Cryptography, Steganography and so forth. Our proposed framework already encompasses three-tier robustness with the existence of two keys and IDWT on the encoder end. We know that there is no bound to the thoughts of a negative mind. Yet considering a scenario in which a Hacker manages to obtain the stego image along with the two keys. In such a case too he shall be unsuccessful in decoding the message. As mentioned earlier, our proposed decoder is not the exact inverse of the encoder. Thus if the Hacker tries to reverse the encoder upon the stego image and if he tries to fiddle with the bits, all he obtains is a completely distorted image. This challenge is a proof to the robustness in steganography that we're proposing.

6.

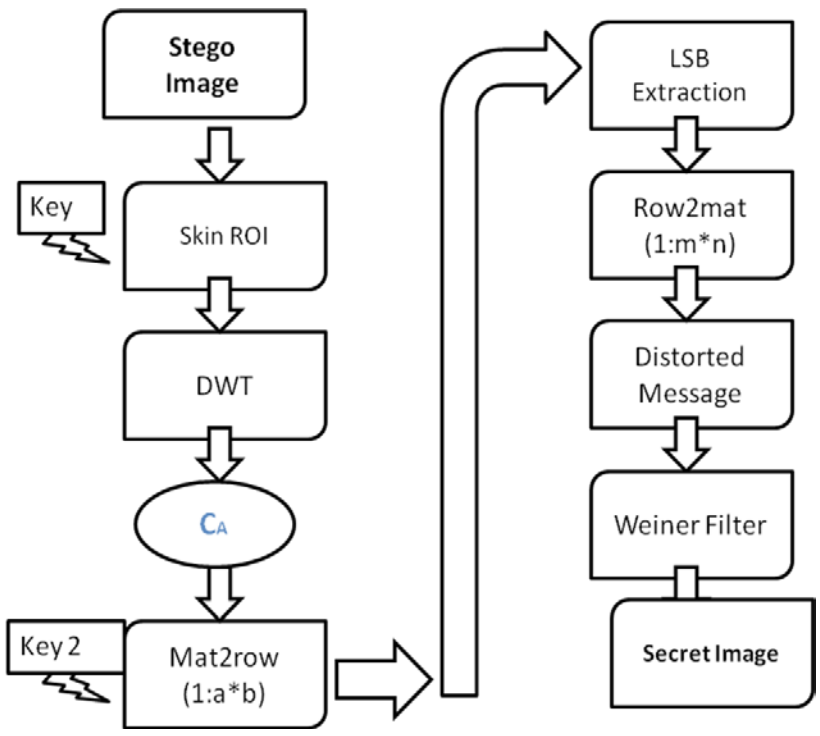

Figure 10:- Proposed Decoder

IX. ANALYSIS

To establish an objective criterion for digital image quality, a parameter named PSNR (Peak Signal to Noise Ratio) is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}$$

MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image. The mathematical definition for MSE is:

$$MSE = \left(\frac{1}{M \times N}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2$$

Where **a***ij* means the pixel value at position (*i*, *j*) in the cover image and **b***ij* means the pixel value at the same position in the corresponding stego-image. The calculated PSNR usually adopts dB value for quality judgment. The larger PSNR is, the higher the image quality is (which means there is only little difference between the cover-image and the stego-image). On the contrary, a small dB value of PSNR means there is great distortion between the cover-image and the stego-image. For color images, the reconstruction of all three color spaces must be considered in the PSNR calculation. The MSE is calculated for the reconstruction of each color space. The average of these three MSEs is used to generate the PSNR of the reconstructed RGB image (as compared to the original 24-bit RGB image). The color PSNR equations are as follows**:-**

$$PSNR = 10\log\frac{255^2}{MSE_{RGB}}$$

$$MSE_{RGB} = \frac{MSE_{red} + MSE_{blue} + MSE_{green}}{3}$$

MSE red (or green or blue) is similar to the main MSE equation for each color space.

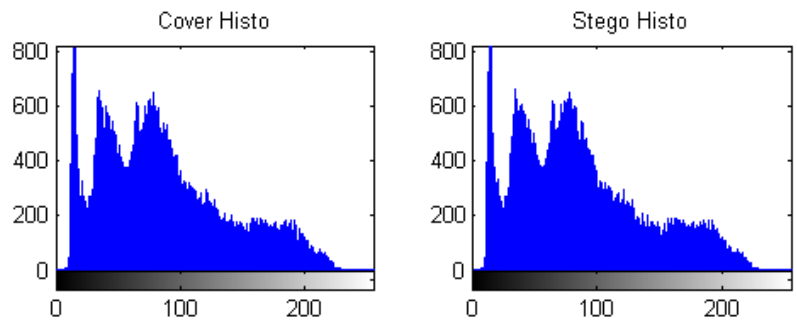

Fig 11. Comparison of Cover and Stego Image

X. CONCLUSION

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. Proposed framework is based on steganography that uses Biometric feature i.e. skin tone region. Skin tone detection plays a very important role in Biometrics and can be considered as secure location for data hiding. Secret data embedding is performed in DWT domain than the DCT as DWT outperforms than DCT. Using Biometrics resulting stego image is more tolerant to attacks and more robust than existing methods.

REFERENCES

1. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Biometric Inspired Digital Image Steganography", *15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems*, 978-0-7695-3141-0/08 $25.00 © 2008 IEEE DOI 10.1109/ECBS.2008.11.159)
2. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography", *Faculty of Computing and Engineering, University of Ulster*, BT48 7JL, Londonderry, Northern Ireland, United Kingdom.
3. Po- Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *Department of Computer Science and Information Engineering, National Changhua University of Education*, No. 2 Shi-Da Road, Changhua City 500, Taiwan, R.O.C.
4. Vladimir Vezhnevets and Vassili Sazonov, "A Survey on Pixel-Based Skin Color Detection Techniques", *Alla Andreeva Graphics and Media Laboratory, Faculty of Computational Mathematics and Cybernetics Moscow State University*, Moscow, Russia.
5. Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information," *IEEE conference on Information Technology*, pp. 113-116, 1998.
6. Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," IEEE *conference on Military communication*, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.
7. Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," International Workshop on Intelligent data Acquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001.
8. LIU Tong, QIU Zheng-ding "A DWT-based color Images steganography Scheme" IEEE International Conference on Signal Processing, vol. 2, pp.1568-1571, 2002.
9. Jessica Fridrich, Miroslav Goijan and David Soukal, "Higher-order statistical steganalysis of palette images" *Proceeding of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of*
   a. *Multimedia ContentsV*, vol. 5020, pp. 178-190, 2003.
10. Jessica Fridrich and David Soukal, "Matrix Embedding for Large Payloads" *SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents* , vol. 6072, pp. 727-738. 2006.
11. Yuan-Yu Tsai, Chung-Ming Wang "A novel data hiding scheme for color images using a BSP tree" *Journal of systems and software*, vol.80, pp. 429-437, 2007.
12. Jun Zhang, Ingemar J. Cox and Gwenael Doerr.G "Steganalysis for LSB Matching in Images With High-frequency Noise" *IEEE Workshop on Multimedia Signal Processing*, issue 1-3, pp.385- 388, 2007.
13. M. Mahdavi, Sh. Samavi, N. Zaker and M. Modarres-Hashemi, "Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram," *Journal of Electrical and Electronic Engineering*, vol. 4, no. 3, pp. 59-70, 2008.