# DWT Technique for Steganography

Dontabhaktuni Jayakumar[1], S. Boopalan[2]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Holy Mary Institute of Technology and Science, Bogaram (V), Keesara (M), Rangareddy (D), Telangana, India
[2]Teaching Fellow, University College of Engineering, Villupuram, Tamilnadu.India

***Abstract—*** *Steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side. This study shows that by adopting an object oriented Steganography mechanism, in the sense that, we track skin tone objects in image, we get a higher security. And also satisfactory PSNR (Peak- Signal-to-Noise Ratio) is obtained.*

## I. INTRODUCTION

In modern digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same color pixels repeated in a row. By applying the encrypted data to this redundant data in some random or nonconspicuous way, the result will be data that appears to have the "noise" patterns of regular, nonencrypted data. A trademark or other identifying symbol hidden in software code is sometimes known as a watermark.

Recently revived, this formerly obsolete term gained currency in its day (1500) from a work by Johannes Trithemius, Steganographia, ostensibly a system of angel magic but also claiming to include a synthesis of how to learn and know things contained within a system of cryptography. The book was privately circulated but never published by the author because those who read it found it rather fearsome.

In Steganography secret message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. The message embedding technique is strongly dependent on the structure of the cover, and in this paper covers and secret messages are restricted to being digital images. The cover-image with the secret data embedded is called the “Stego-Image”. The Stego-Image should resemble the cover image under casual inspection and analysis. In addition, for higher security requirements, we can encrypt the message data before embedding them in the cover-image to provide further protection For this the encoder usually employs a Stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a Stego-image. For proposed method cover image is cropped interactively and that cropped region works as a key at decoding side yielding improved security.

A. **DISCRETE WAVELET TRANSFORM NEEDED:** Although the discretized continuous wavelet transform enables the computation of the continuous wavelet transform by computers, it is not a true discrete transform. As a matter of fact, the wavelet series is simply a sampled version of the CWT, and the information it provides is highly redundant as far as the reconstruction of the signal is concerned. This redundancy, on the other hand, requires a significant amount of computation time and resources. The discrete wavelet transform (DWT), on the other hand, provides sufficient information both for analysis and synthesis of the original signal, with a significant reduction in the computation time.

The DWT is considerably easier to implement when compared to the CWT. The basic concepts of the DWT will be introduced in this section along with its properties and the algorithms used to compute it. As in the previous chapters, examples are provided to aid in the interpretation of the DWT.

The main idea is the same as it is in the CWT. A time-scale representation of a digital signal is obtained using digital filtering techniques. Recall that the CWT is a correlation between a wavelet at different scales and the signal with the scale (or the frequency) being used as a measure of similarity. The continuous wavelet transform was computed by changing the scale of the analysis window, shifting the window in time, multiplying by the signal, and integrating over all times. In the discrete case, filters of different cutoff frequencies are used to analyze the signal at different scales. The signal is passed through a series of high pass filters to analyze the high frequencies, and it is passed through a series of low pass filters to analyze the low frequencies.

The resolution of the signal, which is a measure of the amount of detail information in the signal, is changed by the filtering operations, and the scale is changed by upsampling and downsampling (subsampling) operations. Subsampling a signal corresponds to reducing the sampling rate, or removing some of the samples of the signal. For example, subsampling by two refers to dropping every other sample of the signal. Subsampling by a factor n reduces the number of samples in the signal n times.

Upsampling a signal corresponds to increasing the sampling rate of a signal by adding new samples to the signal. For example, upsampling by two refers to adding a new sample, usually a zero or an interpolated value, between every two samples of the signal. Upsampling a signal by a factor of n increases the number of samples in the signal by a factor of n.

Although it is not the only possible choice, DWT coefficients are usually sampled from the CWT on a dyadic grid, i.e., s0 = 2 and t 0 = 1, yielding s=2j and t =k*2j, as described in Part 3. Since the signal is a discrete time function, the terms function and sequence will be used interchangeably in the following discussion. This sequence will be denoted by x[n], where n is an integer.

The procedure starts with passing this signal (sequence) through a half band digital lowpass filter with impulse response h[n]. Filtering a signal corresponds to the mathematical operation of convolution of the signal with the impulse response of the filter. The convolution operation in discrete time is defined as follows:

$$x[n] * h[n] = \sum_{k=-\infty}^{\infty} x[k] \cdot h[n-k]$$

Half band lowpass filter removes all frequencies that are above half of the highest frequency in the signal. For example, if a signal has a maximum of 1000 Hz component, then half band lowpass filtering removes all the frequencies above 500 Hz.

The unit of frequency is of particular importance at this time. In discrete signals, frequency is expressed in terms of radians. Accordingly, the sampling frequency of the signal is equal to 2p radians in terms of radial frequency. Therefore, the highest frequency component that exists in a signal will be p radians, if the signal is sampled at Nyquist's rate (which is twice the maximum frequency that exists in the signal); that is, the Nyquist's rate corresponds to p rad/s in the discrete frequency domain. Therefore using Hz is not appropriate for discrete signals. However, Hz is used whenever it is needed to clarify a discussion, since it is very common to think of frequency in terms of Hz. It should always be remembered that the unit of frequency for discrete time signals is radians.

After passing the signal through a half band lowpass filter, half of the samples can be eliminated according to the Nyquist's rule, since the signal now has a highest frequency of p/2 radians instead of p radians. Simply discarding every other sample will subsample the signal by two, and the signal will then have half the number of points. The scale of the signal is now doubled. Note that the lowpass filtering removes the high frequency information, but leaves the scale unchanged. Only the subsampling process changes the scale. Resolution, on the other hand, is related to the amount of information in the signal, and therefore, it is affected by the filtering operations. Half band lowpass filtering removes half of the frequencies, which can be interpreted as losing half of the information. Therefore, the resolution is halved after the filtering operation. Note, however, the subsampling operation after filtering does not affect the resolution, since removing half of the spectral components from the signal makes half the number of samples redundant anyway. Half the samples can be discarded without any loss of information. In summary, the lowpass filtering halves the resolution, but leaves the scale unchanged. The signal is then subsampled by 2 since half of the number of samples are redundant. This doubles the scale.

This procedure can mathematically be expressed as

$$y[n] = \sum_{k=-\infty}^{\infty} h[k] \cdot x[2n-k]$$

Having said that, we now look how the DWT is actually computed: The DWT analyzes the signal at different frequency bands with different resolutions by decomposing the signal into a coarse approximation and detail information. DWT employs two sets of functions, called scaling functions and wavelet functions, which are associated with low pass and highpass filters, respectively. The decomposition of the signal into different frequency bands is simply obtained by successive highpass and lowpass filtering of the time domain signal. The original signal x[n] is first passed through a halfband highpass filter g[n] and a lowpass filter h[n]. After the filtering, half of the samples can be eliminated according to the Nyquist's rule, since the signal now has a highest frequency of p /2 radians instead of p . The signal can therefore be subsampled by 2, simply by discarding every other sample. This constitutes one level of decomposition and can mathematically be expressed as follows:

$$y_{high}[k] = \sum_n x[n] \cdot g[2k - n]$$

$$y_{low}[k] = \sum_n x[n] \cdot h[2k - n]$$

where yhigh[k] and ylow[k] are the outputs of the highpass and lowpass filters, respectively, after subsampling by 2. This decomposition halves the time resolution since only half the number of samples now characterizes the entire signal. However, this operation doubles the frequency resolution, since the frequency band of the signal now spans only half the previous frequency band, effectively reducing the uncertainty in the frequency by half. The above procedure, which is also known as the subband coding, can be repeated for further decomposition. At every level, the filtering and subsampling will result in half the number of samples (and hence half the time resolution) and half the frequency band spanned (and hence double the frequency resolution).

## II. TYPES OF SECURITY ALGORITHMS

**A. ENCRYPTION:** The word encryption comes from the Greek word kryptos, meaning hidden or secret. The use of encryption is nearly as old as the art of communication itself. As early as 1900 BC, an Egyptian scribe used non-standard hieroglyphs to hide the meaning of an inscription. In a time when most people couldn't read, simply writing a message was often enough, but encryption schemes soon developed to convert messages into unreadable groups of figures to protect the message's secrecy while it was carried from one place to another. The contents of a message were reordered (transposition) or replaced (substitution) with other characters, symbols, numbers or pictures in order to conceal its meaning. In 700 BC, the Spartans wrote sensitive messages on strips of leather wrapped around sticks. When the tape was unwound the characters became meaningless, but with a stick of exactly the same diameter, the recipient could recreate (decipher) the message. Later, the Romans used what's known as the Caesar Shift Cipher, a monoalphabetic cipher in which each letter is shifted by an agreed number. So, for example, if the agreed number is three, then the message, "Be at the gates at six" would become "eh dw wkh jdwhv dw vla". At first glance this may look difficult to decipher, but juxtapositioning the start of the alphabet until the letters make sense doesn't take long. Also, the vowels and other commonly used letters like T and S can be quickly deduced using frequency analysis, and that information in turn can be used to decipher the rest of the message.

The Middle Ages saw the emergence of polyalphabetic substitution, which uses multiple substitution alphabets to limit the use of frequency analysis to crack a cipher. This method of encrypting messages remained popular despite many implementations that failed to adequately conceal when the substitution changed, also known as key progression. Possibly the most famous implementation of a polyalphabetic substitution cipher is the Enigma electro-mechanical rotor cipher machine used by the Germans during World War Two.

**B. CRYPTOGRAPHY:** Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

a. Confidentiality (the information cannot be understood by anyone for whom it was unintended)

b. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

c. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

d. Authentication (the sender and receiver can confirm each others identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

The word is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar

(100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

C. **STEGANOGRAPHY:** The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks ) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

D. **DIGITAL STEGANOGRAPHY:** Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism. Steganalysis, which is the science of attacking steganography, is not the focus of this survey but nonetheless will be briefly discussed.

## III. METHOD OF TECHNOLOGY

A. **PROPOSED METHOD:** Proposed method introduces a new method of embedding secret data within skin as it is not that much sensitive to HVS (Human Visual System).This takes advantage of Biometrics features such as skin tone, instead of embedding data anywhere in image, data will be embedded in selected regions. Overview of method is briefly introduced as follows. At first skin tone detection is performed on input image using HSV (Hue, saturation, value) color space. Secondly cover image is transformed in frequency domain. This is performed by applying Haar-DWT, the simplest DWT on image leading to four sub bands. Then payload (number of bits in which we can hide data) is calculated. Finally secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band. Before performing all steps cropping on input image is performed and then in only cropped region embedding is done, not in whole image. Cropping results into more security than without cropping. Since cropped region works as a key at decoding side. Here embedding process affects only certain Regions of Interest (ROI) rather than the entire image. So utilizing objects within images can be more advantageous. This is also called as Object Oriented Steganography. Next sub-sections briefly introduce skin tone detection and DWT.

B. **SKIN COLOR TONE DETECTION**: detector typically transforms a given pixel into an appropriate color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier defines a decision boundary of the skin color class in the color space. Although this is a straightforward process has proven quite challenging.

C. The simplest way to decide whether a pixel is skin color or not is to explicitly define a boundary. RGB matrix of the given color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. There exists several color spaces. Mainly two kinds of color spaces are exploited in the literature of biometrics which are HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces it is experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within those two color spaces. Color space used for skin detection in this work is HSV. Any color image of RGB color space can be easily converted into HSV color space.

D. **DISCRETE WAVELET TRANSFORM (DWT):** This is another frequency domain in which Steganography can be implemented. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT.DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

a. LL – Horizontally and vertically low pass

b. LH – Horizontally low pass and vertically high pass

c. HL - Horizontally high pass and vertically low pass

d. HH - Horizontally and vertically high pass

e. Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band. As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. DWT used in this work is Haar-DWT, the simplest DWT.

E. **EMBEDDING PROCESS:** Suppose C is original 24-bit color cover image of M×N Size. It is denoted as:

$$C= \{xij,\ yij,\ zij\ |1 \leq i \leq M,\ 1 \leq j \leq N,\ xij,\ yij,\ zij\ \in \{0,1,..,255\}\}$$

Let size of cropped image is Mc×NC where Mc≤M and Nc≤N and Mc=Nc. i.e. Cropped region must be exact square as we have to apply DWT later on this region. Let S is secret data. Here secret data considered is binary image of size a×b. Fig. 1 represents flowchart of embedding

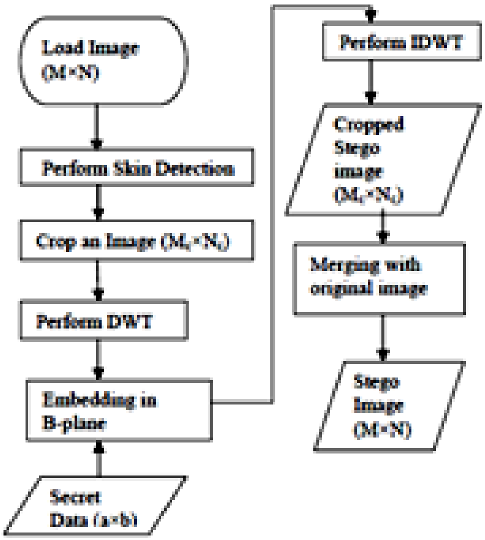
Process. Different steps of flowchart are given in detail below.

**Step 1:** Once image is loaded, apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.

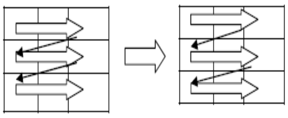
**Step 2:** Ask user to perform cropping interactively on mask image (Mc×NC). After this original image is also cropped of same area. Cropped area must be in an exact square form. It is done for security purpose. Cropped area should contain skin region.

**Step 3:** Apply DWT to only cropped area (Mc×NC) not whole image (M×N). Data can be hidden only in high frequencies. So select one of the high frequency sub band from DWT.

**Step 4:** Perform embedding of secret data in one of sub-band that we obtained earlier by tracing skin pixels in that sub-band. Secret data can b hidden either in green or blue plane but strictly not in red plane



**Flowchart of Embedding Process**

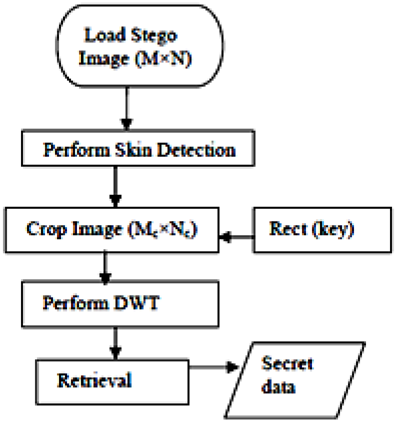


**Raster Scan Order**

**Step 5:** Perform IDWT to combine 4 sub-bands.

**Step6:** A cropped Stego image of size Mc×NC is obtained in above step (step 5). S we need to merge the cropped Stego image with original image to get the Stego image of size M×N. To perform merging we require coefficients of first and last pixels of cropped area in original image so that r calculated.

F. **XTRACTION PROCESS: SECRET DATA EXTRACTION IS EXPLAINED AS FOLLOWS:** 24 bit color Stego image of size M×N is input to extraction process. We must need value of cropped area to retrieve data. Suppose cropped area value is stored in 'rect' variable that is same as in encoder. So this 'rect' will act as a key at decoder side. All steps of Decoder are opposite to Encoder. Care must be taken to crop same size of square as per Encoder. By tracing skin pixels in HHH sub-band of DWT secret data is retrieved. Extraction procedure is represented using Flowchart which is given below:



**Flowchart of Extraction Process**

G. **SIMULATION RESULTS:** In this section we demonstrate simulation results for proposed scheme. This has been implemented using MATLAB7.0.

## IV. CONCLUSION

Biometric Steganography is presented that usesskin region of images in DWT domain for embedding secret data. By embedding data in only certain region and not in whole image security is enhanced. Also image cropping concept introduced, maintains security at respectable level since no one can extract message without having value of cropped region. Features obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of Stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive too. According to simulation results, proposed approach provides fine image quality.

## REFERENCES

[1] Heena Malik*, Sandeep Singh Kang Department of Computer Science Punjab Technical University India "Designing and Evaluation of Performance of a Spread Spectrum Technique for Audio Steganography"in International Journal of Advanced Research in Computer Science and Software Engineering 3(8), August - 2013, pp. 374-378.

[2] Ming Li, Michel Kulhandjian, Dimitris A. Pados†, Stella N. Batalama Department of Electrical Engineering State University of New York at Buffalo "Extracting Spread-Spectrum Hidden Data from Digital Media" in IEEE Transactions on Image Processing

[3] Discrete Wavelet Transforms - Algorithms and Applications,Author(s) Hannu Olkkonen

[4] Efficient Algorithms for Discrete Wavelet Transform With Applications to Denoising and Fuzzy Inference Systems.Authors: Shukla, S K, Tiwari, Arvind K.