ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse101842019.pdf
https://doi.org/10.30534/ijatcse/2019/101842019

A Randomized Hiding Technique in Skin tone based Images

Smitha Vas P[1,2], Abdul Rahiman M [3, 4]
[1]Research Scholar, Karpagam Academy of Higher Education, Coimbatore, India, smithavas@rediffmail.com
[2]Department of Computer Science & Engineering, LBSITW, Thiruvananthapuram, India
[3] Research Guide, Karpagam Academy of Higher Education, Coimbatore, India, rehmanpaika@gmail.com
[4] Managing Director, C-APT, Thiruvananthapuram, Kerala, India

ABSTRACT

Skin tone based steganography refers to a steganography technique where the secret information is inserted in the skin tone area of images. Skin tone area of an image provides an excellent place for data hiding. In traditional image steganography, a user can insert covert information anywhere in a picture, while in biometric-based steganography skin tone area is chosen as the biometric highlight. To apply skin tone based steganography we select the skin tone zone in digital images that it gives an incredible zone to concealing data. In this work, a DWT based image steganography technique is suggested that conceals information in the discrete wavelet coefficients of blocks that are selected arbitrarily. In the proposed approach, two ideas are incorporated. Initially, the skin region is partitioned into blocks and secret information is embedded on arbitrarily picked blocks to oppose steganalysis. Second, the inserting limit is expanded by concealing several secret images and text in various blocks at the same time. The proposed approach is tested by placing secret images and text within twenty different skin tone cover images. The experimental findings indicate that in terms of imperceptibility and quality measures, the system developed offers remarkable improvements to prevailing works.

Key words: Blocking, DWT steganography, Randomized hiding, Skin tone region, Skin tone detection.

1. INTRODUCTION

Steganography, also known as covered writing, is the practice of covert communication so that it is not possible to detect the presence of a message [1]. The steganography technique aims to hide a secret message or file in a carrier file such that it can be later retrieved by the intended recipient and no one else can see the secret communication between the two parties [2]. With the increase in usage of Internet and digital media, new techniques have been developed to communicate secretly between parties. In recent years, there exists a threat that terrorist groups can communicate using these techniques to hide data.

Section 2 covers the related works done in DWT based steganography. Section 3 describes the proposed randomized steganography model. Section 4 presents the experiment results and their analysis. Finally, conclusion is given in Section 5.

2. RELATED WORKS

Steganography is an area where active research is carried out for the past few decades. Various steganography methods have been developed to hide data in a cover medium and transmit it securely. These methods can be realized either in spatial domain or in transform domain. Least Significant Bit (LSB), in which information is covertly placed in LSB of the image pixels, is the most well-known steganography technique in the spatial domain and many works are published in this field. The drawback of this method is that it is easily detectable and no robust to statistical attacks. In transform domain, the data hiding methods are based on Discrete Cosine Transform, Discrete Wavelet Transforms etc.

Abbas Cheddad et.al [4] [5] developed a novel color space method for skin tone detection in which clusters of human skin were well classified with carefully selected borders. The encrypted data was embedded in the cover image by an object oriented embedding procedure. In [7] [8], Anjali et. al proposed a method using wavelet transform in which data to be hidden is embedded in skin region of images. The skin region was detected using HSV color space and data was embedded in two ways, with cropping and without cropping of skin part. It was concluded that both methods provide security. In [9] [10] [11], the authors implemented a method in which the skin detection was performed on the input image using HSV color space. Next, from the cover image, the skin region is cropped and is transformed into frequency domain using Haar-wavelet transform. In one of the high frequency bands, the secret information is incorporated. Since the embedding is done only on a selected region of the image, it provides security. Swathi Kumaravar proposed a method using DWT and LSB matching algorithm. The author has performed skin detection using HSV color space and then the cropped image is converted into frequency domain using 2D DWT. Then LSB matching method is used to insert the covert image into the cropped image. In addition, optimum

pixel adjustment method is used to adjust the pixel values to reduce LSB distortion. The quality of the obtained stego image was improved.

Amritha et.al [13] implemented a dual biometric steganography using DWT and spread spectrum. Using HSV color space, skin region is identified and cropped from the cover image. The cropped image is converted into transform domain using 2D Haar DWT. At first, the secret data is encrypted using stream cipher encryption algorithm RC4. The cipher is then inserted into one of the high frequency bands. During decoding data is extracted using session key and payload of data. In [14] Ratnakirthi et.al detected human skin area from images and secret data is hidden in the selected skin pixels. Matrix encoding mechanism was used for hiding message in the selected skin region so as to reduce the number of bits that were overwritten. The embedding algorithm used a threshold based skin detection mechanism to identify skin pixels in the cover image. The process of extraction is the inverse of the embedding process. In [15], a new method was proposed by the authors to incorporate confidential data not only in skin but also in the edge regions. They performed skin detection using HSV color space, cropped the skin area from cover image and transformed into frequency domain using DD-DWT. Then secret message was encrypted using Optimal Asymmetric Encryption Padding algorithm. Aruna et.al [16] implemented a method that detected skin tone region using HSV color space and hid the confidential information in edges along with the skin region. After cropping the skin region from cover image, they transformed the cropped image into transform domain using DWT. Histogram modification was done to adjust the contrast of the colors. The secret code was assigned in limited areas of the cropped region with optimal parity. Souvik et.al [17] performed a spatial domain technique for embedding biometric information in bit stream format. Here they detected skin area of the image using HSV color space and then the message bits were embedded into the skin area using a polynomial function. They applied a variable length embedding technique and here the image was not cropped.

3. MATERIALS AND METHODS

The proposed method consists of three stages: skin detection, embedding and extraction.

3.1 Skin Detection

As the Region of Interest is skin area of an image, the preprocessing step is skin detection. Skin detection is applied so that non-skin pixels can be sepa rated from skin pixels in an image. As the color of human skin differs between people and across from region to region, this is a difficult task. In this work, skin tone detection is done using HSV color space model. Any RGB color image can be altered to HSV (Hue, Saturation and Value) color space as given in (1)-(3).

$$H = \begin{cases} h, B \le G \\ 2\pi\pi - h, B > \end{cases}$$

$$where\ h = cos\text{-}1 \frac{\frac{1}{2(R-G)} + (R - B)}{\sqrt{(R - G)^2 + (R - G)(G - B)}} \quad (1)$$

$$S = \frac{\max (R,G,B) - \min (R,G,B)}{\max (R,G,B)} \quad (2)$$

$$V = \max (R,G,B) \quad (3)$$

In the HSV color space, threshold values for human skin tone is determined as hue_range = [0, 0.11] and sat_range = [0.2, 0.7] by many researchers [13]. Sobottaka and Pitas [3] have found out that the color of a human skin can be roughly obtained from a sector out of a hexagon by limiting it to the values: smin= 0.23, smax =0.68, hmin =0^0 and hmax=50^0.

3.2 Embedding Phase

The steps of embedding phase are as follows:

1. Divide the skin cropped area of the cover image into blocks of size 150 x 150.
2. Select one of the blocks randomly using a pseudorandom generator.
3. Apply Discrete Wavelet Transform on the selected block. One level DWT of input image results in decomposition of four subbands, i.e., LL, LH, HL and HH subbands are obtained.
4. Next, the secret information (image or text) to be hidden is taken and embedded into one of the high frequency sub bands.

4.1 If secret data is an image then hide it in the LH sub band. Go to step 5.

4.2 If secret data is a text message, then perform the following steps.

4.2.1 The text message is shortened by replacing common phrases with abbreviations.

4.2.2 Length of the text message obtained from step 4.2.1 is further reduced by removing weak words such as articles etc.

4.2.3 Embed message in the LH sub band. Figure 2 shows the steps.

5. Apply Inverse DWT on the block.
6. Merge this block having confidential data with the remaining blocks to obtain the stego image.

The information about the key i.e. selected blocks in which data is hidden, is encoded within the stego image to ensure secure communication to the intended recipient.

Figure 1 presents the block diagram used for the randomized steganography model.

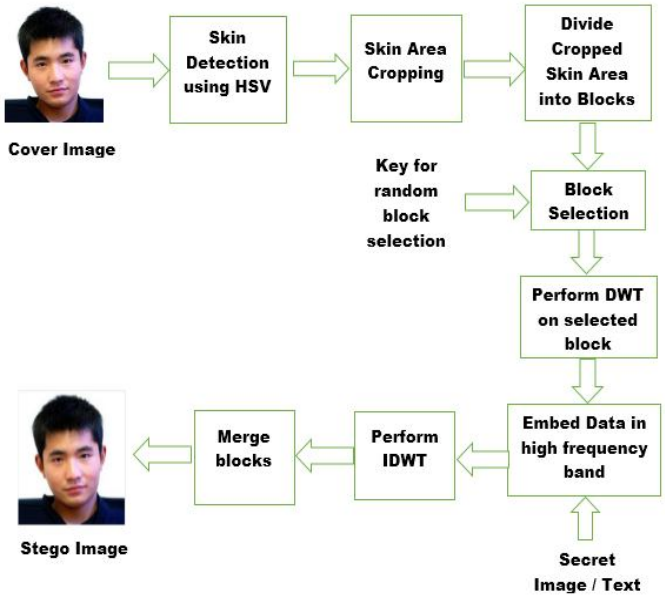

Figure 1: Proposed Embedding Method

3.3 Message Compression

In the proposed system, the concealed information to be transmitted can be a text message or an image. In case of secret text data, the length of the message is compressed as shown in Figure 2, whereby any lengthy text can be transmitted. It also reduces the variations made by embedding algorithm. Initially shorter words, abbreviations or acronyms will replace the most commonly used phrases. Nowadays people communicate through social media and the use of abbreviations and acronyms have become more popular. A lookup table, Table 1, is used for this purpose which contains the phrases and its corresponding short words.

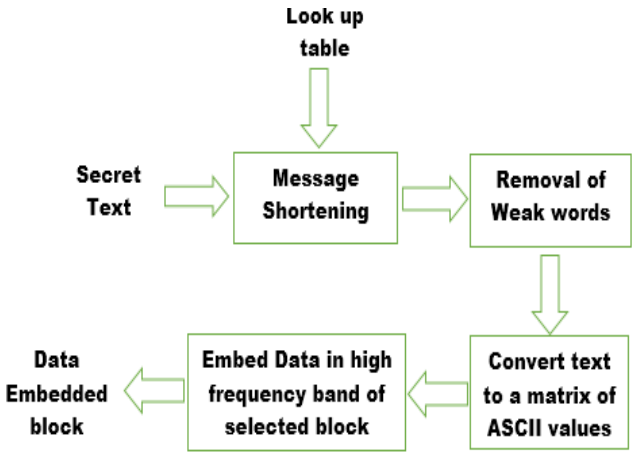

Figure 2: Stages of Secret Message Length Reduction

At the next stage, the weak words such as articles are removed from the message without changing the meaning of the message. The message obtained from the previous step is then converted into a matrix of numbers (corresponding to ASCII values), and embedded in the selected block.

Table 1: Sample of phrases and their abbreviations

Phrase	Abbreviation	Phrase	Abbreviation
Anything	Anytng	LinkedIn	LI
Age sex location	Asl	YouTube	YT
To whom it may concern	2wimc	As soon as possible	ASAP
At the weekend	Atw	Before	B4
Across	Acr	be right back	BRB
Mobile	Mob	by the way	BTW
Managing Director	MD	see you	CU
Long distance relationship	Ldr	for your information	FYI
Excellent	Xlnt	How are you?	HRU
What's up	Wassup	Please	PLS
Language	Lan	Somebody	SBY
Whatever	Wtr	Something	STH
FB	Facebook	Thanks	THX
G+	Google+	Weekend	WKND

3.4 Extraction Phase

Figure.3 depicts the overall extraction procedure. Here, the stego image undergoes skin detection using HSV. The skin detected area is cropped and divided into blocks. The key i.e selected block is extracted from the stego image. Then DWT is performed and secret data is retrieved.

In case of secret text message, first message widening is done with the help of look up table to obtain the original word.

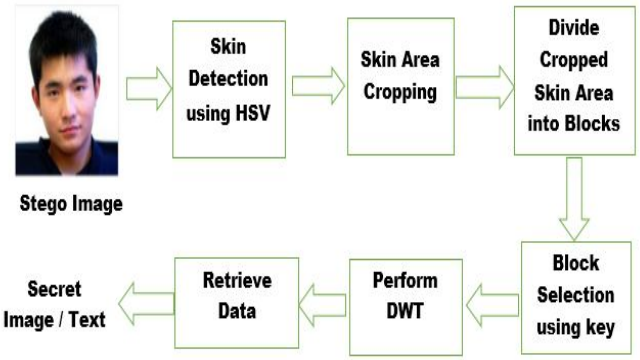

Figure 3: Proposed Decoding Method

4. RESULTS AND DISCUSSIONS

Experiments were carried out in MATLAB to evaluate the performance of the proposed approach. The test database was created using randomly collected images from the Internet. A 24-bit color image of size 512 x 512 pixels and with optimum number of skin pixels is selected. The proposed scheme was applied on twenty cover images of jpeg format. Next, to locate the human skin tone area, the cover image is transformed to HSV color space.

Figure 4 shows a sample cover image, corresponding HSV image and the skin detected area.

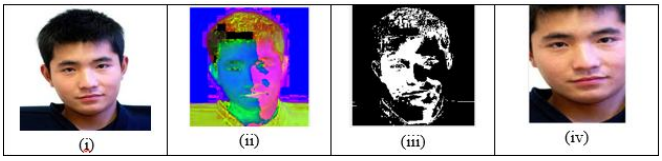

Figure 4: Skin tone detection of cover image. (i)Cover image (ii) HSV image (iii) Skin Area (iv) Skin cropped part

Also skin color can vary from individual to individual belonging to diverse cultural groups and also from different regions [13]. Figure 5 shows the results of skin tone detection technique applied on different races. Sample cover images, corresponding HSV images, skin detected areas and skin cropped areas are presented in Figure.5 (i), (ii), (iii) and (iv) respectively. The results show that the skin pixels were clearly separated out from the non-skin pixels.

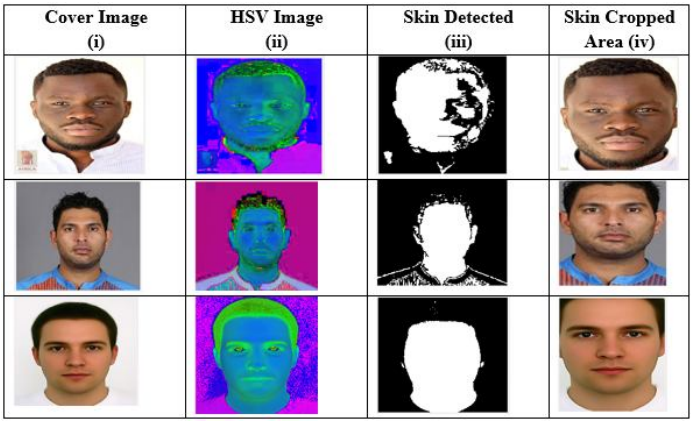

Figure 5: Samples of Images with varied skin tones

4.1 Results of Embedding Process

The skin cropped part of cover image is decomposed into blocks and one block among them is selected arbitrarily for hiding secret data.

Figure 6(i) shows the division of skin cropped area into blocks of size 150 x 150. Figure 6(ii) shows the randomly selected block and Figure 6(iii) displays the DWT form of the selected block

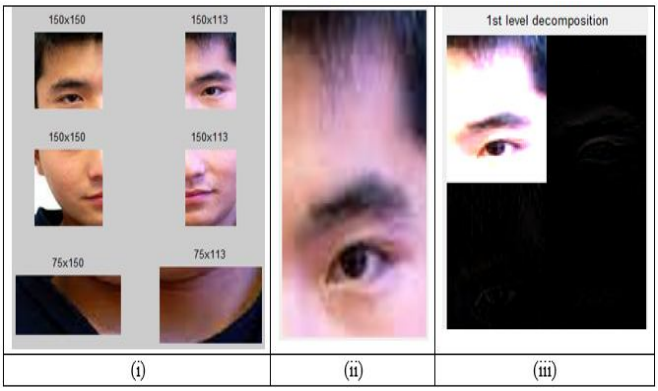

Figure 6: (i) Skin Area divided into blocks (ii) Selected block (iii) DWT of selected block

Figure 7(a) shows a sample secret image to be hidden in a cover image. Figure 7(b) -7 (c) show the results of embedding process in the cropped image. The cropped portion of image (which includes secret information) is then combined with the original image to reconstruct the stego image. Figure 7 (d) shows the stego image obtained after the encoding procedure.

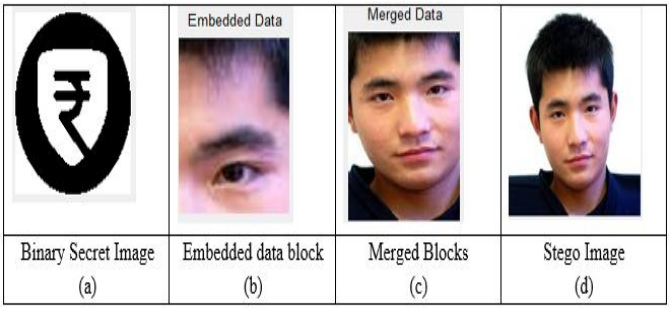

Figure 7: Stages of hiding Secret Image in selected block

The proposed method conjointly conceals a secret text message within a cover image. A sample text message is shown in Figure 8(a). The length of the text message is further reduced by referring the look up table and removing weak words from the original message. Figure 8(b)-(c) shows the stages of message compression.

Poetry is the language of the imagination and the passions.	Poetry is the lan of the imagination and the passions.
(a) Original Text Message	(b) Shortened Message
Poetry is lan of imagination and passions.	
(c) Final Text Message	

Figure 8: Stages of Message Compression

Figure 9(a) -9 (f) show the results of embedding a text message inside the cropped image. The cropped part of image (with compressed secret text embedded) is then merged with the original image to reconstruct the stego image. Figure 9(g) shows the stego image obtained after the encoding procedure.

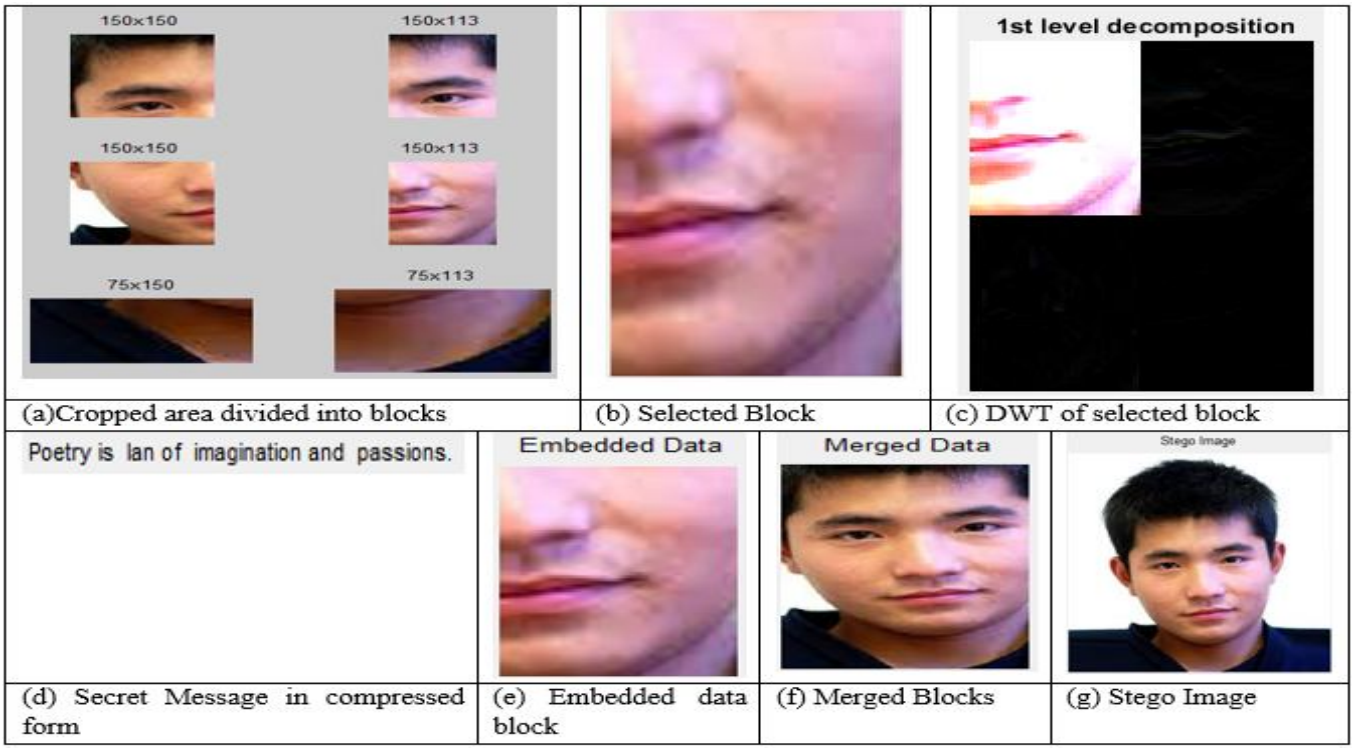

Figure 9: Stages of hiding Secret Text in selected block

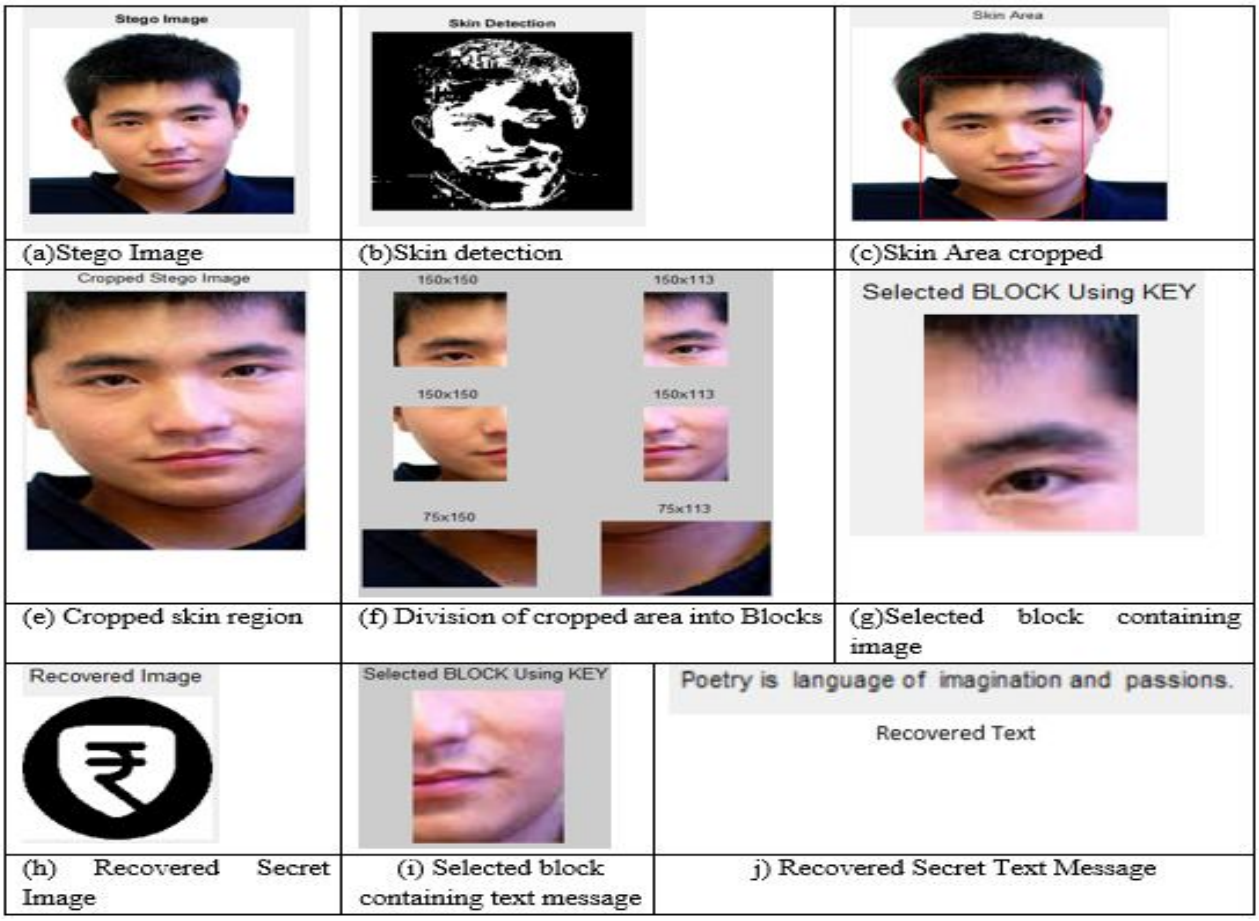

Figure 10: Decoding Stages

The decoding procedure is the inverse process of encoding method. The results of decoding stage are presented in Figure 10(a)-(j). After the stego image has been decoded, the retrieved confidential image and text are shown in Figure 10(h) and Figure 10 (j) respectively.

4.2 Performance Analysis

The proposed method has been applied on twenty cover images to analyze its performance. When data is embedded into the cover image, some distortion is created in the image. The quality of stego image as compared to original image can be evaluated using the following statistical measures.

a) Mean Square Error (MSE): MSE refers to the average squared error difference between the cover medium and stego medium.

b) The mathematical representation of the MSE is given as

$$MSE = \frac{1}{M\,X\,N}\sum_{k=1}^{M}\sum_{l=1}^{N}\left\|O(k,l) - S(k,l)\right\|^2 \quad (4)$$

where M and N refers to height and width of the cover/stego images

O (k, l) denotes value of pixel at location (k, l) of cover medium, and

S (k, l) denotes value of pixel at the same position in the corresponding stego medium.

c) Peak Signal to Noise Ratio (PSNR): The mathematical representation of the PSNR is given as

$$PSNR = 10\log_{10}\frac{max^2}{MSE} \quad (5)$$

where max refers to maximum value of pixels.

An image with higher value of PSNR means that larger is the quality of the image. PSNR values above 40 db indicate an image of high quality.

Table 2 shows the values of MSE and PSNR obtained for 'jpg' images with secret image in '.png' format and secret text message.

Table 2: MSE and PSNR analysis of images

Image	PSNR_text	PSNR_image	MSE_text	MSE_image
JPG01.jpg	61.34946	61.35319	0.04766	0.04762
JPG02.jpg	55.36058	55.40403	0.18924	0.18736
JPG03.jpg	53.40595	53.42516	0.29681	0.29550
JPG04.jpg	57.65266	57.68338	0.11164	0.11085
JPG05.jpg	54.57868	54.62212	0.22658	0.22432
JPG06.jpg	55.40132	55.43044	0.18748	0.18622
JPG07.jpg	60.83927	60.93566	0.05360	0.05242
JPG08.jpg	57.50908	57.49261	0.11539	0.11583
JPG09.jpg	56.08855	56.14325	0.16004	0.15804
JPG10.jpg	57.56849	57.61741	0.11382	0.11255
JPG11.jpg	54.39172	54.41280	0.23654	0.23540
JPG12.jpg	57.98810	58.07963	0.10334	0.10119
JPG13.jpg	54.21335	54.16578	0.24646	0.24917
JPG14.jpg	57.32727	57.46225	0.12032	0.11664
JPG15.jpg	56.06343	56.03156	0.16097	0.16215
JPG16.jpg	58.24260	58.31440	0.09746	0.09586
JPG17.jpg	56.02207	55.98147	0.16251	0.16403
JPG18.jpg	52.93559	52.94858	0.33077	0.32978
JPG19.jpg	52.62566	52.54279	0.35523	0.36208
JPG20.jpg	56.73889	56.75603	0.13778	0.13724
Average	**56.31514**	**56.34013**	**0.17268**	**0.17221**

Figure 11 and Figure 12 shows the graphical representation of the above analysis.

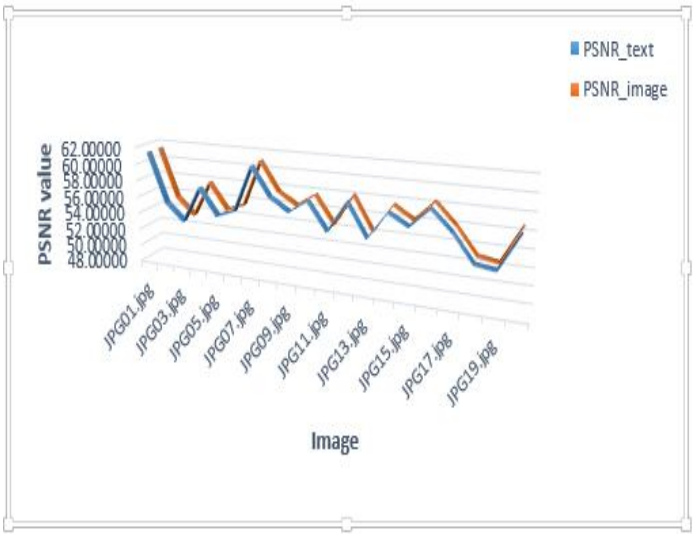

Figure 11: PSNR values of images

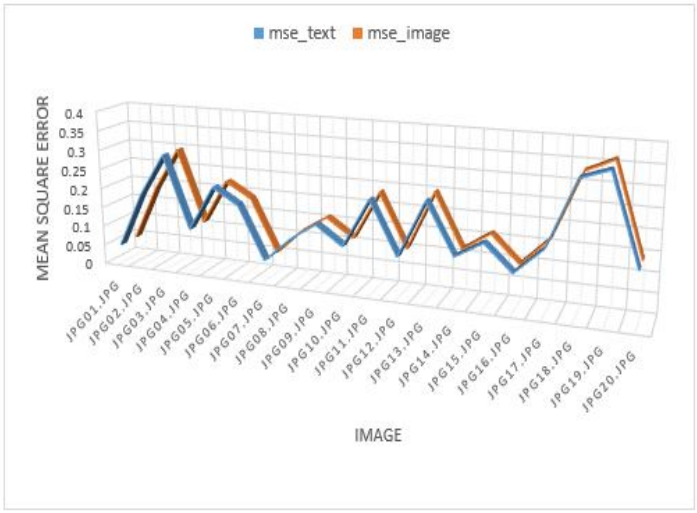

Figure 12: MSE values of images

4.3 Comparison with Previous Works

Table 3 provides a comparison between the proposed system and existing works, related to skin tone images. From the experimental findings, as shown in table 3, it can be concluded that the average value of PSNR achieved by the proposed system is superior to the existing methods.

Table 3: Comparison of Proposed method with Existing Methods

Sl. No.	Existing Work	PSNR
1	Anjali et.al [7]	50.7 (without cropping) 48.70 (with cropping)
2	Sunita *et.al* [20]	27.33
3	Meena *et.al* [12]	24.92
4	Nerkar et.al [15]	47.82
5	Aruna Mittal [16]	51.97
6	Rekha Nagar [21]	34.47
7	**Proposed Method**	**56.31(text message)** **56.34(secret image)**

5. CONCLUSION

An efficient steganography method is proposed in this paper to hide information in skin tone areas of images using DWT. Two ideas have been incorporated in this work. First it determines the skin region of an image and segment the skin area from the cover image. The cropped section is then divided into blocks and information is hidden in one of the arbitrarily selected block using DWT. Secret text as well as image can be send by this approach. Experiments show that the proposed approach gives a PSNR value of 56.3 which is superior to existing methods. Thus skin tone area provides a secure location for hiding information.

ACKNOWLEDGEMENT

The authors would like to thank Dr. N. Mohanasundaram, Professor, Dept. of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore for his valuable suggestions.

REFERENCES

1. Christian Cachin, **An Information-Theoretic Model for Steganography**, *Information and Computation*, Vol. 192, Issue 1, pp.41-56, , July 2004. ISSN 0890-540, https://doi.org/10.1016/j.ic.2004.02.003
2. 2. Johnson, N. F. and Jajodia, S.: **Exploring Steganography: Seeing the Unseen**, *IEEE Computer*, 31 (2), pp. 26-34, Feb 1998. https://doi.org/10.1109/MC.1998.4655281
3. Petitcolas, Fabien & Anderson, Ross & Kuhn, Markus. (1999). **Information Hiding - A Survey**, in *Proceedings of the IEEE. 87*, pp.1062-1078. 10.1109/5.771065.
4. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, **Biometric inspired digital image Steganography**,in *Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engineering of Computer Based Systems (ECBS'08)*, Belfast, 2008, pp.159-168. https://doi.org/10.1109/ECBS.2008.11
5. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, **A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography**, Signal Processing, Vol. 89 Issue 12, pp. 2465-2478, December 2009. https://doi.org/10.1016/j.sigpro.2009.04.022
6. Sarkar, Anindya & Solanki, K & Manjunath, B, **Further study on YASS: Steganography based on randomized embedding to resist blind steganalysis,** in *Proceedings of SPIE - The International Society for Optical Engineering*. 10.1117/12.767893
7. Anjali A. Shejul and U. L. Kulkarni, **A DWT Based Approach for Steganography Using Biometrics,** in *Proceedings of the 2010 International Conference on Data Storage and Data Engineering (DSDE '10*). IEEE Computer Society, Washington, DC, USA, pp. 39-43. https://doi.org/10.1109/DSDE.2010.10
8. Anjali A Shejul and Umesh L Kulkerni, **A Secure Skin tone based Steganography using wavelet transforms**, *International Journal of Computer Theory and Engineering*, Vol.3, No.1, pp. 1793-8201, Feb 2011.
9. N.Lavanya et al., **Robust and Secure Data Hiding in Image Using Biometric Technique,** *International Journal of Computer Science and Information Technologies*, Vol. 5 (2) , pp.1785-1787, 2014.
10. Rupa Maan and Lovneesh Bansal, **Comparison and Implementation of Biometric Inspired Digital Image Steganography**, IJCST, Vol.3 Issue 4, Dec 2012.

11. Snehal Manjare and S.R Chougule, **Steganography using concept of Skin tone Detection**, *International Journal of Scientific Research Engineering & Technology (IJSRET)*, Vol. 2 Issue4 pp. 189-193, July 2013.
12. Meena, Danvir Mandal **Object Oriented Steganography based on Biometric and Spread Spectrum**, *International Journal of Scientific and Engineering Research*, Vol. 3,Issue 6 pp.1355-1359, June 2012.
13. Amritha. G and Meethu Varkey, **Biometric Steganographic Technique Using DWT and Encryption,** *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3, Issue 3, pp. 566-572, March 2013.
14. Sobottka, K. and Pitas, I **Extraction of facial regions and features using color and shape information**, in *Proc. IEEE International Conference on Image Processing*, pp. 483-486. 1996. https://doi.org/10.1109/ICPR.1996.546982
15. Vijay B. Nerkar , Prof Abhisekh , Kumar Tripathi, Ganesh Bhadane, **A Secure Skin Tone Based Steganography Using Double Density Discrete Wavelet Transform,** *International Journal of Electrical, Electronics and Computer Engineering* 2(2), pp 83-90 Oct 2013.
16. Aruna Mittal, **Object Oriented Steganography using Skin Tone Detection and RSA Encryption Scheme**, *International Journal of Science and Research (IJSR)*, Vol. 2 Issue 2, pp.59-66, February 2013.
17. Souvik Bhattacharyya and Indradip Banerjee and Anumoy Chakraborty and Gautam Sanyal, **Biometric Steganography Using Variable Length Embedding**, *International Journal of Computer and Information Engineering*, Vol: 8, No: 4, pp. 668 – 679, 2014.
18. Tulasidasu, M. et al. **Steganography Based Secret Image Sharing Using Block Division Technique**." *2015 International Conference on Computational Intelligence and Communication Networks (CICN)* (2015), pp. 1173-1176. https://doi.org/10.1109/CICN.2015.227
19. Attaby, Abdelhamid & Mursi, Mona & el sammak, Abdelwahab, **Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3**, *Ain Shams Engineering Journal*. 10.1016/j.asej.2017.02.003.
20. Barve, Sunita & Nagaraj, Uma & Gulabani, Rohit., **Efficient and Secure Biometric Image Steganography using Discrete Wavelet Transform**, *International Journal of Computer Science & Communication Networks*, Vol 1(1), pp. 96-99, September-October 2011.
21. Rekha Nagar, **An Image Hiding Algorithm Using DWT Skin Tone Detection and SHA-512**, in International Conference on Advanced Computing (ICAC-2017), pp.5-13.
22. H. Raviya, Kaushik & Dwivedi, Vedvyas & Kothari, Ashish., **SVD Based Performance Improvement in Hiding a Message Behind an Image**, *International Journal of Advanced Trends in Computer Science and Engineering.*, Vol. 8, No.2, pp. 182-186, March - April 2019. 10.30534/ijatcse/2019/12822019.
23. Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Rushdi Abu zneit, **Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography**, *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 8, No.3, pp. 748-754, May - June 2019. https://doi.org/10.30534/ijatcse/2019/64832019