Research Inventy: International Journal of Engineering And Science
Vol.5, Issue 2 (February 2015), PP 67-78
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

A Dwt Based Approach for Steganography Using Biometrics

[1] B Satyanarayana, [2] S China Venkateswarlu, [3]Dr. Chennappa Keshava Murthy
[1] Assistant Professor, [2,3]Professor, Department of ECE,
Holy Mary Institute of Technology & Science

Abstract: *Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Steganography method used in this paper is based on biometrics. And the biometric feature used to implement Steganography is skin tone region of images. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. 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 this highly digitalized world, the Internet serves as an important role for data transmission and sharing. However, since it is a worldwide and publicized medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue.So, instantly there are three security methods are in use. They are well known methods in this modern world i.e., encryption, cryptography and Steganography.

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.

II. TYPES OF SECURITY ALGORITHMS

2.1 ENCRYPTION

The first encryption methods date back to 4,000 years ago and were considered more of an ancient art. As encryption evolved, it was mainly used to pass messages through hostile environments of war, crisis, and for negotiation processes between conflicting groups of people. Throughout history, individuals and governments have worked to protect communication by encrypting it. As time went on, the encryption algorithms and the devices that used them increased in complexity, new methods and algorithms were continually introduced, and it became an integrated part of the computing world.

Encryption, sometimes called encipherment, is the act of concealing the meaning of a message. Decryption or decipherment is the inverse process of returning it to its original form. Any other, unauthorized method of recovering the original message is known as cryptanalysis or "breaking" the message. Cryptanalysis is the combination of science, art, and luck used to break messages or entire systems. The word cryptology nowadays refers to the study of both cryptography and cryptanalysis.

2.2 CRYPTOGRAPHY

The word cryptography and the associated word cryptology have very similar etymological origins. They are derived from the Greek words crypto's, which means "hidden"; graphics, which translates to "writing"; and logos, which is "word" or "speech." In current usage, however, they have slightly different meanings. Cryptography is the science of hiding information.

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources. So a more realistic goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker.

2.3 STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphia meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and Steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. Steganography can in done in audio, video, image, text etc.

The advantage of Steganography, over cryptography alone, is

- Messages do not attract attention to themselves.
- Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.
- Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties.

Steganography has been widely used, including in recent historical times and the present day. Possible permutations are endless and known examples include:

- Hidden messages within wax tablets — in ancient Greece, people wrote messages on the wood, and then covered it with wax upon which an innocent covering message was written.
- On the number and size of messages that can be encoded on one person's scalp.
- During World War II, the French Resistance sent some messages written on the backs of couriers using invisible ink.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages.
- Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on envelopes in the area covered by postage stamps.

There are mainly types of Steganography. They are namely:

- Digital Steganography.
- .Network Steganography.
- Printed Steganography.
- Text Steganography.

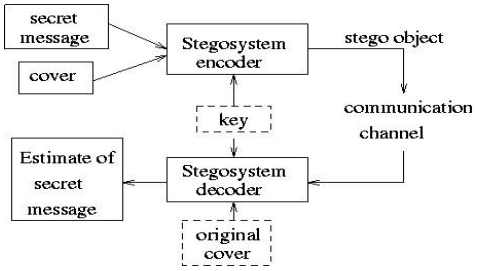
2.3.1DIGITAL STEGANOGRAPHY

Modern Steganography entered the world in 1985 with the advent of the personal computer being applied to classical Steganography problems. Development following that was slow, but has since taken off, going by the number of "Stego" programs available: Over 800 digital Steganography applications have been identified by the Steganography Analysis and Research Center.

Digital Steganography techniques include:

- Concealing messages within the lowest bits of noisy images or sound files.
- Chaffing and winnowing.
- Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
- Pictures embedded in video material (optionally played at slower or faster speed).

- Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in key presses in some applications (telnet or remote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
- Changing the order of elements in a set.



2.3.1 General steganographic model

2.3.2 NETWORK STEGANOGRAPHY

All information hiding techniques that may be used to exchange Steganography in telecommunication networks can be classified under the general term of network Steganography. This nomenclature was originally introduced. Contrary to the typical Steganography methods which utilize digital media (images, audio and video files) as a cover for hidden data, network Steganography utilizes communication protocols' control elements and their basic intrinsic functionality. As a result, such methods are harder to detect and eliminate.

Typical network Steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU (Protocol Data Unit) to the time relations between the exchanged PDUs.

Network Steganography covers a broad spectrum of techniques, which include, among others:

- Steganophony
- WLAN Steganography

2.3.3 PRINTED STEGANOGRAPHY

Digital Steganography output may be in the form of printed documents. A message, the plaintext, may be first encrypted by traditional means, producing a cipher text. Then, an innocuous cover text is modified in some way so as to contain the cipher text, resulting in the Stego text. For example, the letter size, spacing, typeface, or other characteristics of a covert ext can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. Francis Bacon developed Bacon's cipher as such a technique. Printing introduces much noise in the cipher text, generally rendering the message unrecoverable. There are techniques that address this limitation; one notable example is ASCII Art Steganography.

2.3.4 TEXT STEGANOGRAPHY

Steganography can be applied to different types of media including text, audio, image and video etc. However, text Steganography is considered to be the most difficult kind of Steganography due to lack of redundancy in text as compared to image or audio but still has smaller memory occupation and simpler communication. The method that could be used for text Steganography is data compression. Data compression encodes information in one representation into another representation. The new representation of data is smaller in size. One of the possible schemes to achieve data compression is Huffman coding. Huffman coding assigns smaller length code words to more frequently occurring source symbols and longer length code words to less frequently occurring source symbols. In general, terminology analogous to (and consistent with) more conventional radio and communications technology is used; however, a brief description of some terms which show up in software specifically, and are easily confused, is appropriate. These are most relevant to digital Steganography systems.

2.4 STEGANOGRAPHY IN IMAGES

When hiding information inside images the LSB (Least Significant Bit) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of.

Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion. It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

2.5 STEGANOGRAPHY IN AUDIO

When hiding information inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. Spread Spectrum is another method used to conceal information inside of an audio file. This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum.

Echo data hiding is yet another method of hiding information inside an audio file. This method uses the echoes in sound files in order to try and hide information. By simply adding extra sound to an echo inside an audio file, information can be concealed. The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file.

2.6 STEGANOGRAPHY IN VIDEO

When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. DCT works by slightly changing the each of the images in the video, only so much though so it's isn't noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up. For example if part of an image has a value of 6.667 it will round it up to 7.Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video. When only a small amount of information is hidden inside of video it generally isn't noticeable at all, however the more information that is hidden the more noticeable it will become.

2.7 STEGANOGRAPHY IN DOCUMENTS

Steganography can be used in documents? Yes it's true! The use of Steganography in documents works by simply adding white space and tabs to the ends of the lines of a document. This type of Steganography is extremely effective, because the use white space and tabs is not visible to the human eye at all, at least in most text/document editors. White space and tabs occur naturally in documents, so there isn't really any possible way using this method of Steganography would cause someone to be suspicious. The most popular piece of software used to perform this type of Steganography is a piece of software called SNOW.

2.8 WATERMARKING

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness or density variations in the paper. There are two main ways of producing watermarks in paper; the dandy roll process, and the more complex cylinder mould process.

Watermarks vary greatly in their visibility; while some are obvious on casual inspection, others require some study to pick out. Various aids have been developed, such as watermark fluid that wets the paper without damaging it. Watermarks are often used as security features of banknotes, passports, postage stamps, and other documents to prevent counterfeiting watermark is very useful in the examination of paper because it can be used for dating, identifying sizes, mill trademarks and locations, and the quality of a paper.

Encoding an identifying code into digitized music, video, picture, or other file is known as a digital watermark.

2.9 STEGANOGRAPHY IN SPATIAL DOMAIN

This is a simplest Steganography technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the right most bits (bits with the smallest weighting) so that the greatly. The mathematical representation for LSB is:

$$x_i' = x_i - x_i \bmod 2^k + m_i \qquad (1)$$

In equation (1), xi' represents the Ith pixel value of the Stego-image and xi represents that of the original cover image. M_i represents the decimal value of the I Th block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$$m_i = x_i \bmod 2^k \quad (2)$$

Hence, a simple permutation of the extracted mi gives us the original confidential data. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane.

2.10 STEGANOGRAPHY IN FREQUENCY DOMAIN

Robustness of Steganography can be improved if properties of the cover image could be exploited. For example it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to human HVS (Human Visual System). Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it. Different sub-bands of frequency domain coefficients give significant information about where vital and non vital pixels of image resides. These methods are more complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in DCT or DWT.

2.11 ADAPTIVE STEGANOGRAPHY

Adaptive Steganography is special case of two former methods. It is also known as "Statistics aware embedding" Masking" This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficient.

III. WAVELET TRANSFORMS

A wavelet is a mathematical function used to divide a given function or continuous-time signal into different scale components. Usually one can assign a frequency range to each scale component. Each scale component can then be studied with a resolution that matches its scale. A wavelet transform is the representation of a function by wavelets. The wavelets are scaled and translated copies (known as "daughter wavelets") of a finite-length or fast-decaying oscillating waveform (known as the "mother wavelet").

Wavelet transforms have advantages over traditional Fourier transforms for representing functions that have discontinuities and sharp peaks, and for accurately deconstructing and reconstructing finite, non-periodic and/or non-stationary signals. Wavelets are classified in to following types they are:

- Discrete wavelet transform (DWT)
- Discrete cosine transform (DCT)
- Lifting scheme & Generalized Lifting Scheme(LSGLS)
- Wavelet packet decomposition (WPD)
- Continuous wavelet transform(CWT)

3.1 DISCRETE WAVELET TRANSFORM

In numerical analysis and functional analysis, a **discrete wavelet transform** (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time).

There are various types of DWT.They are:

- Haar wavelet
- Daubechies wavelets etc.,

3.1.1 HAAR WAVELETS

The first DWT was invented by the Hungarian mathematician Alfred Haar. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale: finally resulting in $2^n - 1$ differences and one final sum.

3.1.2 PROPERTIES

- The Haar DWT illustrates the desirable properties of wavelets in general. First, it can be performed in $O(n)$ operations

Second, it captures not only a notion of the frequency content of the input, by examining it at different scales, but also temporal content, i.e. the times at which these frequencies occur.

3.1.3 APPLICATIONS

- The discrete wavelet transform has a huge number of applications in science, engineering, and mathematics and computer science.
- Most notably, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression.

3.2 JPEG THEORY

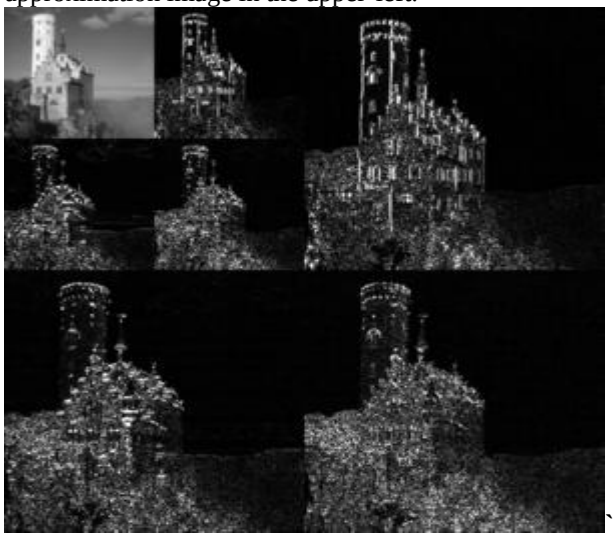
JPEG is an image compression standard used for storing images in a compressed format. It stands for Joint Photographic Experts Group. The remarkable quality of JPEG is that it achieves high compression ratios with little loss in quality.JPEG format is quite popular and is used in a number of devices such as digital cameras and is also the format of choice when exchanging large sized images in a bandwidth constrained environment such as the Internet. The DCT is used in JPEG image compression and Theory of video compression. There, the two-dimensional DCT-II of $N \times N$ blocks is computed and the results are quantized and entropy coded. In this case, *N* is typically 8 and the DCT-II formula is applied to each row and column of the block. The result is an 8 × 8 transform coefficient array in which the (0,0) element (top-left) is the DC (zero-frequency) component and entries with increasing vertical and horizontal index values represent higher vertical and horizontal spatial frequencies.

JPEG2000

Overview: JPEG2000 features: "compress once, decompress many ways".

- Quality and resolution scalability.
- Spatial random access.
- color / grayscale component random access (up to 2^{14})
- Region of interest coding.

The original image is high-pass filtered, yielding the three large images, each describing local changes in brightness (details) in the original image. It is then low-pass filtered and downscaled, yielding an approximation image; this image is high-pass filtered to produce the three smaller detail images, and low-pass filtered to produce the final approximation image in the upper-left.



3.3BIOMETRICS

Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric characteristics can be divided in two main classes:

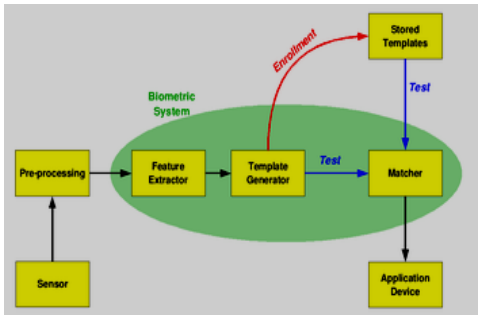
- **Physiological** are related to the shape of the body.
- Ex:fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, which has largely replaced retina, and odor/scent.
- **Behavioral** are related to the behavior of a person
- Ex: typing rhythm, gait, and voice. Some researchers have coined the term **behaviometrics** for this class of biometrics.

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- **Universality** – each person should have the characteristic.
- **Uniqueness** – is how well the biometric separates individuals from another.
- **Permanence** – measures how well a biometric resists aging and other variance over time.
- **Collectability** – ease of acquisition for measurement.
- **Performance** – accuracy, speed, and robustness of technology used.
- **Acceptability** – degree of approval of a technology.
- **Circumvention** – ease of use of a substitute.

A biometric system can operate in the following two modes:

- **Verification** – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number.
- **Identification** – A one too many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.



3.3 BASIC BLOCK DIAGRAM OF BIOMETRIC SYSTEM

3.3.1 PERFORMANCE

The following are used as performance metrics for biometric systems just a trial:

- False accept rate or false match rate (FAR or FMR)
- False reject rate or false non-match rate (FRR or FNMR)
- Receiver operating characteristic or relative operating characteristic (ROC)
- Equal error rate or crossover error rate (EER or CER)
- Failure to enroll rate (FTE or FER).
- Failure to capture rate (FTC) template capability.

3.3.2 ISSUES AND CONCERNS

- Privacy and discrimination.
- Danger to owners of secured items.
- Cancelable biometrics**.**

3.3.3 ADVANTAGES

- The primary advantage of biometric authentication methods i.e., authenticates the user.
- These methods use real human physiological or behavioral characteristics to authenticate users.
- These bio-metric characteristics are (more or less) permanent and not changeable.
- It is also not easy (although in some cases not principally impossible) to change one's fingerprint, iris or other biometric characteristics.
- Biometric objects cannot be stolen as tokens, keys, cards or other objects used for the traditional user authentication

3.3.4 DISADVANTAGES

- Biometric systems may violate user's privacy
- Use of biometric systems may also imply loss of anonymity.
- The fact that biometric characteristics are not secret brings some issues that traditional authentication systems need not deal with.
- Some biometric sensors (particularly those having contact with users)also have a limited lifetime

.

3.4 CROPPING (IMAGE)

Cropping refers to the removal of the outer parts of an image to improve framing, accentuate subject matter or change aspect ratio. Depending on the application, this may be performed on a physical photograph, artwork or film footage, or achieved digitally using image editing software. The term is common to the film, broadcasting, photographic, graphic design and printing industries

3.4.1 CROPPING IN PHOTOGRAPHY, PRINT & DESIGN

3.4 wide views, UN cropped photograph

3.4.1 cropped version, accentuating subject

3.4.2 CROPPED VERSION, ACCENTUATING SUBJECT

In the printing, graphic design and photography industries, cropping refers to removing unwanted areas from a photographic or illustrated image. One of the most basic photo manipulation processes, it is performed in order to remove an unwanted subject or irrelevant detail from a photo, change its aspect ratio, or to improve the overall composition.

3.5 CROPPING IN CINEMATOGRAPHY & BROADCASTING

In certain circumstances, film footage may be cropped to change it from one aspect ratio to another, without stretching the image or filling the blank spaces with ***letterbox*** bars

Aspect ratio concerns are a major issue in film making. Rather than cropping, the cinematographer traditionally uses mattes to increase the latitude for alternative aspect ratios in projection and broadcast. Since the advent of widescreen television, a similar process removes large chunks from the top & bottom to make a standard 4:3 image fit a 16:9 one, losing 25% of the original image. This process has become standard in the United Kingdom, in TV shows where many archive clips are used, which gives them a zoomed-in, cramped image with significantly reduced resolution. This is nonetheless preferred to a process called pillar boxing, where black bands are placed down the sides of the screen, allowing the original image to be shown full-frame within the wider aspect ratio (fig. 6). See this article for a fuller description of the problem.

- Typical cropping in cinematographic and broadcast applications

3.5 original images with widescreen aspect ratio, showing alternative aspect ratios

3.5.1 Image with letterbox resized to 4:3, the whole image is visible

3.6 PEAK SIGNAL-TO-NOISE RATIO

The phrase peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec's (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. It is most easily defined via the mean squared error (MSE) which for two m×n monochrome images m_i and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

Here,

- MAX_I is the maximum possible pixel value of the image. Sample, MAX_I is 2^B-1.
- MSE is the sum over all squared value differences divided by image size and by three.

Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, where higher is better.

IV. 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.

4.1 SKIN COLOR TONE DETECTION

A skin 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.

. 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. A face localization based on HSV. They found that human flesh can be an approximation from a sector out of a hexagon with the constraints:

- S min= 0.23, S max =0.68, H min =00 and H max=500

4.1.2 DIFFERENT CHOICES FOR COLOR SPACES

- RGB
- Normalized RGB
- HIS, HSV, HSL
  Fleck HSV
- TSL
- YCbCr
- Perceptually uniform colors
  CIELAB, CIELUV
- Others
  YES, YUV, YIQ, CIE-xyz

4.2 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

- LL – Horizontally and vertically low pass
- LH – Horizontally low pass and vertically high pass
- HL - Horizontally high pass and vertically low pass
- HH - Horizontally and vertically high pass

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.

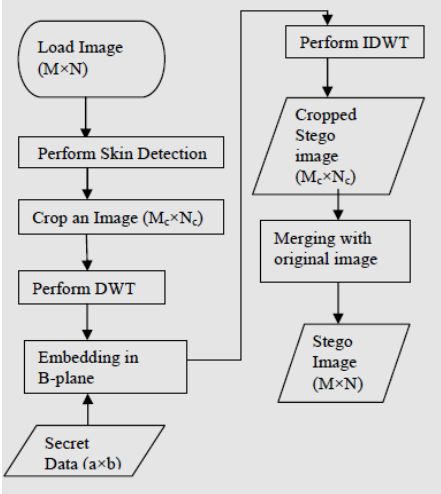
4.3 EMBEDDING PROCESS

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

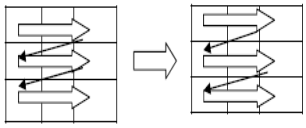
$$C= \{x_{ij}, y_{ij}, z_{ij} \mid 1 \le i \le M, 1 \le j \le N, x_{ij}, y_{ij}, z_{ij} \in \{0,1,..,255\}\}$$

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



4.3 Flowchart of Embedding Process



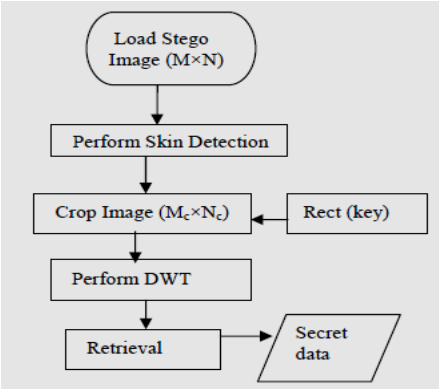
4.3.1 Raster Scan Order

- **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.

4.4 EXTRACTION PROCESS

4.4.1 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:



4.4 Flowchart of Extraction Process

V. SIMULATION RESULTS

In this section we demonstrate simulation results for proposed scheme. This has been implemented using MATLAB 7.0.

A 24 bit color image is employed as cover-image of size 356×356, shown in Fig. 4. Fig. 5 shows sample secret image to hide inside cover image.

VI. CONCLUSION

Biometric Steganography is presented that uses skin 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.

It is used to hide the date further by using various types of Steganography and biometrics

REFERENCES

[1.] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric Inspired digital image Steganography", in: Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'08), Belfast, 2008, pp. 159-168.

[2.] Petit colas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petit colas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

[3.] Lin, E. T. and Delp, E. J.:"A Review of Data Hiding in Digital Images". Retrieved on 1.Dec.2006 from Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999

[4.] Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998.

[5.] Fridrich, J., Goljan, M. and Du, R.., (2001). "Reliable Detection of LSB Steganography in Grayscale and Color Images." Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.

[6.] Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290

[7.] Chang, C. C., Chen, T.S and Chung, L. Z., "A Steganographia method based upon JPEG and quantization table modification," Information Sciences, vol.[4], pp. 123-138(2002).

[8.] Provos, N. and Honey man, P: "Hide and Seek: An introduction to Steganography". IEEE security and privacy, 01 (3): 32-44, May-June 2003

[9.] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography" , School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, BT48 7JL, Londonderry, Northern Ireland, UK,2008

[10.] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009

[11.] Sobottka, K. and Pitas, I.:"Extraction of facial regions and features using color and shape information." Proc. IEEE International Conference on Image Processing, pp. 483-486. (1996)