**IMAGE STEGANOGRAPHY USING HIGH CAPACITY WAVELET ALGORITHM**

**CONTENTS**

**CHAPTER PAGE NO.**

**1. INTRODUCTION**

**ABSTRACT**

**2. LITERATURE SURVEY**

**ABSTRACT:**

A new high capacity method for transform domain imagesteganography is introduced in this paper. The proposed steganography algorithm works on the wavelet transform coefficients of the original image to embed the secret data. As compared to current transform domain data hiding methods, this scheme can provide a larger capacity for data hiding without sacrificing the cover image quality. This is achieved through retaining integrity of the wavelet coefficients at high capacity embedding. This improvement to capacity-quality trading-off interrelation is analyzed in detailed and experimentally illustrated in the paper.

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) colour 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 subbands. 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.

**CHAPTER - I**

**INTRODUCTION**

**1. introduction**

**1.1 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](http://en.wikipedia.org/wiki/Security_through_obscurity). The word *steganography* is of [Greek](http://en.wikipedia.org/wiki/Ancient_Greek) origin and means "concealed writing" from the Greek words *steganos* (στεγανός) meaning "covered or protected", and *graphein* (γράφειν) meaning "to write". The first recorded use of the term was in 1499 by [Johannes Trithemius](http://en.wikipedia.org/wiki/Johannes_Trithemius) in his [*Steganographia*](http://en.wikipedia.org/wiki/Johannes_Trithemius#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 *covertext* and, classically, the hidden message may be in [invisible ink](http://en.wikipedia.org/wiki/Invisible_ink) between the visible lines of a private letter.

The advantage of steganography, over [cryptography](http://en.wikipedia.org/wiki/Cryptography) alone, is that 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](http://en.wikipedia.org/wiki/Encryption) is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th [pixel](http://en.wikipedia.org/wiki/Pixel) to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

**1.2 STEGANOGRAPHIC TECHNIQUES**

**1.2.1 Ancient steganography**

The first recorded uses of steganography can be traced back to 440 BC when [Herodotus](http://en.wikipedia.org/wiki/Herodotus) mentions two examples of steganography in [*The Histories of Herodotus*](http://en.wikipedia.org/wiki/The_Histories_of_Herodotus). [Demaratus](http://en.wikipedia.org/wiki/Demaratus) sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. [Wax tablets](http://en.wikipedia.org/wiki/Wax_tablet) were in common use then as reusable writing surfaces, sometimes used for [shorthand](http://en.wikipedia.org/wiki/Stenography). Another ancient example is that of [Histiaeus](http://en.wikipedia.org/wiki/Histiaeus), who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the [Persians](http://en.wikipedia.org/wiki/Persian_Empire)

### 1.2.2 Physical steganography

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](http://en.wikipedia.org/wiki/Wax_tablet): in ancient [Greece](http://en.wikipedia.org/wiki/Greece), people wrote messages on the wood, then covered it with [wax](http://en.wikipedia.org/wiki/Wax) upon which an innocent covering message was written.
* Hidden messages on messenger's body: also used in ancient Greece. [Herodotus](http://en.wikipedia.org/wiki/Herodotus) tells the story of a message [tattooed](http://en.wikipedia.org/wiki/Tattoo) on a [slave](http://en.wikipedia.org/wiki/Slave)'s [shaved](http://en.wikipedia.org/wiki/Shaving) head, hidden by the growth of his hair, and exposed by shaving his head again. The message allegedly carried a warning to Greece about [Persian](http://en.wikipedia.org/wiki/Persian_Empire) [invasion](http://en.wikipedia.org/wiki/Invasion) [plans](http://en.wikipedia.org/wiki/Plan). This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.
* In WWII, the French Resistance sent some messages written on the backs of couriers using invisible ink.
* Hidden messages on paper written in [secret inks](http://en.wikipedia.org/wiki/Invisible_ink), under other messages or on the blank parts of other messages.
* Messages written in Morse code on knitting [yarn](http://en.wikipedia.org/wiki/Yarn) and then knitted into a piece of clothing worn by a courier.
* Messages written on the back of [postage stamps](http://en.wikipedia.org/wiki/Postage_stamp).
* During and after [World War II](http://en.wikipedia.org/wiki/World_War_II), [espionage](http://en.wikipedia.org/wiki/Espionage) agents used photographically produced [microdots](http://en.wikipedia.org/wiki/Microdot) to send information back and forth. Microdots were typically minute, approximately less than the size of the [period](http://en.wikipedia.org/wiki/Full_stop) produced by a [typewriter](http://en.wikipedia.org/wiki/Typewriter). WWII microdots needed to be embedded in the paper and covered with an adhesive (such as [collodion](http://en.wikipedia.org/wiki/Collodion)). This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
* During [World War II](http://en.wikipedia.org/wiki/World_War_II), a spy for [Japan](http://en.wikipedia.org/wiki/Japan) in [New York City](http://en.wikipedia.org/wiki/New_York_City), [Velvalee Dickinson](http://en.wikipedia.org/wiki/Velvalee_Dickinson), sent information to accommodation addresses in neutral [South America](http://en.wikipedia.org/wiki/South_America). She was a dealer in [dolls](http://en.wikipedia.org/wiki/Doll), and her letters discussed how many of this or that doll to ship. The stegotext was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
* Cold War counter-propaganda. In 1968, crew members of the [USS Pueblo (AGER-2)](http://en.wikipedia.org/wiki/USS_Pueblo_%28AGER-2%29) intelligence ship held as prisoners by [North Korea](http://en.wikipedia.org/wiki/North_Korea), communicated in sign language during staged photo opportunities, informing the [United States](http://en.wikipedia.org/wiki/United_States) they were not defectors but rather were being held captive by the North Koreans. In other photos presented to the US, crew members gave "[the finger](http://en.wikipedia.org/wiki/The_finger)" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

### 1.2.3 Digital 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](http://en.wikipedia.org/wiki/Image_noise) images or sound files.
* Concealing data within encrypted data or within random data. The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the [one-time pad](http://en.wikipedia.org/wiki/One-time_pad) generates ciphertexts that look perfectly random if you don't have the private key).
* [Chaffing and winnowing](http://en.wikipedia.org/wiki/Chaffing_and_winnowing).
* [Mimic functions](http://en.wikipedia.org/wiki/Mimic_function) convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a [ciphertext-only attack](http://en.wikipedia.org/wiki/Ciphertext-only_attack).
* Concealed messages in tampered executable files, exploiting redundancy in the targeted [instruction set](http://en.wikipedia.org/wiki/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 keypresses in some applications ([telnet](http://en.wikipedia.org/wiki/Telnet) or [remote desktop software](http://en.wikipedia.org/wiki/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.
* Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non-human adversary/warden.
* [Blog](http://en.wikipedia.org/wiki/Blog)-Steganography. Messages are [fractionalized](http://en.wikipedia.org/w/index.php?title=Fractionalized&action=edit&redlink=1) and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole [blogosphere](http://en.wikipedia.org/wiki/Blogosphere).

### 1.2.4 Network steganography

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. This nomenclature was originally introduced by Krzysztof Szczypiorski in 2003. Contrary to the typical steganographic 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](http://en.wikipedia.org/wiki/Protocol_Data_Unit)), to the time relations between the exchanged PDUs, or both (hybrid methods).

Moreover, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol steganography.

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

* Steganophony - the concealment of messages in [Voice-over-IP](http://en.wikipedia.org/wiki/Voice-over-IP) conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called LACK - Lost Audio Packets Steganography), or, alternatively, hiding information in unused header fields.
* WLAN Steganography – the utilization of methods that may be exercised to transmit steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks) .

### 1.2.5 Printed steganography

Digital steganography output may be in the form of printed documents. A message, the [*plaintext*](http://en.wikipedia.org/wiki/Plaintext), may be first encrypted by traditional means, producing a [*ciphertext*](http://en.wikipedia.org/wiki/Ciphertext). Then, an innocuous *covertext* is modified in some way so as to contain the ciphertext, resulting in the *stegotext*. For example, the letter size, spacing, [typeface](http://en.wikipedia.org/wiki/Typeface), or other characteristics of a covertext 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](http://en.wikipedia.org/wiki/Francis_Bacon) developed [Bacon's cipher](http://en.wikipedia.org/wiki/Bacon%27s_cipher) as such a technique.

The ciphertext produced by most digital steganography methods, however, is not printable. Traditional digital methods rely on perturbing noise in the channel file to hide the message, as such, the channel file must be transmitted to the recipient with no additional noise from the transmission. Printing introduces much noise in the ciphertext, generally rendering the message unrecoverable. There are techniques that address this limitation, one notable example is ASCII Art Steganography.

### 1.2.6 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 codewords to more frequently occurring source symbols and longer length codewords to less frequently occurring source symbols.

### 1.2.7 Steganography using Sudoku Puzzle

This is the art of concealing data in an image using [Sudoku](http://en.wikipedia.org/wiki/Sudoku) which is used like a key to hide the data within an image. Steganography using sudoku puzzles has as many keys as there are possible solutions of a Sudoku puzzle, which is 6.71\times10^{21}. This is equivalent to around 70 bits, making it much stronger than the DES method which uses a 56 bit key.

## 1.3 Applications

### 1.3.1 Usage in modern printers

Steganography is used by some modern printers, including [HP](http://en.wikipedia.org/wiki/Hewlett-Packard) and [Xerox](http://en.wikipedia.org/wiki/Xerox) brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

### Example from modern practice

The larger the cover message is (in data content terms—number of [bits](http://en.wikipedia.org/wiki/Bit)) relative to the hidden message, the easier it is to hide the latter. For this reason, [digital pictures](http://en.wikipedia.org/wiki/Digital_image) (which contain large amounts of data) are used to hide messages on the [Internet](http://en.wikipedia.org/wiki/Internet) and on other communication media. It is not clear how commonly this is actually done. For example: a 24-bit [bitmap](http://en.wikipedia.org/wiki/Bitmap) will have 8 bits representing each of the three color values (red, green, and blue) at each [pixel](http://en.wikipedia.org/wiki/Pixel). If we consider just the blue there will be 28 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the [least significant bit](http://en.wikipedia.org/wiki/Least_significant_bit) can be used (more or less undetectably) for something else other than color information. If we do it with the green and the red as well we can get one letter of [ASCII](http://en.wikipedia.org/wiki/ASCII) text for every three [pixels](http://en.wikipedia.org/wiki/Pixel).

Steganography can be used for [digital watermarking](http://en.wikipedia.org/wiki/Digital_watermark), where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified (for example, [Coded Anti-Piracy](http://en.wikipedia.org/wiki/Coded_Anti-Piracy)), or even just to identify an image (as in the [EURion constellation](http://en.wikipedia.org/wiki/EURion_constellation))

### 1.3.2 Alleged use by terrorists

When one considers that messages could be encrypted steganographically in [e-mail](http://en.wikipedia.org/wiki/E-mail) messages, particularly [e-mail spam](http://en.wikipedia.org/wiki/E-mail_spam), the notion of junk e-mail takes on a whole new light. Coupled with the "[chaffing and winnowing](http://en.wikipedia.org/wiki/Chaffing_and_winnowing)" technique, a sender could get messages out and cover their tracks all at once.

[](http://en.wikipedia.org/wiki/File:Avatar_for_terrorist.png)

[http://bits.wikimedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Avatar_for_terrorist.png)

An example showing how terrorists may use [forum avatars](http://en.wikipedia.org/wiki/Avatar_%28computing%29) to send hidden messages. This avatar contains the message "Boss said that we should blow up the bridge at midnight." encrypted with <http://mozaiq.org/encrypt> using "växjö" as password.

In October 2001, the [*New York Times*](http://en.wikipedia.org/wiki/New_York_Times) published an article claiming that al-Qaeda had used steganography to encode messages into images, and then transported these via e-mail and possibly via [USENET](http://en.wikipedia.org/wiki/USENET) to prepare and execute the September 11, 2001 terrorist attack.

### 1.3.3 Alleged use by intelligence services

In 2010, the [Federal Bureau of Investigation](http://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) revealed that the [Russian foreign intelligence service](http://en.wikipedia.org/wiki/Foreign_Intelligence_Service_%28Russia%29) uses customized steganography software for embedding encrypted text messages inside image files for certain communications with "illegal agents" (agents under non-diplomatic cover) stationed abroad.

**CHAPTER – II**

**LITERATURE SURVEY**

**2. LITERATURE SURVEY**

**2.1 GOAL OF THE PROJECT**

To provide a larger capacity for data hiding without sacrificing cover image quality. This is achieved through retaining integrity of wavelet coefficients at high capacity embedding. The design of the wavelet algorithm is critical to the efficiency of data hiding steganography using discrete wavelet transform.

**2.2 OBJECTIVE**

Discrete wavelet transform uses the technique of wavelet transform representation of the cover image to conceal the data.To do this ,we adapt the amount of embedded data in each region of wavelet transform domain with a measure of noisiness in that region.We segment the wavelet representation of the image into 8x8 blocks and determine the capacity of each block , in terms of bit per pixel , using the BPCS.

**2.3 Implementation plan**

The implementation can be done by using Matrix Laboratory ( MATLAB ) . It is a great tool for simulation and data analysis . It provides a concise matrix notation without the usage of loops . It also provides a easy visualization of the expected results .

**2.4 Phase Description**

|  |  |  |
| --- | --- | --- |
| **Phase** | **Task** | **Description** |
| Phase 1 | Analysis | Analyze the information given in the IEEE paper. |
| Phase 2 | Literature survey | Collect raw data and elaborate on literature surveys. |
| Phase 3 | Design | Assign the module and design the process flow control. |
| Phase 4 | Implementation | Implement the code for all the modules and integrate all the modules. |
| Phase 5 | Testing | Test the code and overall process weather the process works properly. |
| Phase 6 | Documentation | Prepare the document for this project with conclusion and future enhancement. |

**CHAPTER – III**

**SYSTEM STUDY**

**2.2 PROPOSED SYSTEM**

**2.2.1 OVERVIEW**

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) colour 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 subbands. 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.

**2.2.2 Skin Colour Tone Detection**

A skin detector typically transforms a given pixel into an appropriate colour 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 colour class in the colour space. Although this is a straightforward process has proven quite challenging. Therefore, important challenges in skin detection are to represent the colour in a way that is invariant or at least insensitive to changes in illumination and another challenge comes from the fact that many objects in the real world might have skin-tone colours. This causes any skin detector to have much false detection in the background if the environment is not controlled.

The simplest way to decide whether a pixel is skin colour or not is to explicitly define a boundary. RGB matrix of the given colour image can be converted into different colour spaces to yield distinguishable regions of skin or near skin tone. There exists several colour spaces. Mainly two kinds of colour 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 colour constantly resides in a certain range within those two colour spaces. Colour space used for skin detection in this work is HSV. Any colour image of RGB colour space can be easily converted into HSV Colour space. Sobottaka and Pitas defined 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:

Smin= 0.23, Smax =0.68, Hmin =00 and Hmax=500

**2.2.3 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

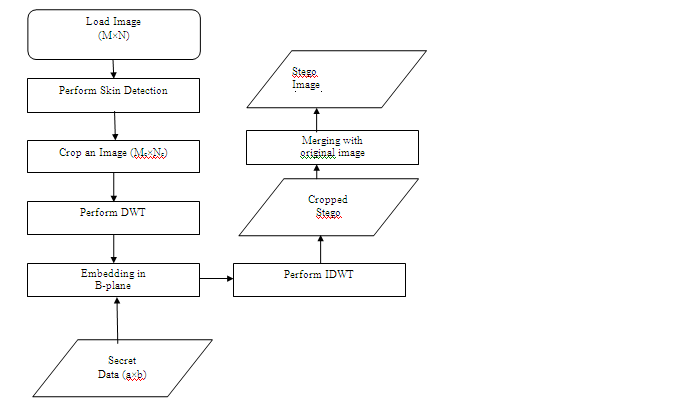
Since Human eyes are much more sensitive to the low frequency part (LL subband) we can hide secret message in other three parts without making any alteration in LL subband. As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn’t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

**2.2.4 Embedding Process**

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

C= {xij, yij, zij |1 ≤ i ≤ M, 1 ≤ j ≤ N, xij, yij, zij Є {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.



**Flowchart for embedding process**

**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 as we have to perform DWT later and cropped area should contain skin region such as face, hand etc since we will hide data in skin pixels of one of the sub-band of DWT. Here cropping is performed for security reasons. Cropped rectangle will act as key at receiving side. If it knows then only data retrieval is possible. Eavesdropper may try to perform DWT on whole image; in such a case attack will fail as we are applying DWT on specific cropped region only

**Step 3**

Apply DWT to only cropped area (Mc×Nc) not whole image (M×N). This yields 4 sub-bands denoted as HLL, HHL, HLH, and HHH. (All 4 sub-bands are of same size of Mc/2, NC/2). Payload of image to hold secret data is determined based on no. of skin pixels present in one of high frequency sub-band in which data will be hidden.

**Step 4**

Perform embedding of secret data in one of sub-band that we obtained earlier by tracing skin pixels in that sub-band. Other than the LL, low frequency sub-band any high frequency sub-band can be selected for embedding as LL sub-band contains significant information. Embedding in LL sub-band affects image quality greatly. We have chosen high frequency HH sub-band. While embedding, secret data will not be embedded in all pixels of DWT subband but to only those pixels that are skin pixels. So here skin pixels are traced using skin mask detected earlier and secret data is embedded. Embedding is performed in G-plane and B-plane but strictly not in R-plane as contribution of R plane in skin colour is more than G or B plane. So if we are modifying R plane pixel values, decoder side doesn’t retrieve data at all as skin detection at decoder side gives different mask than encoder side.

**Step 5**

Perform IDWT to combine 4 sub-bands.

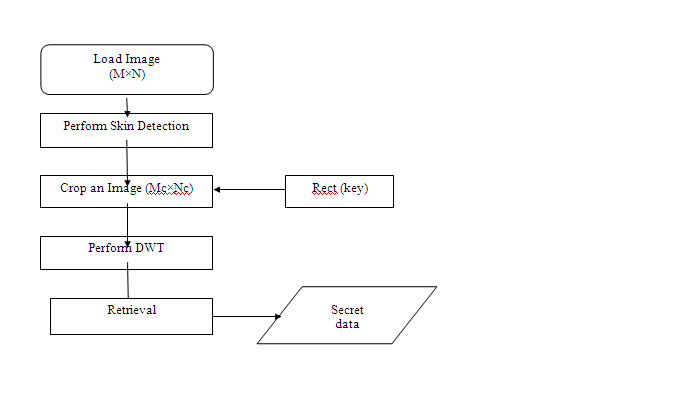
**Step 6**

A cropped stego image of size Mc×Nc is obtained in above step (step 5). This should be similar to original image after visual inspection but at this stage it is of size Mc× Nc, So 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. Thus a stego image is ready for quality evaluation.

**2.2.5 Extraction Process**

Secret data extraction is explained as follows:

24 bit colour 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



**Flowchart for extraction process**

**3. System Study**

**3.1 Existing system:**

In water marking based on multiband wavelets and empirical mode decomposition there is high bit error rate percentage under some geometric error distortion attacks such as rotating, bending, cropping and resizing due to geometric structure of the multi band wavelet decomposition of an image.

In reversible image water marking based on integer to integer wavelet transform, the water mark that was embedded into an image was completely visible but could be removed since it was embedded in a revisable manner.

**CHAPTER – IV**

**CONCLUSION**

**4. CONCLUSION**

We have introduced a new high capacity steganography method in wavelet domain. In order to achieve a higher quality of the stego image, we firstly estimate the capacity of each DWT block using the BPCS. The embedding process is then performed over the whole block, rather than in its bit-planes.This approach to the embedding ensures that no noisy bit-plane is left unused. Therefore, we achieve a much greater capacity as compared to that offered by previous methods, as confirmed by our analysis and experiments. The proposed approach to the embedding process may also be extended to other transform

domains to improve the compromising interrelation between capacity and imperceptibility in image steganography.

**Chapter – V**

**references**

**5. References**

[1] D. Artz, “Digital steganography: hiding data within data,” *IEEE Internet*

*Computing*, pp.75-80, May-June 2001.

[2] L. Sunil, C.D.Yoo, T.Kalker, “Reversible Image Watermarking Based on

Integer-to-Integer Wavelet Transform*”, IEEE Transaction of information,*

*forensics and security ,* September 2007.

[3] T. G. Gao, Q. L. Gu, “Reversible watermarking algorithm based on

wavelet lifting scheme,” *Wavelet analysis and pattern recognition*

*conference*, November 2007.

[4] N. Bi, Q. Sun, D. Huang, Z. Yang and J. Huang, “Robust watermarking

based on multiband wavelets and empirical mode decomposition,” *IEEE*

*transaction on image processing*, August 2007.

[5] S. E. El-Khamy, M. Khedr, A. AlKabbany, “A hybrid fractal-wavelet

data hiding technique” *25th NRCS*, March 2008.

[6] G. Hay-ying, X. Yin, L. Xu and L. Guo-qiang, “A steganographic

algorithm for JPEG2000 image,” *Conference on computer science and*

*software engineering*, 2008.

[7] M. K. Ramani, E. V. Prasad, S. Varadarajan, “Steganography using

BPCS to the integer wavelet transformed image” *IJCSNS*, July 2007.

[8] E. Kawaguchi and R. O. Eason, “Principle and application of BPCSsteganography,”

*in Proc. SPIE, vol* 3529, pp 464-473, 1998.

[9] A. R. Calderbank, 1. Daubechies, W. Sweldens and B. Yeo., "Wavelet

transforms that map integers to integers". Applied and Computational

*Harmonic Analysis,* vol.5, noJ, pp.332-369, 1998.

[10] R. O. El Safy, H.H. Zayed, A. El Dessouki, “An adaptive steganographic

technique based on integer wavelet transform,” 2009.

[11] S. Sarreshtedari, M. Ghotbi, S. Ghaemmaghami, “One-third probability

embedding: less detectable steganography,” *IEEE International*

*conference on multimedia and expo*, July 2009.