ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

A JPEG Steganography Scheme Based on Skin Tone Detection

Swati Kumravat[1], Ms. Kavita Deshmukh[2]

M.Tech (I.T)-4th sem, LNCT, Bhopal, India[1]

Department of I.T, LNCT, Bhopal, India[2]

Abstract— Steganography is a process of hiding secret data into a cover medium so that invisible communication can be achieved. In this paper we present an efficient steganography method for JPEG images. This method uses JPEG image as a cover medium for hiding secret textual data. This JPEG steganography method is based on biometrics and to implement this skin tone detection biometric feature is used. In addition for secret data hiding Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) methods are used. And the performance of this JPEG steganography method is evaluated in terms of Peak-Signal-to-Noise Ratio (PSNR) and embedding capacity.

Keywords— Skin Tone Detection, DWT, LSB, MSE, PSNR.

I. INTRODUCTION

In this modern world, the Internet acts as a medium for data transmission and sharing. It is a global and publicized medium then also some secret information might be stolen, copied, modified, or destroyed by an unintended viewer. Thus, information security becomes an important issue. Encryption of information is a well-known procedure for protecting confidential information. Though encryption provides satisfactory security effect and it makes the secret information unreadable and unnatural. But usually this unreadable information catches the attention of some unintentional observers. For this reason "steganography" technique arises for information security [1]. Steganography means "covered message" and it involves conveying secret messages by apparently innocuous medium. The aim of steganography is to hide the existence of message [2].

Watermarking is another technique of data hiding which is closely related to steganography but used for different purposes. Digital watermarking is the method of embedding digital marks within a container so that embedded data can be extracted in a logical way, while not damage the container in any perceived way. Steganography uses cover medium to convey its messages. In contrast watermarking considers the cover medium as the significant information that is to be preserved. In Steganography purpose of embedded data is to convey secret message. In watermarking, purpose of embedded data is to provide some extra information about the cover image such as image owner to prove image's ownership to get control over the copy process of digital information. The object of communication in Steganography is the concealed message. In digital watermarking, the object of communication is the cover. In short, Steganography concentrated on the degree of invisibility while Watermarking concentrated on the robustness of the information and its ability to survive attacks of removal, such as image operations(rotation, cropping, filtering).A compromise between the embedding capacity, robustness and undetectability exists and can be determined before carrying out the communication. Fig. 1 shows trade off between capacity, robustness, undetectability and shows where Steganography and Watermarking resides [1].

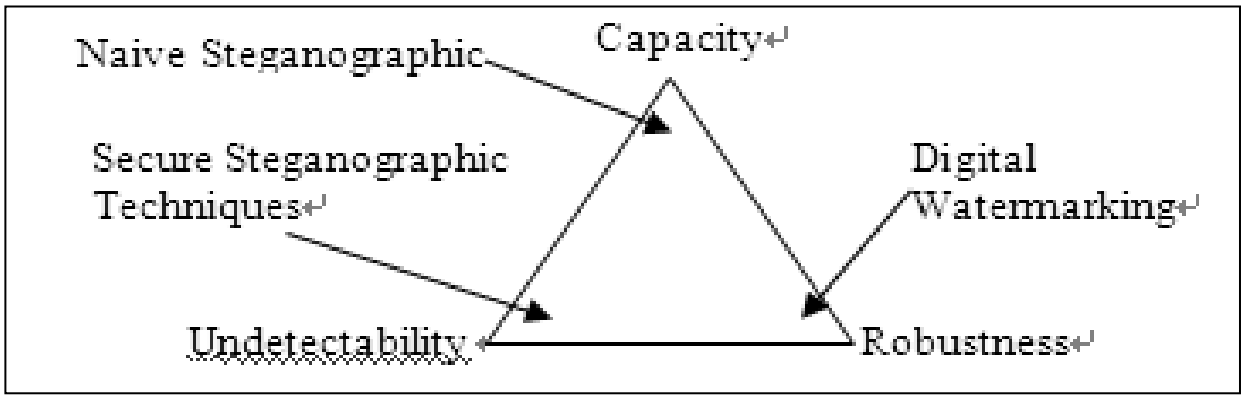

Fig.-1 Trade off between Embedding capacity, Robustness and Undetectability in Data Hiding [1]

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

JPEG (Joint Photographic Experts Group) is the most general image format for Internet and local usage because it provides large compression ratio and preserve high picture quality. Therefore, JPEG compressed images are the most appropriate cover images to be used for steganography. The design of our proposed steganography method is presented in Section III. The results of our experiment are discussed and shown in Section IV. Finally, the conclusion is presented in Section V.

II. RELATED WORK

In this section we describe some popular steganography algorithms, Skin tone detection, Discrete Wavelet Transform, Least significant bit embedding and optimal pixel adjustment. These are the base of our proposed method.

2.1 Popular Steganography Algorithms

A. JSteg

Among one of the first JPEG steganography algorithms JSteg comes. It was developed by Derek Upham. JSteg embeds message bits in LSB of the JPEG coefficients. JSteg doesn't randomize the index of JPEG coefficients to hide message bits. Hence, the alterations are concentrated to one part of the image if all the coefficients are not used. Using all the coefficients might eliminate this anomaly but will perturb too many bits to be easily detected. JSteg doesn't hide any message in DCT coefficients with value 0 and 1.This is to avoid changing too many zeros to 1's since number of zeros is extremely high as compared to number of 1's. Hence, more number of zeros will be altered to 1's as compared to 1's being altered to zeros. To hide a message bit, it just changes the LSB of the DCT coefficient with the message bit to embed [3].

B. JP Hide and Seek

"JP Hide and Seek" is another JPEG steganography algorithm, improving secrecy by using the Blowfish encryption algorithm to randomize the index for storing the message bits. This guarantees that the alteration are not concentrated in any particular segment of the image, a disadvantage that made Jsteg more easily detectable. Same as the JSteg algorithm, it also conceals data by replacing the LSB of the DCT coefficients. The only difference is that it also uses all coefficients including the ones with value 0 and 1.The maximum capacity of "JP Hide and Seek" is around 10% to minimize visual and statistical changes. Hiding extra data can lead to visual alterations in the image which can be identified by the human eye [5].

C. F5

F5 is one of the most popular algorithms, and is untraceable using the chi-square method. F5 applies matrix encoding along with permutated straddling to encrypt message bits. Permutated straddling assists distribute the alterations evenly throughout the stego image. Matrix encoding can hide K bits by altering only one of $n = 2K - 1$ places. This guarantees less coefficient alterations to encode the same quantity of message bits. F5 also avoids making alterations to any DC coefficients and coefficients with zero value. If the value of the message bit doesn't equal to the LSB of the coefficient, the coefficient's value is constantly decremented, so that the general nature of the histogram is preserved. However, a one can alter to a zero and therefore the same message bit must be embedded in the successive coefficients until its value becomes non-zero, because zero coefficients are ignored on decoding. However, this method changes the histogram of JPEG coefficients in a predictable manner. This is because of the shrinkage of one's converted to zeros increases the number of zeros while decreases the histogram of other coefficients and hence can be detected once an estimate of the original histogram is obtained [7].

D. Outguess

Outguess, proposed by Niels Provos, was first algorithm to use first order statistical restoration method. The algorithm works in two stages, the embed stage and the restoration stage. After the embedding stage, the algorithm makes alterations to the unvisited coefficients to match it to the cover histogram using a random walk. Outguess does not make any alteration to coefficients with 1 or 0 value. It uses an error threshold for each coefficient to determine the amount of alteration which can be tolerated in the stego histogram. If a coefficient alteration ($2i \rightarrow 2i + 1$) results in exceeding of threshold, it will attempt to compensate for the alteration with one of the neighbouring coefficients ($2i + 1 \rightarrow 2i$) in the same iteration. But, it may not be capable to do so since the chances of finding a coefficient to compensate for the alterations is not 1. At the end of the embedding process, it tries to fix all the remaining faults. But, not all the improvement might be possible if the error threshold is too large. This means that algorithm may not be able to re-establish the histogram absolutely as contrast to the cover image. If the threshold is also small, the data capacity can reduce radically since there will be too many unused coefficients. Also, the portion of coefficients used to hold the message, α, is inversely proportional to the total number of coefficients in the image. This means Outguess will carry out poorly when the amount of available coefficients is too large. Since, Outguess conserve only the first order histogram; it is detectable using second order statistics and image cropping techniques to guess the cover image [9].

E. Steghide

Another algorithm is Steghide, where the authors claim to use exchanging coefficients rather than overwriting them

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

to embed bits in DCT coefficients. They use graph theory methods where two inter-changeable coefficients are connected by an edge in the graph with coefficients as vertices of the graph. The embedding is done by solving the combinatorial problem of maximum cardinality matching. If a coefficient needs to be altered in order to embed the message bit, it is substituted by one of the other coefficients associated through the graph. This guarantees that the global histogram is conserved and hence it is hard to notice any distortion using first order statistical analysis. However, exchanging two coefficients is effectively changing two coefficients which will distort the intra/inter block dependencies. The capacity of Steghide is only 5.86% with respect to the cover file size as compared to J3 which has a capacity of 9% [11].

2.2 Skin Tone Detection

A skin detector typically converts a given pixel into a suitable 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 describes a decision limit of the skin color class in the color space. Though this is a straightforward process has proven quite challenging. Consequently, important challenges in skin detection are to represent the color in a way that is invariant or at least insensitive to changes in illumination and another challenge is that many objects in the real world might have skin-tone colors. This causes any skin detector to have a large amount false detection in the background if the environment is not controlled. The simplest way to find skin pixel is to explicitly define a limit. RGB matrix of the given color image can be transformed into different color spaces to produce distinguishable regions of skin or near skin tone. There are several color spaces. Mainly two types 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. Sobottaka and Pitas defined a face localization based on HSV [10]. 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 =0^0 and Hmax=50^0 [10].

2.3 Discrete Wavelet Transform

Wavelet analysis can be used separated the information of an image into approximation and detailed sub signal. The approximation sub signal demonstrate the general trend of pixel value, and three detailed sub signal demonstrate vertical, horizontal and diagonal details or alterations in image. If these detail is very small than they can be set to zero without significantly changing the image. If the number of zeroes is higher than the compression ratio is also high. There is two variety of wavelet is used. First one is Continues wavelet transform and second one is discrete wavelet transform. Wavelet analysis is computed by filter bank. There is two type of filter which is as follows:

1) High pass filter: high frequency information is kept, low frequency information is lost.

2) Low pass filter: law frequency information is kept, high frequency information is lost.

So signal is effectively decomposed into two parts, a detailed part (high frequency) and approximation part (low frequency). Level 1 detail is horizontal detail, level2 detail is vertical detail and level 3 details is diagonal detail of the image signal [6].

In our steganography method we use Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Complete procedures of a 2-D Haar-DWT are described as follows [12]:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, do the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right as illustrated in Fig.-2. Repeat this operation until all the rows are processed. The pixel sums denote the low frequency part (denoted as symbol L) while the pixel differences denote the high frequency part of the original image (denoted as symbol H).

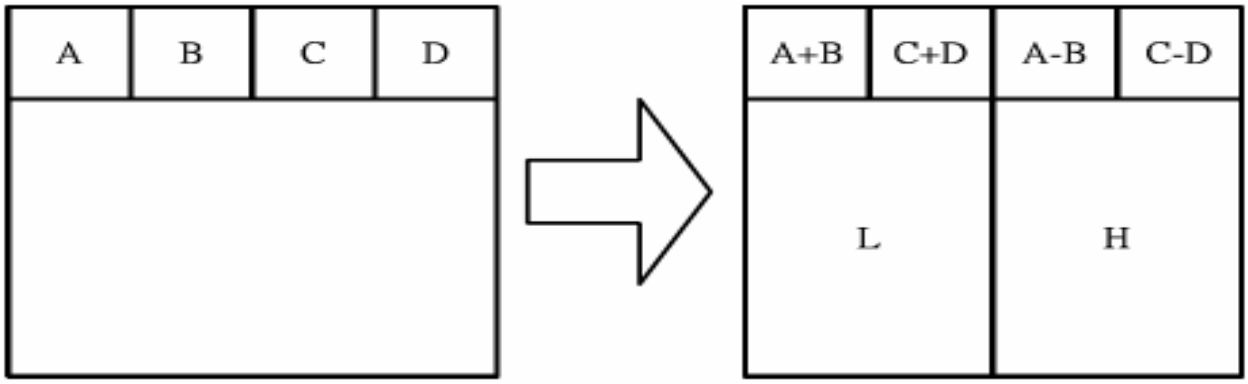

Fig.-2 the horizontal operation on the first row [12]

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Do the addition and subtraction operations on neighbouring pixels and then store the sum on the top and the difference on the bottom as illustrated in Fig.-3. Repeat this operation until all the columns are processed. Finally we will get 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence seems very similar to the original image.

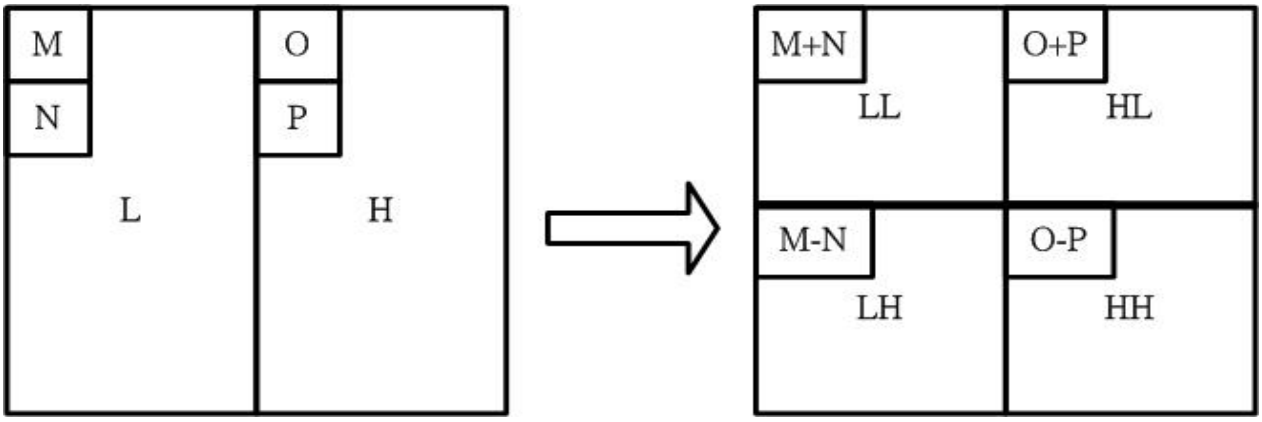

Fig.-3 the vertical operation [12]

2.4 Least Significant Bit Embedding

The most commonly used steganography technique is the method of LSB substitution. We use this method in our proposed steganography method. In a gray-level image, every pixel consists of 8 bits. One pixel can hence display 28 =256 variations. The weighting arrangement of an 8-bit number is shown in Fig.-4 [12].

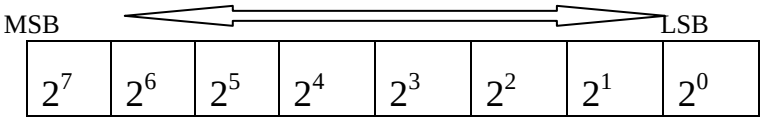

Fig.-4 Weighting of an 8-bit pixel

The basic concept of LSB embedding is to embed the secret data at the rightmost bits (bits with the smallest weighting) so that the embedding process does not change the original pixel value greatly. The mathematical representation for LSB method is:

$$X_i' = X_i - X_i \bmod 2^k + B_i \quad (1)$$

In Equation (1),
X_i' represents the i th pixel value of the stego-image, X_i represents that of the original cover-image, and B_i represents the decimal value of the i th block in secret data. The number of LSBs to be substituted is represented as k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$$B_i = X_i \bmod 2^k \quad (2)$$

Hence, a simple permutation of the extracted B_i gives us the original confidential data [12].

2.5 Optimal Pixel Adjustment

The Optimal Pixel adjustment (OPA) reduces the distortion caused by the LSB substitution method. In OPA technique the pixel value is adjusted after the concealing of the secret data is done to improve the quality of the stego image without disturbing the hidden data. Procedure for OPA is as follows [13]:

- Let n LSBs be substituted in each pixel.
- Let d= decimal value of the pixel after the substitution.
- d1 = decimal value of last n bits of the pixel.
- d2 = decimal value of n bits hidden in that pixel.

```
If (d1~d2) <= (2^n)/2
    then no adjustment is made in that pixel.
Else
    If (d1<d2)
        d = d – 2^n.
    If (d1>d2)
        d = d + 2^n.
```

This d is converted to binary and written back to pixel [13].

III. PROPOSED METHOD

Proposed method presents a method of data hiding in which secret data is embedded within skin region of image. This method uses skin tone detection, discrete wavelet transform, LSB substitution algorithm and optimal pixel adjustment. These are already described

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

above in related work, now we are going to elaborate embedding procedure and extraction procedure briefly.

A. *Embedding Procedure*

In the process of embedding following steps are involved (which is also depicted in Fig.-5):

1. First of all cover image of size (M × N) is loaded.
2. Then Skin tone detection is performed to find the skin region of cover image.
3. In the skin portion detected in previous step, cropping is performed. This is performed to ensure security by hiding data within limited skin pixel positions.
4. In this step histogram equalization is performed for enhancing the quality of cropped image.
5. In key generation step pseudo key is generated for encryption.
6. Discrete Wavelet Transformation is performed in this step.
7. Secret data is embedded using LSB^{+} matching.
8. To reduce the distortion caused by the LSB substitution method in this step we use optimum pixel adjustment (OPA).
9. Inverse DWT is performed.
10. Finally reconstruction of cover image with secret data is done. This reconstructed image is called Stego-image.

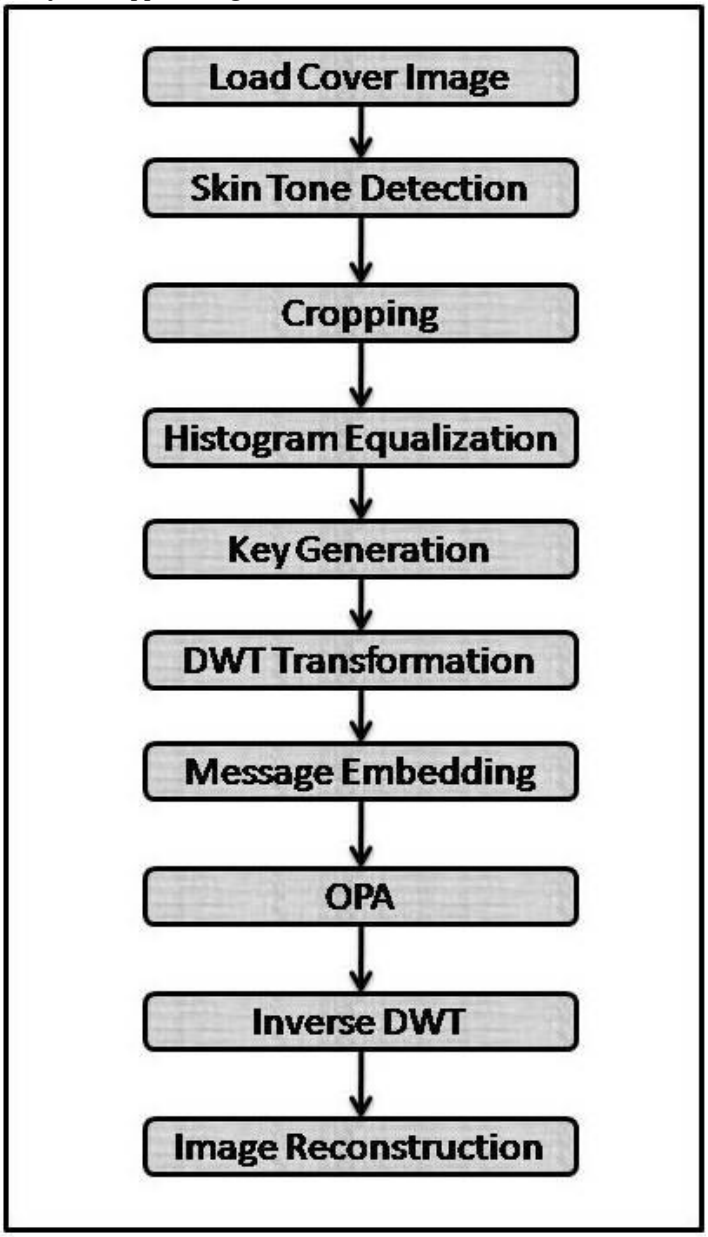

Fig.-5 Embedding Procedure

B. *Extraction Procedure*

In the process of embedding following steps are involved (which is also depicted in Fig.-6):

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

1. Stego-image is loaded.
2. Cropping of stego-image is performed.
3. DWT is performed on cropped image.
4. Secret message is extracted from transformed cropped image.
5. Performance Parameters MSE, PSNR and Embedding capacity is calculated as a result of extraction process.

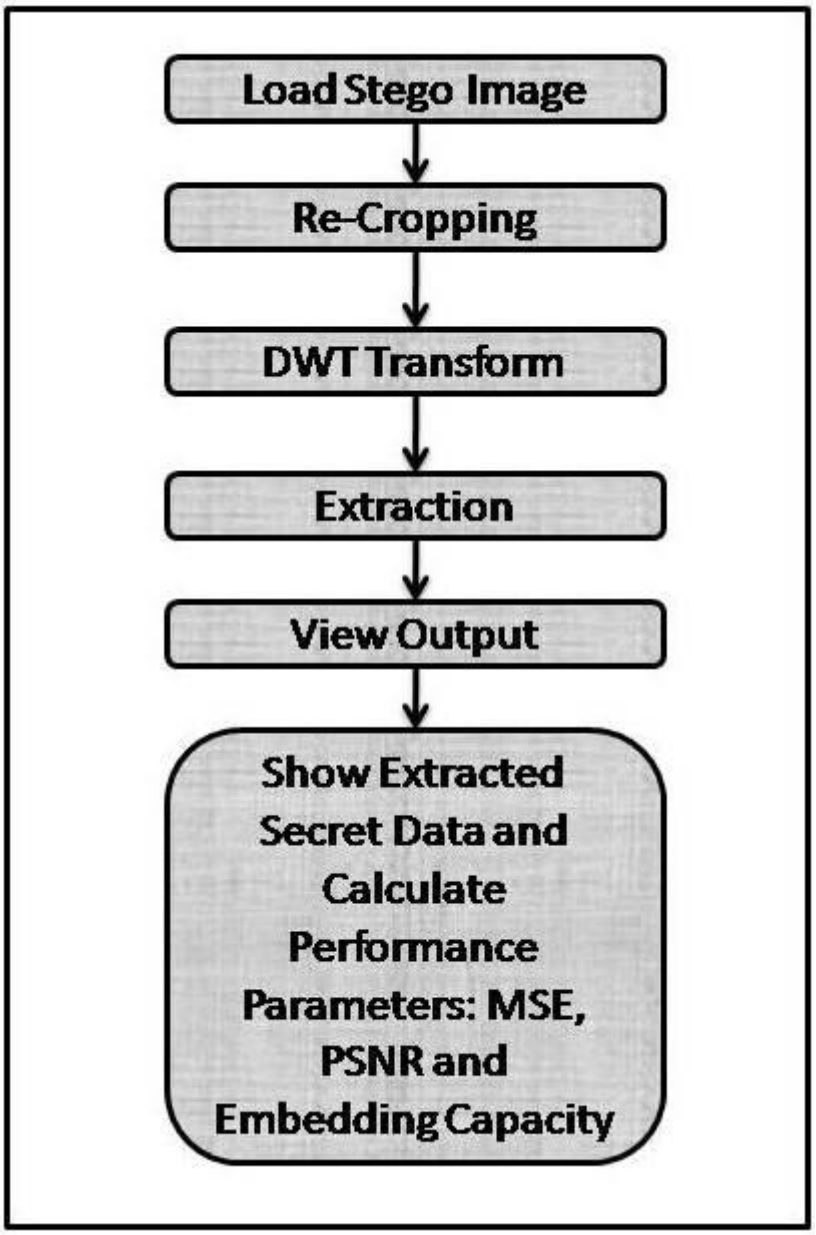

Fig.-6 Extraction Procedure

IV. Result And Discussion

In this section we demonstrate results and performance of our proposed JPEG steganography scheme. This steganography scheme has been implemented in MATLAB R2010a (V 7.10.0) and run on a PC Pentium 4 with 1GB of RAM under Windows 7 operating system.
GUI for JPEG Steganography implementation has been shown in Fig.-7.We take a 24-bit color image as cover image of size 256×256, as shown in Fig.-8. And choose a secret data text file of size of 0.5KB say msg.txt (shown in Fig.-9) but we can choose a text file of size up to 20KB.We calculate performance parameter MSE, PSNR and Embedding capacity, which are discussed below:

- MSE: MSE denotes the Mean Square Error which is given as:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

MSE= $\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$ (3)

And C_{max} holds the maximum value in the image, for example:

$C_{max} \leq \begin{cases} 1 & \text{in double precision intensity image} \\ 255 & \text{in 8 bit unsigned integer intensity image} \end{cases}$

x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated stego-image and C_{xy} is the cover image [4]. MSE should be low for less distorted Stego-image.

- PSNR: As a performance measurement for image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego images. It is defined as [4] :

PSNR= $10\log_{10}\left(\frac{C^2_{max}}{MSE}\right)$ (4)

PSNR is calculated in dB.The greater the PSNR value the higher the Image Quality means a very little difference between cover image and stego image.

- Embedding Cpapcity: The embedding capacity is the maximum number of bits that can be embedded in a given cover image.It is considered as the size of data embedded within a cover image (KB) [2].

Fig.-7 GUI of Proposed JPEG Steganography

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

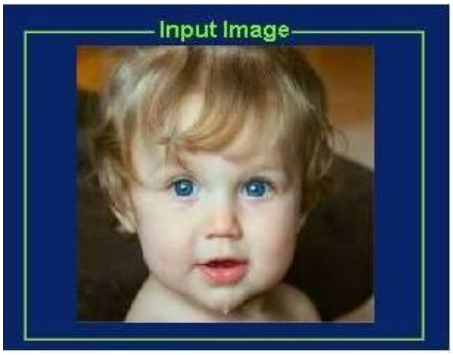

Fig.-8 Cover Image

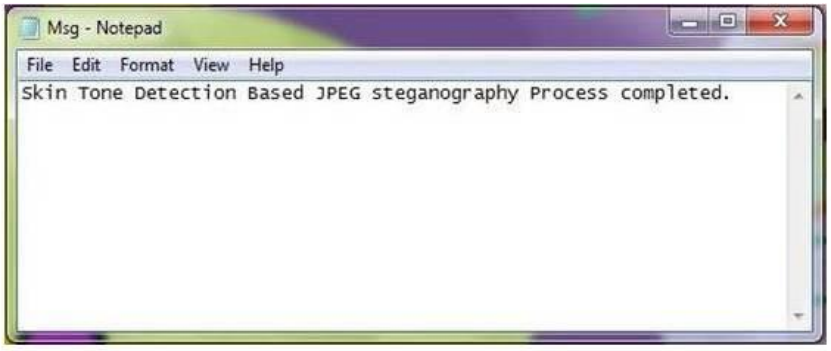

Fig.-9 Secret Data Text File

After performing skin tone detection, cropping and embedding secret data we get skin region of cover image (shown in Fig.-10), cropped region of skin portion (shown in Fig.-11) and embedded image (shown in Fig.-12) respectively. And finally after embedding procedure we get stego-image (shown in Fig.-13) and then through extraction procedure we get our secret data in output.txt file (shown in Fig.-14).

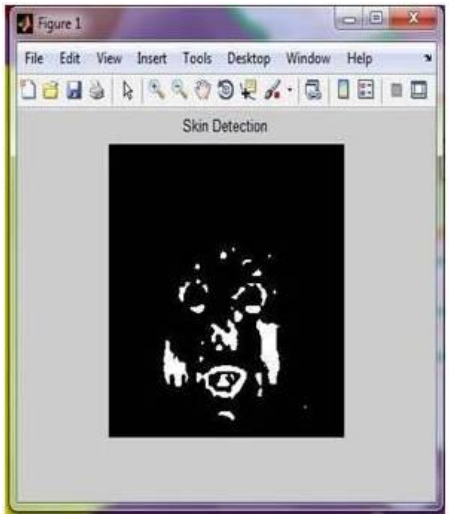

Fig.-10 Skin Region of Cover-Image

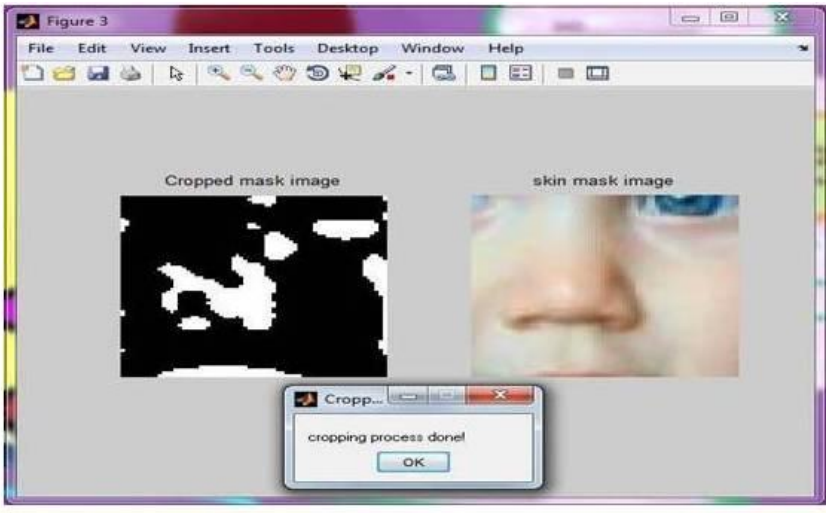

Fig.-11 Cropped Region of Skin Portion

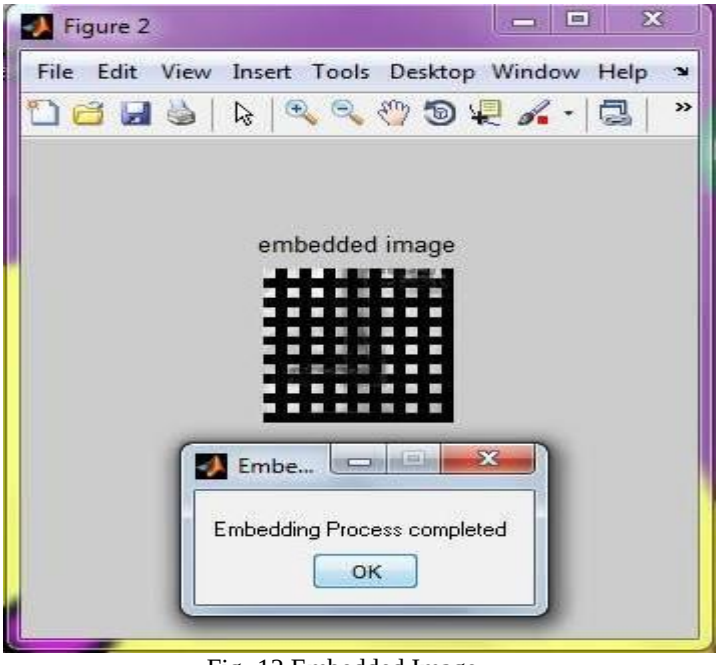

Fig.-12 Embedded Image

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

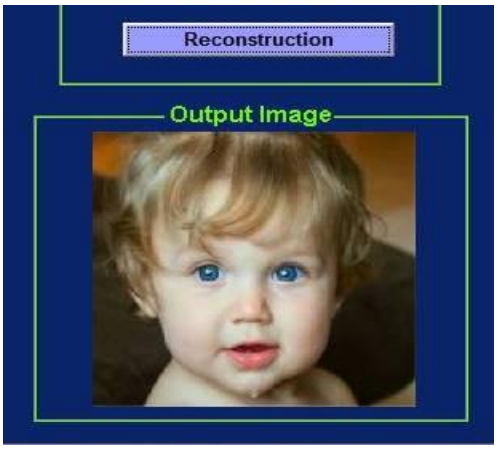

Fig.-13 Stego-image

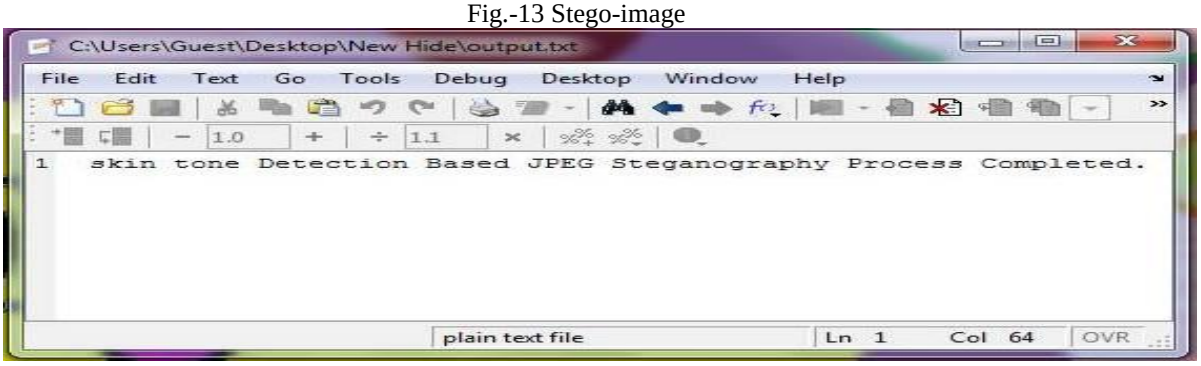

Fig.-14 Extracted Secret Data in output.txt

Performance of our proposed JPEG steganography is shown Table-1 in terms of MSE, PSNR and Embedding Capacity for 6 sample cover images.

TABLE -1

Cover Image (256×256)	**Performance Evaluation**		
	MSE	**PSNR (dB)**	**Embedding Capacity (KB)**
Image 1	0.3352	52.87	19.69
Image 2	0.3862	52.26	19.69
Image 3	0.4130	51.96	19.69
Image 4	0.4881	51.24	19.69
Image 5	0.5072	51.08	19.69
Image 6	0.7072	49.63	19.69
Average PSNR		51.50	

Our Proposed JPEG Steganography Scheme Provide better embedding capacity as compared to Sunyy Sachdeva and Amit Kumar's method [2] and better average PSNR value.

V. CONCLUSIONS

In this paper JPEG image steganography is presented that uses skin tone detection for finding skin portion of image and within this skin portion using DWT domain secret data embedding has been done. Hiding of secret data in only the cropped skin portion enhances the security. We use LSB method for embedding and which is simple and straightforward. But, in LSB method when the capacity is highly increased, the image quality decreases very much. And, the secret data might be easily stolen. For overcoming this deficiency of LSB method we use OPA (optimal pixel adjustment). And according to result and discussion proposed scheme provides well image quality.

.

REFERENCES

[1] Anjali A. Shejul and Umesh L. Kulkarni, *"A Secure Skin Tone Based Steganography Using Wavelet Transform"*, International Journal of Computer Theory and Engineering, vol. 3, No. 1, Feb. 2011.

[2] Sunny Sachdeva and Amit Kumar, "*Colour Image Steganography Based on Modified Quantization Table"*, Second International Conference on Advanced Computing & Communication Technologies, 2012.

[3] J. Kodovsky and J. Fridrich, "*Quantitative structural steganalysis of jsteg*", Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, pp. 681–693, 2010.

[4] Abbas Cheddad, John Condell, Kevin Curran and Paul Mc Kevitt, "*Biometric Inspired Digital Image Steganogrphy"*, 15th Annual IEEE International Conference and Workshop on Engineering of Computer Based Systems, 2008.

[5] A. Latham. (1999, August) Jp hide&seek. [Online]. Available: http://linux01.gwdg.de/~alatham/stego.html.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

[6] Anil Kumar Katharotiya, Swati Patel and Mahesh Goyani, *"Comparative Analysis between DCT & DWT Techniques of Image Compression",* Journal of Information Engineering and Applications, vol. 1, No. 2, 2011.
[7] A. Westfeld, "*F5-a steganographic algorithm*," in IHW '01: Proceedings of the 4th International Workshop on Information Hiding. Springer-Verlag, 2001, pp. 289–302.
[8] Abbas Cheddad, John Condell, Kevin Curran and Paul Mc Kevitt , *"A skin tone detection algorithm for an adaptive approach to steganography",* ELSEVIER, Signal Processing, 2009.
[9] J. Fridrich, M. Goljan, and D. Hogea, "*New methodology for breaking steganographic techniques for JPEGs*," Submitted to SPIE: Electronic Imaging, 2003.
[10] S.Swarnalatha and T.Harikala, "*Implementation of Skin Tone Based Steganography in Biometric Applications*", International Journal of Engineering Research and Applications, Vol. 1, Issue 4, pp.1696-1701.
[11] S. Hetzl and P. Mutzel, "A graph-theoretic approach to steganography," Lecture Notes in Computer Science, vol. 3677, p. 119, 2005.
[12] Po-Yueh Chen and Hung-Ju Lin,"*A DWT Based Approach for Image Steganography"*, International Journal of Applied Science and Engineering, 2006.
[13] R.Amirtharajan, R. Akila and P.Deepikachowdavarapu*,"A Comparative Analysis of Image Steganography*", International Journal of Computer Applications, vol. 2, no.3, May 2010.