spatial domain to a sum of sine and cosine transforms with different amplitudes in the frequency domain[10].

The steps used in this technique are following:

- Read the colour host frame i.e. cover frame, Select a grayscale bitmap image of size 256*256.
- Get the RGB component.

**LSB**

The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures .For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel. Features of LSB (Least-Significant-Bit)

**Algorithm For LSB**

*A. The LSB based Steganography encoding algorithm had been developed as follows,*

Step 1: Read the cover image and text message is to be hidden in the cover image.
Step 2: Convert the color image into greyimage.
Step 3: Convert text message in binary.
Step 4: Calculate LSB of each pixels of Cover image.
Step 5: Replace LSB of cover image with each bit of secret message one by one.
Step 6: Write stego image

*B. The decoding algorithm had been developed as follows,*

Step 1: Read the stego image.
Step2: Calculate LSB of each pixel of stego
Step 3: Retrieve bits and convert each 8 bit into character.

**DCT**

A DCT expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCT‘s are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG), to spectral methods for the numerical solution of partial differential equations. The use of cosine functions is best suited for approximating the coefficients. The DCT is purely real unlike discrete Fourier transform which is complex. DCT domain watermarking is a type of frequency domain watermarking which is similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to the lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture. Upon inverse transformation, watermarks applied to frequency domain will be dispersed over the entire spatial image, so these methods are not as susceptible to defeat by cropping as the spatial techniques. However, the trade-off between invisibility and robustness is greater here. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over exposing themselves to removal through compression and noise attacks (high frequencies).The principle advantage of image transformation is the removal of redundancy between neighbouring pixels. This leads to uncorrelated transform coefficients which can be encoded independently. DCT exhibits excellent energy compaction for highly

correlated images. The uncorrelated image has its energy spread out, whereas the energy of the correlated image is packed into the low frequency region. The DCT does a better job of concentrating energy into lower order coefficients than does the DFT for image data. The inverse discrete transform is orthogonal and separable which gives it the much needed robustness towards external attacks.

The general equation for a 1D DCT is defined by the following equation

A 2 – D Discrete Cosine Transform is defined by the equation

$$X(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\nabla(i)\nabla(j)\cos\left[\frac{\pi}{2}.\frac{u}{N}(2i+1)\right]\cos\left[\frac{\pi}{2}.\frac{v}{M}(2j+1)\right]x(i,j)$$

eq(3)

and the corresponding inverse 2D DCT transform is X -1 (u)

Embedding using Discrete Cosine Transform

The data embedding procedure in most of the frequency domain techniques are one and the same except for some minor modifications. To begin with the cover image, watermarks in the form of hospital logo and doctor‘s signature are taken as shown in figure 4.1.The cover image is a MRI brain image of dimension 512 x 512 and divided into sub blocks of 32 x 32. To each of the 32 x 32 block the DCT is applied and the resulting image is shown in

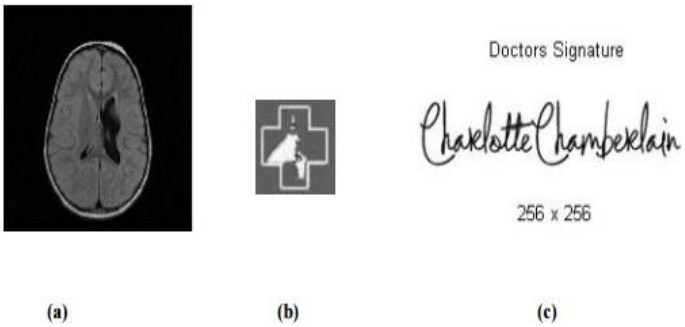



Figure 1

Fig-Input images and payload a. Cover MRI brain image b. Hospital logo (watermark1) c. Doctors signature (watermark2)

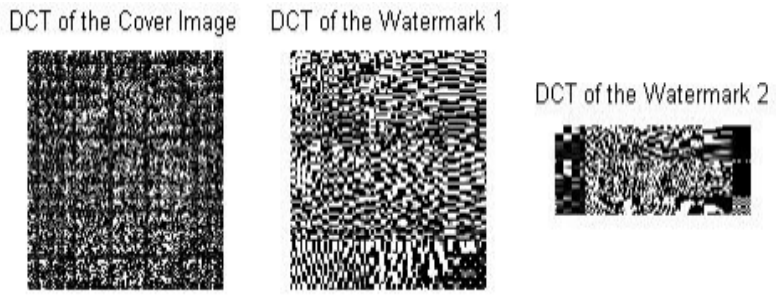



Fig DCT transformed cover image and watermarks

The DCT transforms the image into low, mid and high frequency bands. Since robustness is one of the key criteria, high frequency regions are selected as locations for embedding and the payload and watermarks are cast into the cover image as per the embed equation given below.

$$C\_DCT_{new}\{i,j\} = C\_DCT_{old}\{i,j\} + \propto W_{DCT\{i,j\}}$$

eq(4)Once the embedding is done, the inverse DCT is applied to get back the image in the spatial domain as shown in figure

**Extraction using Discrete Cosine Transform**

The Extraction follows the reverse of the embedding process where the DCT is applied to the embedded image, followed by identification of the embedding location and then differencing it from the original image to get the watermarks and differencing from the original watermarks to get the cover image.

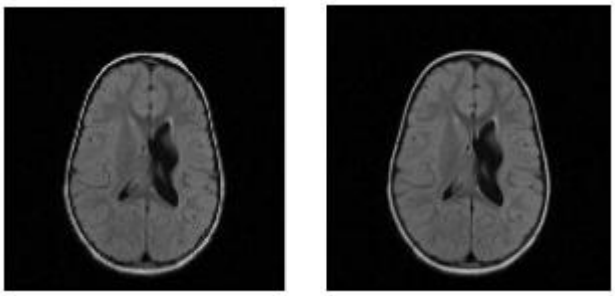


Fig- Original and embedded image using DCT

**Algorithm for DCT**

*The DCT Based Steganography encoding algorithm had been developed as follows,*

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8 x 8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.

*D. The decoding algorithm had been developed as follows,*

Step 1: Read stego image
Step 2: Stego image is broken into 8 x 8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step6: calculate LSB of each coefficient

**DWT**

The basic implementation of DWT for images is described as follows. First, an image decomposed into four parts of low, middle and high frequency sub components LL1, LH1, HL1 and HH1 by samplingc horizontal and vertical channels using subband filters. The sub components LH1, HL1 and HH1 represent the first level decomposition. To obtain the next level decomposition the sub component LL1 is further decomposed as shown in figure (3.2). This process of subsampling is repeated several times based on the requirement. In this work biorthogonal wavelets are used to perform watermark embedding and extraction. Biorthogonal wavelet generates two basis functions for decomposition and reconstruction.

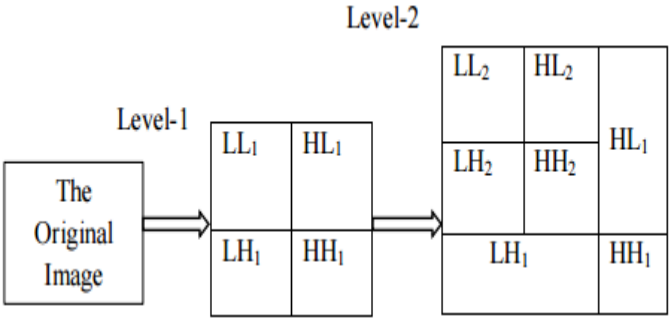



Fig- Discrete Wavelet Transformation

**Algorithm for DWT**

*The DWT Based Steganography encoding algorithm had been developed as follows,*

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2D Haar transform on the cover image.

Step 3: Obtain the horizontal and vertical filtering coefficients of the cover imagCover image is added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

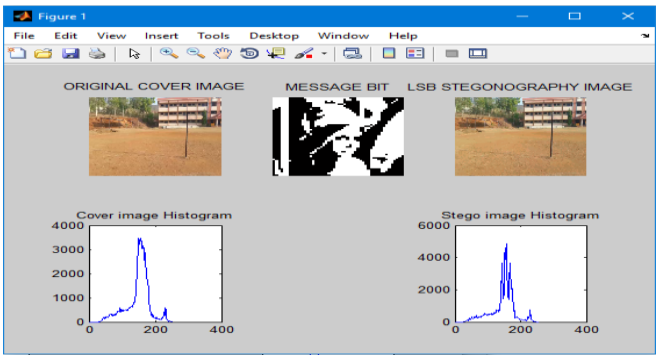
*F. The decoding Algorithm had been developed as follows,*

Step 1: Read the stego image.
Step 2: Obtain the horizontal and vertical filtering coefficients of the cover image.
Step 3: Extract the message bit by bit and recomposing the cover image.
Step 4: Convert the data into message vector. Compare it with original message.

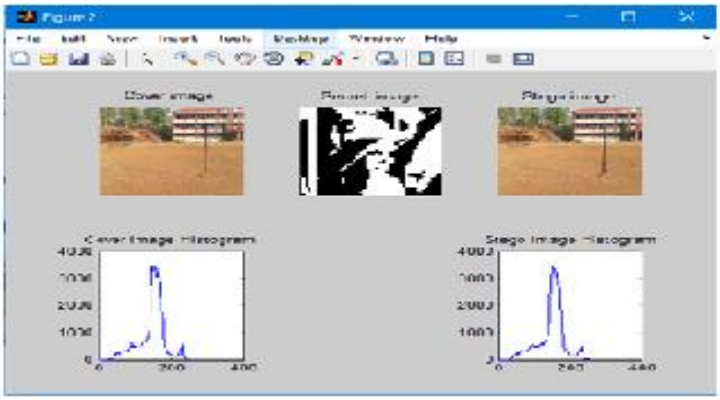
**Results and Conclusions**

In this project we have achieved the LSB, DCT, and DWT algorithms on steganography application. The LSB, DCT, and DWT algorithms are implemented for steganography application. In this experiment, performance analysis of LSB, DCT, and DWT methods is successfully completed and experimental results are discussed. The MSE and PSNR values are compared for the LSB, DCT, and DWT algorithms. The PSNR value shows the quality of image after embedding the data. From the experiment results it is observed that the PSNR of DCT is high as compared to the other two algorithms. Thus, the experiment concludes the DCT algorithm is more suitable for the steganography application compared to the LSB and the DWT based algorithms.

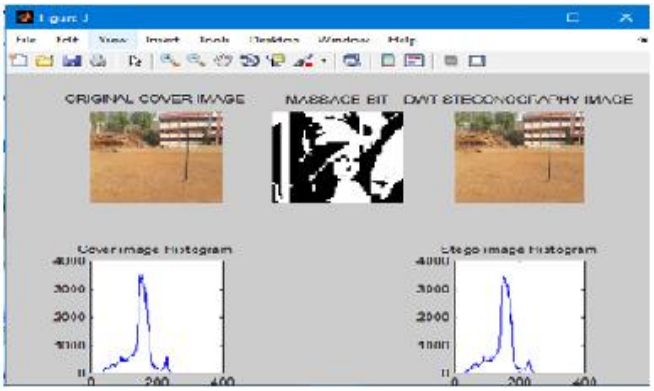
LSB Result Analysis




DCT Result analysis



DWT Result analysis




**Refrences**

1]S. Lyu and H. Farid, "Steganalysis using color wavelet statistics and oneclassvector support machines," in Proc. SPIE Security, Steganography,Watermarking Multimedia Contents, vol. 5306, E. J. Delp III and P. W.Wong, Eds., 2004, pp. 35–45.

2]J. Fridrich, "Feature-based steganalysis for JPEG images and its implicationsfor future design of steganographic schemes," in Proc. Inf. HidingWorkshop, Springer LNCS, vol. 3200, 2004, pp. 67–81

3] Gonzalez, Rafael C., and Paul A. Wintz. "Image Compression Standards."Digital Image Processing. 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.492-510. Print.

4] Lyu, S., & Farid, H.(2006).Steganalysis using higher-order image statistics.Forensics and Security, IEEE Transactions on, 1(1), 111-119.

5]Kundur, Deepa. Watermarking with diversity: Insightsand implications. IEEE Multimedia, 2001, 8(4), 46-52.

6] Page, Thomas. Rights management: Digitalwatermarking as a form of copyright protection. Computer Law & Sec. Rep., 1998, 14(6), 390-92.

7] Rao,N.V.& Pandit, S.N.N. Multimedia digital rightsprotection using watermarking techniques. Inform.Sys. Sec., 2007, September, 93-99.

8] Rosenblatt, Bill. DRM, law and technology: AnAmerican perspective. Online Inform. Rev., 2007

**BIOGRAPHIES**

**Talakal Sowmya**: Talakal Sowmya is a M.Tech scholar from G.M Institute of Technology, Davangere, Karnataka, She completed her B.E from GMIT College, Davangere in 2013,Her Interested areas are

Digital signal Processing, Image processing, Digital Electronics

.

**Ms.Latha B M**: Latha B M is a Assistant Professor of the G M Institute Of Technology, Davangere

**Ms Usha Devi M B:**Usha Devi is a Professor and Hod of JNNCE,Shimoga