An Image Hiding Algorithm Using DWT Skin Tone Detection and SHA-512

REKHA NAGAR
COMPUTER SCIENCE DEPARTMENT
GURGAON INSTITUTE OF TECHNOLOGY AND MANAGEMENT
GURGAON, HARYANA
INDIA
rekha.nagar7jan@gmail.com

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 an algorithm to hide the data into cover image which is converted from RGB to YCbCr. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding so skin tone detection is performed using YCbCr Yellow, Chromatic blue,Chromatic red) color space. Additionally secret data encrypted by SHA-512 Algorithm embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine transform). Secret Encrypted data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. 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.**

Keywords: Biometrics; Skin tone detection; DWT; DCT; Security; PSNR.

I. INTRODUCTION

In this highly digitalized world, the Internet serves as an important role for data transmission and sharing. Some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-known procedure for secured data transmission and frequently used encryption methods include RSA, DES (Data encryption standard). Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach called "steganography" arises. 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.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.

There are two things that need to be considered while designing the steganographic system: Invisibility: Human eyes cannot distinguish the difference between original and stego image. (b) Capacity: The more data an image can carry better it is. However large embedded data may degrade image quality significantly. A modern steganography system contains following modules.. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes .

Rest of the paper is organized as follows. Section II presents Previous stegnography methods. In next section proposed method is described in detail with skin tone detection, DWT,embedding and extraction procedure step by step and

demonstrated the experimental results. Finally conclusions are provided in next section.

II. PAST STEGANOGRAPHY METHODS

A. Steganography in Spatial Domain

This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a graylevel image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so embedding procedure does not affect the original pixel value greatly [5]. The mathematical representation for LSB is:

$$xi' = xi - xi \bmod 2k + mi \quad (1)$$

In equation (1), *xi' represents* the *i* th pixel value of the stego-image and *xi represents* that of the original coverimage. *mi 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:

$$mi = xi \bmod 2k \quad (2)$$

Hence, a simple permutation of the extracted *mi gives* us the original confidential data [6]. 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.

B. *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 [7].

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.

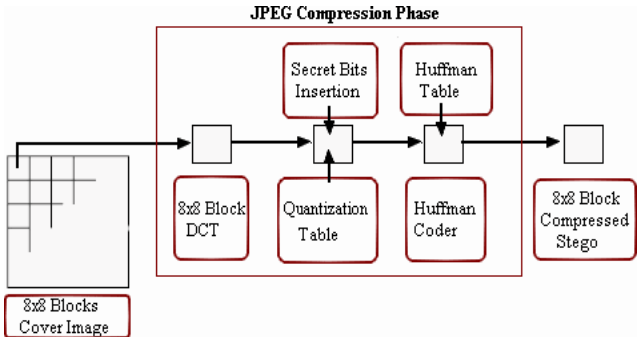


Figure 1. Data Flow Diagram showing a general process of embedding in the frequency domain.

C. *Adaptive Steganography*

Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" [8] and "Masking" [4]. This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

III. PROPOSED METHOD

Introduces a replacement technique of embedding secret knowledge inside skin because it isn't that a lot of sensitive to HVS (Human Visual System) [1].This takes advantage of life science options like skin tone, rather than embedding knowledge anyplace in image, knowledge are going to be embedded in hand-picked regions. Summary of technique is concisely introduced as follows. Initially skin tone detection is performed on input image victimisation YCbCr(Yellow, Chromatic blue ,Chromatic red) color area. Second cowl image is remodeled in frequency domain. This can be performed by applying Haar-DWT, the only DWT on image resulting in four subbands. Then payload (number of bits within which we will hide data) is calculated. Actually we discover the dimensions of concealing image. Finally secret knowledge embedding is performed in one amongst the high frequency sub-band by tracing skin pixels therein band. Here embedding method affects solely sure Regions of Interest (ROI) instead of the complete image. Therefore utilizing objects inside pictures are often a lot of

advantageous. This can be additionally referred to as as Object orienting steganography .

A. Colouring Tone Detection

A skin detector usually transforms a given pel into associate degree acceptable color area so uses a skin classifier to label the pel whether or not it's a skin or a non-skin pel. A skin categoryifier defines a call boundary of the colouring class within the color area. Though this is often a simple method has verified quite difficult. Therefore, necessary challenges in skin detection area unit to represent the colour in away that's invariant or a minimum of insensitive to changes in illumination.[2] and Another challenge comes from the actual fact that a lot of objects within the planet might need skin-tone colours. This causes any skin detector to own a lot of false detection within the background if the setting isn't controlled [3]. The best thanks to decide whether or not a pel is colouring or not is to expressly outline a boundary. RGB matrix of the given color image will be reborn into YCbCr color areas to yield distinguishable regions of skin or close to skin tone .Mainely 2 sorts of color areas area unit exploited within the literature of bioscience that area unit HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) areas. It's by experimentation found and in theory verified that the distribution of human colouring perpetually resides in a very bound vary among those 2 color areas . Color area used for skin detection during this work is YCbCr (Yellow, Chromatic Blue, Chromatic red). Any color image of RGB color area will be simply reborn into YCbCr (Yellow, Chromatic Blue, Chromatic red) color area. Sobottaka and Pitas outlined a face localization supported HSV. They found that human flesh will be associate degree approximation from a sector out of a polygonal shape with the constraints:

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

1) B. A New Image Secret Writing Rule

Secure Hash Algorithm is a Class of cryptographic hash functions implemented by the national Institute of Standards and Technology and published by federal information processing standard in 1993, and generally told as SHA1.The actual standards documents is called Secure Hash Standard document.SHA -1 generates a hash length of 160 bits. In 2002 NIST generates a new version of the standard FIPS 180-2, that defined three new standards of SHA, with hash lengths of 256, 384 and 512 bits, known as SHA-256 standard, SHA-384 standard, and SHA-512 standard. These new standards have the same structure and use the same types of arithmetic and binary operations as SHA1.

This proposal exploits the strength of a 1D hash rule, SHA-2, and extends it to handle 2nd information like pictures. SHA functions "are extremely versatile primitives which will be wont to acquire privacy, integrity and authenticity". The vector H, treated as a string of hex characters, is then reborn to its decimal version and eventually reworked to slightly stream matrix of fastened dimension [8x32]. Parallel to the current, the first image A is reborn to slightly stream and reshaped to the order8 x MN . The partly extended key, herein K', remains short to accommodate the image bit stream. Therefore, the rule performs key full enlargement towards the required dimension, herein8 x MN . Obviously, this step would lead to repetitive patterns that may build the ciphered image vulnerable to attacks, a retardant that was severally detected in .

As such, pictures will be simply encoded firmly with word protection. Note that this theme with efficiency encrypts grayscale and binary pictures. However, for RGB pictures it's detected that victimization a similar word for the 3 primaries yields some traceable patterns transmitted from the first image, RGB colors area unit extremely related . This is often simply overcome through the subsequent 2 choices: either the user provides 3 words every of that encrypts one color channel or a lot of handily generates another 2 distinctive keys from the first provided password. As an example, one key will be utilized to come up with the subsequent completely different hash functions H(K),H(K) and H(H(K)) to code the R, G and B channels, severally. K denotes the provided key, the arrows indicate the string reading directions and H(H(•)) denotes double hashing. There area unit several applications for this extended 2nd SHA-2 rule, but this thesis concentrates exclusively on the strengthening of digital image steganography.

These are the steps:

Step 1: Append padding bits: The message is padded so that its length is congruent to 896

modulo1024.Padded is always added even if the message is already of the desired length. Append the size of the original message as an unsigned 64 bit integer.

Step 2:Append Length: A block of 128 bits is appended to the message. This block is treated as an unsigned 128 bit integer and contains the length of original message.

Step 3:Initialize hash buffer: A 512 bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers .

Step 4: Process message in 1024-bit blocks: The heart of the algorithm is a module that consists of 80 rounds. Each round takes as input the 512 – bit buffer value abcdefgh and updates the contents of the buffer.

Step 5: After all N 1024 –bit blocks have been

annoying interference whole. This disadvantage of DCT is eliminated victimization DWT. DWT applies on entire image. DWT offers higher energy compaction than DCT with none interference whole. DWT splits part into varied frequency bands referred to as sub bands referred to 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

3)

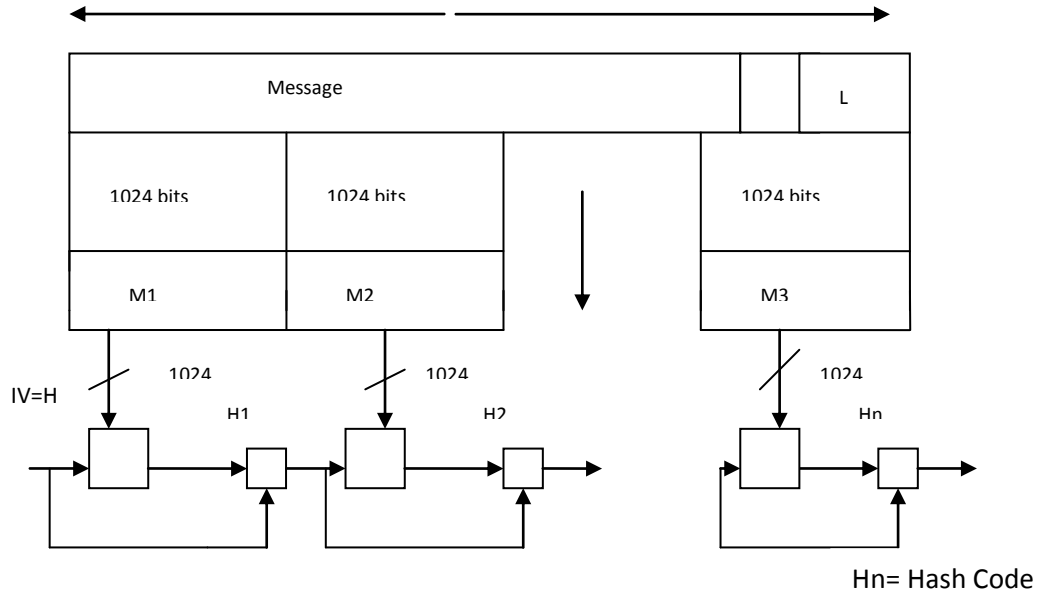


Fig 2: Message Digest Generation Using SHA2

2) processed , the output from the Nth stage is the 512 bit message digest.

C. Separate Moving Ridge Rework (DWT)

This is another frequency domain within which steganography will be enforced. DCT is calculated on blocks of freelance pixels, a writing error causes separation between blocks leading to

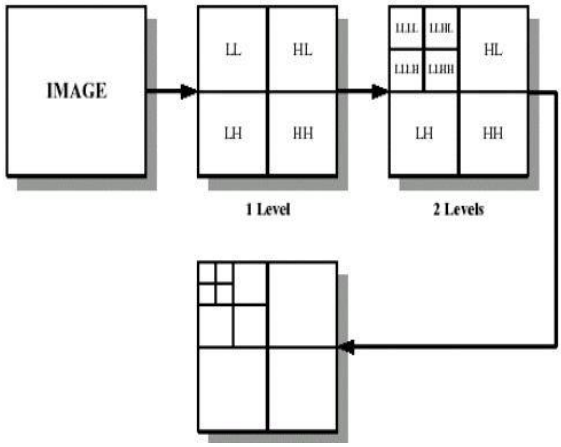


Figure 3: 2D DWT For Image

Since Human eyes area unit far more sensitive to the low frequency half (LL subband) we are able to hide secret message in alternative 3 elements while not creating any alteration in LL subband [5]. As alternative 3 sub-bands area unit high frequency sub-band they contain insignificant information. concealment secret information in these sub-bands doesn't degrade image quality That a lot of. DWT employed in this work is Haar-DWT, the best DWT.

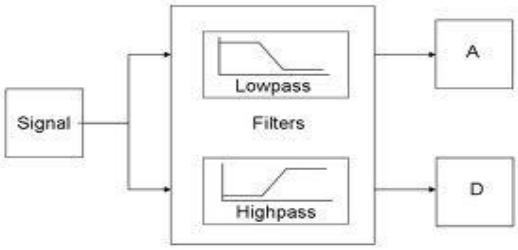


Figure 4: Low Pass Filter and High Pass Filter

It converts an input series x0, x1, ..xm, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series (of length n/2 each) given by

$$\mathbf{H_i} = \sum_{m=0}^{k-1} \mathbf{x_{2i-m} \cdot s_m(z)} \qquad (1)$$

$$\mathbf{L_i} = \sum_{m=0}^{k-1} \mathbf{x_{2i-m} \cdot t_m(z)} \qquad (2)$$

where sm(Z) and tm(Z) are called *wavelet filters*, K is the length of the filter, and i=0, ..., [n/2]-1.

In practice, such transformation will be applied recursively on the low-pass series until the desired number of iterations is reached.

IV. IMPLEMENTATION

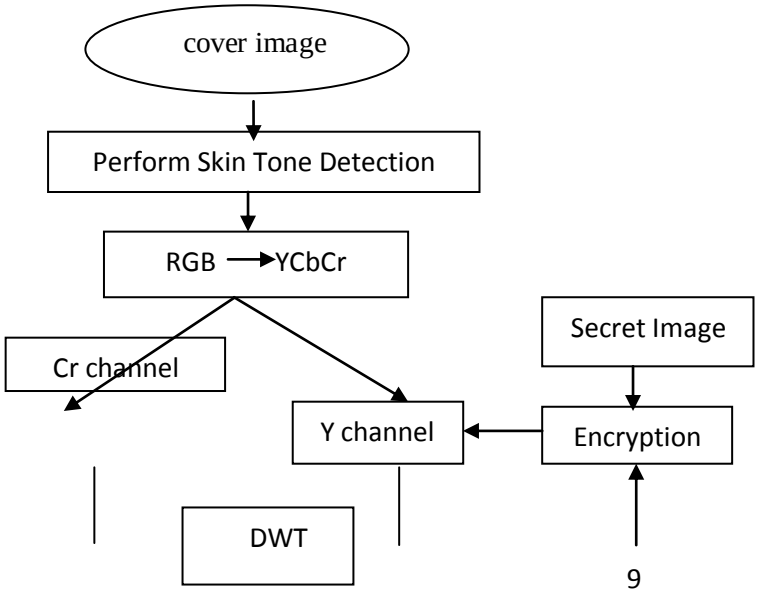
In this chapter the concept of object oriented is introduced in to information hiding in general and particular to steganography. The algorithm takes advantage of computer vision to orient the embedding process. Although any existing algorithm can benefit from this technique to enhance its performance against stagnalysis attacks. Furthermore, the chapter proposes enhancing steganography employing a new entity of security that encrypts the key image before embedding it within the original image. Various hash algorithms area unit offered like MD5, Message Digest five, and SHA-2, Secure Hash algorithmic program, that hash information strings, therefore ever-changing their state from being in a state of nature to a ostensibly unnatural state.

A hash perform is a lot of formally outlined as the mapping of bit strings of associate absolute finite length to strings of a set length . Here the aim is to increase SHA-2 to cipher 2nd digital information, the nomenclature and functions area unit delineate within the North American nation Secure Hash algorithmic program (SHA, 2001). The introduction of 2 transforms combined with the output of the SHA-2 algorithmic program creates a powerful image secret writing setting. Embedding Process

Suppose C is original 24-bit color 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 S is secret data. Here secret data considered is binary image of size a×b. Y and Cr are two channels.Fig. 1 represents flowchart of embedding process. Different steps of flowchart are given in detail below.



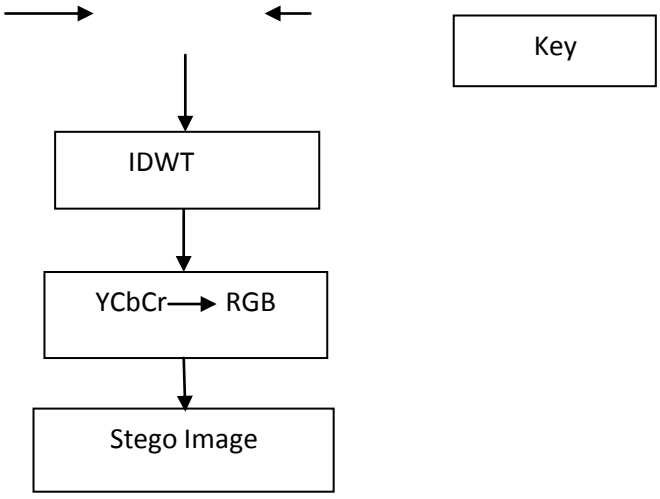


Figure 5 Flowchart of Embedding process

A. Proposed algorithm

1) Step 1*:* Once image is loaded, Transform the image in to luminance and chrominance (YCbCr) components .Apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.

2) Step 2*:* Apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.

3) Step 3*:* Apply DWT .This yields 4 sub-bands denoted as HLL,HHL,HLH,HHH . (All 4 sub-band 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.

4) 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. So here skin pixels are traced using skin mask detected earlier and secret data is embedded.

5) Step 5: Perform encryption with the help of key. Use Secure hash algorithm.

6) Step 6: Perform IDWT to combine 4 sub-bands.

7) Step 7: Thus a stego image is ready for quality evaluation.

B. *Extraction Process*

Detect the area of hiding image using key at encoding side. Detect the pixel of high frequency subband using DWT method. Then convert YCbCr in to RGB image. Extract the image.. Extraction procedure is represented using

Flowchart in Fig:

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

2) Step 2*:* Transform the image in to luminance and chrominance (YCbCr) components.

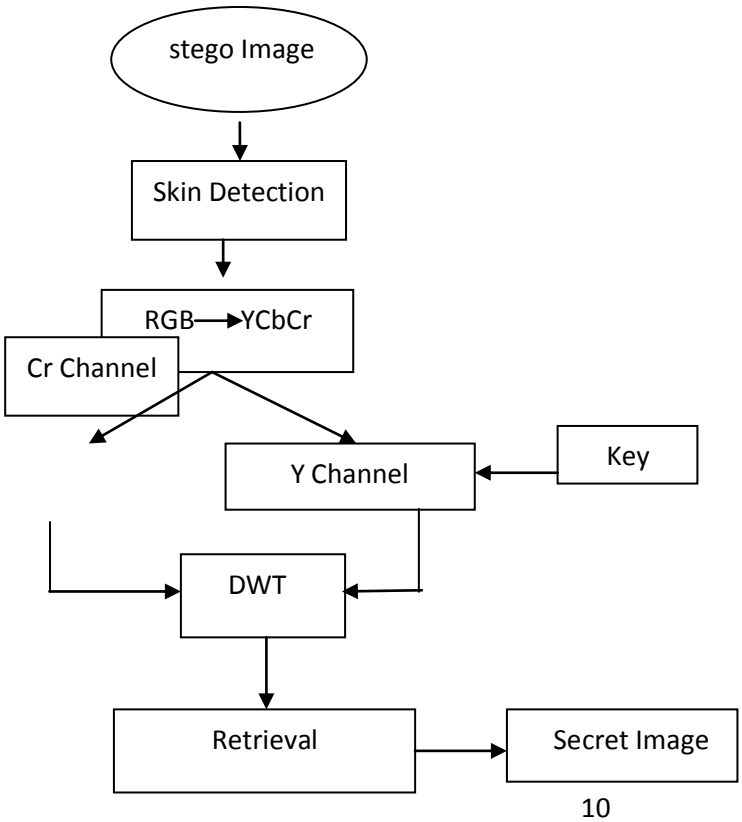


Figure 6 Flowchart of Decoding process

3) Step 3*:* Apply key on luminance components. Apply DWT .This yields 4 sub-bands denoted as HLL, HHL, HLH, HHH . (All 4 sub-band are of same size of Mc/2,Nc/2). Data is hidden in one of the high frequency subband. With the help of key extract the secret image from high frequency subband.

4) Step 4*:* Apply IDWT and convert the YCbCr image in to RGB image. Thus a secret image extracted.

V. RESULTS AND DISCUSSION

A. Embedding process:

1. Take the input image as cover image.
   - (i) We can Take .Jpeg, .Bmp as cover image.
   - (ii) Cover image should be a skin image.
   - (iii) Maximum Size = 669KB

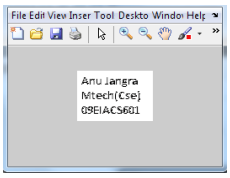


Fig. 7. Input image Fig. 8. Secret Image

2. Take the Secret image.

(i) Secret Image should be grayscale image. (ii) Secret Image should be any signature logo and secret code

(ii) Maximum size should be 9 KB.

3. There are many color spaces . But we are using YCbCr(Luminance , chrominance) color space And then transform input image in to YCbCr (luminance, chrominance) components. Skin tone segmentation on input image. Skin Classifier find the skin and non skin pixels. In figure calculated skin and non skin area.

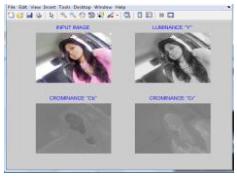


Fig. 9 Luminance and Chrominance Components

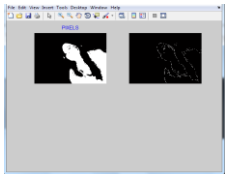


Fig. 10 Skin Tone Segmentation

4. DWT is the frequency domain approach in which steganography is implemented. Wavelets are the mathematical functions which transforms one functions representations to another.Apply DWT on the whole image (M×N). This yields 4 sub-bands denoted as HLL, HHL, HLH, HHH . (All 4 sub-band are of same size). 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.Encrypt *P* using the proposed encryption method to find *P'*. Secret data embedding in one of the high frequency sub-band by tracing skin pixels in that band.

5. After embedd the data behind the cover image .IDWT(Inverse discrete wavelet transform) is performed .Got the Steganographed Grayscale image.

Fig. 11 Steganographed Image

6. Convert Y'CbCr to RGB color space and obtain the final stego-image.

Fig. 12 Stego Image

B. Extraction Process:

1. Take the stego image behind that secret data is hidden.

Sr. No.	COVER IMAGES	PSNR(db)
1.		36
2.		36
3.		38
4.		37
5.		35

Fig. 13 Stego Image

2. Detecting the skin area by skin tone detection algorithm. Convert RGB image into YCbCr color space.Apply DWT(Discrete wavelet Transform) method on image . With the help of key extract the secret data from the stego image.

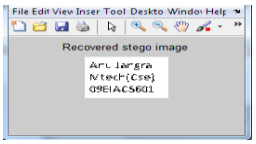


Fig. 14 Recovered Stego Image

PSNR(Peak Signal To Noise ratio) is calculated for final stego image resulted from a considered image and five more sample images. This PSNR for different cases is shown in table 1. Average PSNR of proposed method is calculated based on the obtained PSNR. PSNR values falling below 30dB indicate fairly a low quality. However, high quality strives for 35dB or more . It is defind as:

$$PSNR = 10\log_{10}\left(\frac{C^2_{max}}{MSE}\right)$$

Where MSE denotes the mean square error is given by:

Method	Type Of Transform	Image	PSNR (db)	Payload (bits)
Chang et al.,2007	DCT	Lena(512*512)	30.34	36,850
Proposed Method	DWT	Lena(512*512)	34.47	60,000

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2$$

Whre x and y are the image coordinates. M and N are the dimensions of the image.

Table 1 PSNR For Different Images In Proposed method

Cover Images	Size of Cover Object	Size of Hide Images	Capacity (bits)	MSE (db)	PSNR (db)
Image 1	440*330	45*39	24,576	57.12	34.05
Image 2	512*512	62*90	60,000	93.5	34.47
Image 3	256*256	76*94	80,000	15.23	36.33
Image 4	416*528	34*36	25,000	53.01	36.33
Image 5	432*528	51*29	29,000	54.01	35.30

Table 2 Capacity And PSNR Of 5 Stego Images In Proposed Method

Table 3 Distortion Comparision

VI. CONCLUSIONS & SUGGESTIONS FOR FUTURE WORK

Digital Steganography may be a fascinating scientific space which falls below the umbrella of security systems. We have got during this work some background discussions on algorithms of Steganography in digital imaging.

The rising methods such as DCT, DWT and accommodative Steganography don't seems to be straightforward target for attacks, particularly once when the hidden message is little. That is because they alter bits with in the remodel domain, therefore image distortion unbroken to a minimum. Typically these strategies tend to process a lower payload compared to spatial domain algorithms. In brief there has continually been a always been a trade off between lustiness and payload. Our purposed framework, relies on embedding within the DWT domain victimization skin tone detection in RGB successive image files. We have tendency to selected the latter to catch up on the restricted capability that edge embedding techniques demonstrate. We have a tendency to use the components of the image once concealing a message. This results in several exciting and difficult future analysis issues. In future this work will be extended to the embedding with in the edges drawn from skin portion.

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.

[2] Abbas Chedda, 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,2010

[3] Yun Q Shi,Ni "New lossless data hiding Algorithm Based on Histrogram Modification". International Conference on Information & Communication Technologies.

[4] A. Nag , S. Biswas, D. Sarkar, P.P.sarkar :"A novel technique for image steganography based on Block-DCT and Huffman Encoding". International journal of computer science and information technology , Volume 2, Number 3, june 2010.

[5] Chen,P. ,Y.and Liao,E.C., :"A new Algorithm for Haar Wavelet Transform," 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp.453-457(2002).

[6] Johnson, N. F. and Jajodia, S.:" Exploring Steganography: Seeing the Unseen". IEEE Computer, 31 (2): 26-34, Feb 2003.

[7] Yun Q. Shi1.: "Losless Data Hiding:Fundamentals, Algorithms And Applications. International Conference on Information & Communication Technologies": From Theory to Applications. Tongji University: April 19 - 23, 2004.

[8] N Verma :" Review of Steganography Techniques". International Conference on Workshop on Emerging Trends in Technology (2011).

[9] Anjali . Shejul, Umesh L. Kulkarni "A Secure Skin Tone based Steganography Using Wavelet Transform. International journal of computer theory and Engineering. Vol. 3, No. 1 ,Febuary, 2011.

[10] Paul Mc Kevitt:"Steganoflage: "Digital image steganography:Survey and Analysis of current methods" School of Computing & Intelligent Systems, University Of Ulster (US) 2009.

[11] Condell, J. ; Curran, K. ; McKevitt, P. : "Biometric inspired digital image steganography". Proceedings of 15th Annual IEEE International Conference and Workshop in Univ. of Ulster, Londonderry March2010.

[12] Shejul,Anjali .A. Kulkarni, U.L. : "A DWT based Approach for Steganography Using Biometrics". Proceedings of IEEE's International Conference on Data Storage and Data Engineering (DSDE) 9 - 10 Feb. 2010 .