Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Hash-Based Approach on Secure Skin Tone Stegnography using Wavelet Transform

Ms.Rekha D.Kalambe, Prof.Rakesh Pandit, Prof .Sachin Patel

Information Technology

RGPV Bhopal, India

Abstract— Steganography is the skill of hiding the existence of confidential data in other transmission medium to attain secret communication like image, audio, video etc. It does not restore cryptography but quite boost the security using its abstruse features. In this paper the biometric characteristic is used to apply steganography technique in skin tone region of images [1]. For detecting skin tone in colour images a novel technique skin likelihood model is used [2]. By using this colour model important data is implanted within skin region of image which will give an outstanding secure location for data hiding. The different steps of data hiding can be applied by cropping and without cropping an image interactively. With the help of cropping an image improved security than hiding data without cropping the whole image, so cropped region works as a key at decoding region [3]. Again, we have proposed a method of Steganography based on embedding encrypted message using MD5 hash function, which provide highly secure and robust skin tone data hiding. Cryptography algorithm is used to convert the secret messages to an unreadable form before embedding; which provides a strong backbone for data security. This paper focuses on illuminating the technique to secure data or message with authenticity and non-repudiation. Here we have also provided integrity using MD5 hash algorithm. The analysis shows that the PSNR got better in the case of DWT technique [15]. Use of hash algorithm provides secure and fast approach for color image data hiding. So with this object oriented steganogaphy we track skin tone objects in image with the higher security and satisfactory PSNR .Modern steganography's goal is to keep its mere presence undetectable.

Keywords: Setganography, skin tone detection, skin likelihood color model, MD5 hashing, DCT, DWT, PSNR.

I. INTRODUCTION

A. *Steganography*

Steganography is the skills of writing secrete messages in such a way that no one, other than the sender and receiver, suspects the survival of the message, a form of security through obscurity.

As compared to cryptography, the advantage of steganography is that messages do not soak up awareness to themselves. On the other hand, the cryptography protects the contents of a message; and steganography can protect both messages and communicating parties.

B. *Digital Water marking*

A digital watermark is a type of indicator secretly implanted in a noise- tolerant signal such as audio or image data. It is classically used to recognize ownership of the copyright of such signal. "Watermarking" is the process of concealing digital information in a carrier signal [6]. Both steganography and digital watermarking use steganographic techniques to implant data secretly in noisy signals. But whereas steganography aims impossible to perceive by human senses, digital watermarking attempts to control the robustness as top priority.

C. *Skin tone detection*

In Steganography, secret message is the data that the intended is the medium in which the message is sender needs to remain secret. The host implanted and serves to hide the presence of the message. Skin detection is the process of finding skin-colored pixels and regions in an image, audio or a video. This process is typically used as a pre-processing step to find regions that potentially have human faces and limbs in images. Actually it is nothing but the color of human skin. Following figure shows the various samples of skin tones.

Fig.1 Skin tone levels

D. Cryptography

Cryptography before the current era was effectively identical with encryption, the conversion of information from a clear state to evident garbage. The creator of an encrypted message shared the decoding technique required to recover the original information only with destined recipients, thereby preventing unwanted intruder to do the same.

II. LITERATURE SURVEY

A. *RGB Color Space and Skin Detection:*

The most commonly used color space in digital images RGB is color space. It encodes colors as an additive combination of three primary colors: red(R), green (G) and blue (B). RGB Color space is often visualized as a 3D cube where R, G and B are three perpendicular axes. Simplicity is the most important advantage of the RGB space. However, it is not perceptually uniform; it means distances in the RGB space do not linearly correspond to human perception. In addition, RGB color space does not separate luminance and chrominance, Because R, G, and B components are highly correlated. The luminance of a given RGB pixel is a linear composition of the R, G, and B values. Therefore, varying the luminance of a given skin patch affects all the R, G, and B components. Otherwise stated, the location of a given skin patch in the RGB color cube will change based on the intensity of the illumination under which such patch was imaged! This results in a much stretched skin color cluster in the RGB color cube.

B. *TV Color Spaces and Skin Detection:*

There are different classes of color spaces like orthogonal color spaces, which are used in TV transmission. This includes YUV, YIQ, and YCbCr. YIQ is used in NTSC TV broadcasting although YCbCr is used in JPEG image compression and MPEG video compression. The main advantage of using these color spaces is that most video media are already encoded using these color spaces. Transforming from RGB into any one of these spaces is a straightforward linear transformation [5]. Here all these color spaces separate the illumination channel (Y) from two orthogonal chrominance channels (UV, IQ, and CbCr). Therefore, unlike RGB, the region of the skin color in the chrominance channels will not be affected by changing the intensity of the illumination. In the chrominance channels, generally the skin color is located as a compact cluster with an elliptical shape. This makes easier to building skin detectors that are invariant to illumination intensity and that use simple classifiers. The density of the skin color over the chrominance channels can be easily approximated using a multivariate Gaussian distribution. Furthermore, the skin colors of different races almost co-locate in the chrominance channels. Therefore, using such color spaces results in skin detectors, which are invariant to human race. The simplicity of the transformation and the invariant properties made such spaces widely applicable in skin detection [3].

C. *Perceptual Color Spaces and Skin Detection:*

The perceptual color spaces, such as HSI, HSV/HSB, and HSL (HLS), have also been favoured in skin detection. These color spaces separates three components: the hue (H), the saturation (S) and the brightness (I, V or L). Essentially, HSV-type color spaces are deformations of the RGB color cube and they can be mapped from the RGB space via a nonlinear transformation. One of the advantages of these color spaces in skin detection is that they allow users to intuitively specify the boundary of the skin color class in terms of the hue and saturation. However, due to the brightness of information I, V or L often dropped to reduce illumination dependency of skin color.

D. *Skin Tone detection using skin classifier*

A variety of categorization methods has been used in the literature for the task of skin categorization. A skin classifier is a one-class classifier that defines a decision boundary of the skin color class in a feature room. The feature space in the context of skin detection is simply the color space chosen. Any pixel which color falls inside the skin color class boundary is labelled as skin. Therefore, the selection of the skin classifier is straight induced by the shape of the skin class in the color space chosen by a skin detector. Compact and regularly formed the skin color class tends to greater extent classifier.

E. *Object Oriented Steganography using Skin Tone Detection and RSA Encryption Scheme*

This paper 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 which can be considered as a secure location for data hiding. Secret data is encrypted using RSA and OAEP; keep the message more secure and tolerant to attacks. The limitation for this paper, the PSNR is 51.97db only.

F. *Image Steganography using DWT and Blowfish Algorithms*

This work addressed the technique for steganography in DWT domain, which related to image science. Without producing any major changes, a new and efficient steganographic method have been proposed for embedding secret messages into images. In this paper, multilayer security is use by applying cryptography and steganography together. Here Blowfish algorithm is use for encryption. From the comparative study, it has been seen this method is better in terms of various image similarity parameters as compared to others. Embedding capacity of this method is much better than other exiting methods in transform domain. Compare with, this method is a robust method, which can avoid various image attacks noise addition, compression. However, this paper offers embedding data on complete image, which loose the security.

G. *Skin tone Stegnography using Feistel Cipher*

Feistel cipher is a symmetric structure used in the construction of block ciphers, to overcome the drawbacks of RSA, a randomization approach is combined to it namely Feistel network. Optimal Asymmetric Encryption Padding (OAEP) is a padding scheme in the form of a Feistel network, which uses a pair of random oracles G and H to process the plaintext prior to asymmetric encryption. When combined with any secure trapdoor one-way permutation f, this processing is prove in the random oracle model to result in a combined scheme, which is semantically secure under chosen plaintext attack (IND-CPA). When implemented with certain trapdoor permutations (e.g.RSA), Feistel network is also tested secure against chosen cipher text attack. Feistel network can be use to build an all-or-nothing transform.

H. *LSB (Least significant Bit) Substitution based Steganography*

In this method, spatial features of image are used. This is very simple steganographic technique, which embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In gray-level images, every pixel consists of 8 bits. In LSB substitution, the confidential data is embed at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [6]. This method is easy and straightforward but this has low ability to bear some signal processing or noises. Moreover, secret data can be easily stolen by extracting whole LSB plane.

I. *Transform Domain based Steganography*

Robustness of steganography can make better if properties of the cover image could exploited. Considering these aspects working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it [11]. Different sub-bands of frequency domain coefficients give significant information about where vital and non-vital pixels of image resides. Using transform-domain techniques, it is possible to embed a secret message in different frequency bands of the cover. Embedding in the high frequencies creates less impact on the perceivability of the media but provide less robustness to various attacks. In contrast, embedding in the lower frequencies helps to withstand many attacks but creates perceptible impact on the media. Therefore, a middle frequency band offers excellent location for data hiding. 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 in either DCT or DWT.

III. PROPOSED SYSTEM

A. *Skin tone detection*

1) Skin Likelihood Color Model

In order to segment human skin regions from non-skin regions based on color, we need a reliable skin color model that is adaptable to people of different skin colors and to different lighting conditions. In the following section, we will describe a model of skin color in the chromatic color space for segmenting skin.

The common RGB representation of color images is not suitable for characterizing skin-color. In the RGB space, the triple component (R, G, and B) represents not only color but also luminance. Luminance may vary across a person's face due to the ambient lighting and is not a reliable measure in separating skin from non-skin region. Luminance can be removed from the color representation in the chromatic color space. A normalization process shown below defines chromatic colors, also known as “pure” colors in the absence of luminance:

$r = R/(R+G+B)$

$g=G/(R+G+B)$

$b = B/(R+G+B)$

Chromatic colors effectively used to segment color images in many applications [4]. It is also well suitable in this case to segment the skin regions from non-skin regions. The color distribution of skin colors of different people found to be clustered in a small area of the chromatic color space. Although skin colors of different people appear to vary over a wide range, they differ much less in color than in brightness. In other words, skin colors of different people are very close, but they vary mainly in intensities [1]. With these findings, we could proceed to develop a skin-color model in the chromatic color space. A total number of 32500 skin samples from 17 color images were use to determine the color distribution of human skin in chromatic color space. Our samples are taken from persons of different qualities: Asian, Caucasian and African. As the skin samples are extracted from color images, the skin samples are filtered using a low-pass filter to reduce the effect of noise in the samples.

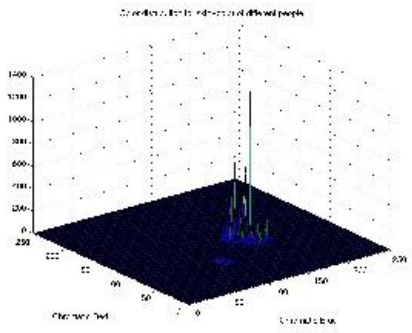

Fig. 2 Color distribution for skin-color of different people

The color histogram revealed that the distribution of skin-color of different people is clustered in the chromatic color space and a Gaussian model N (m, C) can represent a skin color distribution, where:

Mean: m = E { x } where x = (r b)T

Covariance: C = E {(x – m)(x – m)T}.

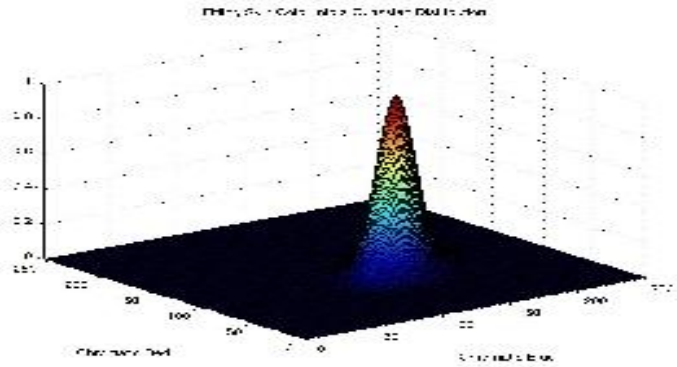

Fig .3 Fitting skin color into a Gaussian distribution

With this Gaussian fitted skin color model, we can now find the likelihood of skin for any pixel of an image. Therefore, if a pixel, having transform from RGB color space to chromatic color space, has a chromatic pair value of (r,b), the likelihood of skin for this pixel can then be computed as follows:

Likelihood=p(r, b) =exp [-0.5(x-m) rC-1(x-m)] Where: x=(r, b) r.

Hence, this skin color model can transform a color image into a gray scale image such that the gray value at each pixel shows the likelihood of the pixel belonging to the skin. With appropriate thresholding, the gray scale images can then be further transformed to a binary image showing skin regions and non-skin regions. A sample color image and its skin-likelihood image are shown in Figure.

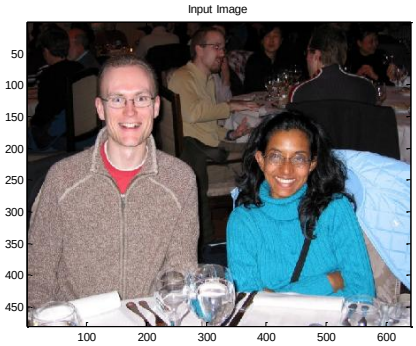

Fig. 4 Input Image

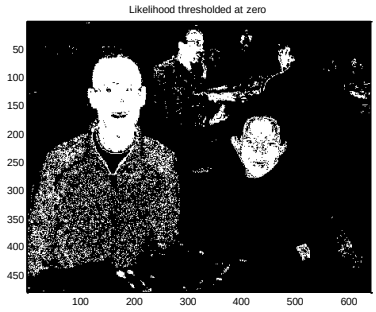

Fig 5 skin Likelihood Image

2) Skin Segmentation

Segmentation is a process, which partitions an image into regions. There are different segmentation methods; segmentation based on color is which is considered. Precise segmentation of the input image is the most important step that contributes to the efficient detection and localization of multiple faces in skin tone color images. Skin regions are brighter than the other parts of the images, the skin regions can be segmented from the rest of the image through a thresholding process. To process of dissimilar images of different people with dissimilar skin, a fixed threshold value is not possible to be finding out. Since people with different skins have dissimilar likelihood, an adaptive thresholding process is required to achieve the optimal threshold value for each case. The adaptive thresholding is based on the observation that stepping the threshold value down may intuitively increase the segmented region. However, the increase in segmented region will gradually decrease (as percentage of skin regions detected approaches 100%), but will increase sharply when the threshold value is substantially too small that other non-skin regions get included. The threshold value

at which the minimum increase in region size is observed while stepping down the threshold value will be the optimal threshold. In our program, the threshold value get decremented from 0.65 to 0.05 in steps of 0.1. The minimum increase occurs when the threshold value is changed from 0.45 to 0.35, then the optimal threshold will be taken as 0.4. Using this adaptive thresholding technique, many images give good results; the skins colored regions are effectively segmented from the non-skin colored regions. The skin-segmented image of a color image is shown in figure.

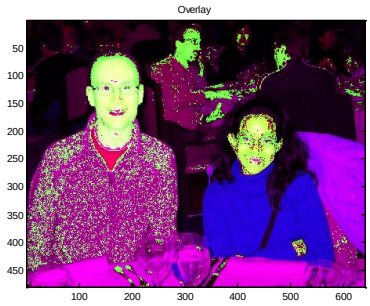

Fig 6 skin Likelihood Image

B. *MD5 algorithm:*

Information security has become very important for many purposes, sharing information between parties, mail, private information [10], business deal, and protection [14] from unauthorized user. There are many algorithms for image steganography. Some steganography techniques use perfect hash function.

This algorithm very workable for authentication .It makes assure to the intended receiver that whether the received information is correct or distorted by the unauthorized user. It calculates a message of arbitrary length and generates as result of a 128-bit "fingerprint" or "message digest". It is constructed as computationally with much effort to generate two messages with the same signature of message digest, or to generate other message having a predetermined target message digest. The MD5 algorithm is mostly for digital signature, there a very large file must be "compressed" with very secure process before encryption with a private (secret) key under a public-key like RSA [4]. Also the MD5 algorithm is a block-chained hash algorithm. The first block will be hashed with previous module, gives result in a hash. The hash is combining with the module, and that generated result goes the module for the next block. As the last block will be computed, it's "next-module' value will become the hash for the all stream. Therefore, the module for block will depends on the hash and the seed of its coming block. Therefore a result blocks can never be hashed in parallel manner.

1) Operation

MD5 Algorithm Description:

In this paper, we have a bit message as a input message, which compute message digest of message as hexadecimal digest. Here message is an arbitrary non-negative integer; which may be 0 and need not be multiple of eight, and it may be arbitrarily large.

The following five steps are perform to compute message digest of input message.

Step 1. Append Padding Bits

The padding is always made of one bit set to 1 and the rest all zeros, in quantity sufficient to bring the message length modulo 512 minus 64 (the reason for 64 is keep room for the message length).The message is “padded” (extended) so that its length (in bits) is corresponding to 448, modulo 512.that is the message is extended so that it is just 64 bits being a multiple of 512 bits long. Padding is always performed, even if the length of message is already corresponding to 448, modulo 512.

Padding is performed as follows: a single “1” bit is appended to the message, and then “0” bits are appended so that the length in bits of the padded message becomes corresponding to 448, modulo 512.In all, at least one bit and at most 512 bits are appended.

Step 2.Append Length

A 64-bit representation of message (the length of the message before the padding bits were added) is appended to the result of the previous step. In the unlikely event that message is greater than 2^64 ,then only the low order 64- bits of message are used.(the bits are appended as two 32-bit words and appended low-order word first in accordance with the previous conventions).

At this point, the resulting message (after padding with bits and with message) has a length that is an exact multiple of 16(32-bit) words.

Step 3.Initialize MD Buffer

A four-word buffer (A, B, C, D) is used to compute the message digest. Here each of A, B, C, D is a 32-bit registers. These registers are initialized to the following values in hexadecimal, low-order bytes first:

Word A: 01 23 45 67
Word B: 89 ab cd ef
Word C: Fe dc ba 98
Word D: 76 54 32 10

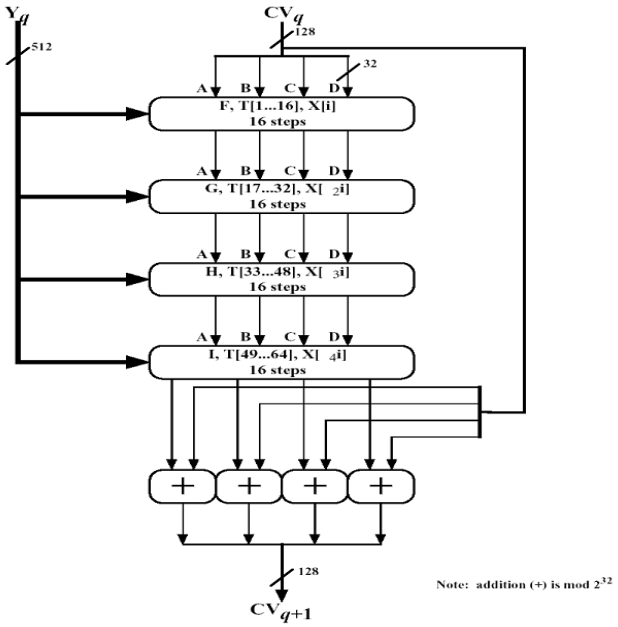

Fig 7 MD5 processing of single-512 bit block

Step 4. Process Message in 16- word Blocks
We first define four auxiliary functions (F, G, H, I) that each tales as input three, 32-bit words and output 32-bit word. As expressed in following diagram.

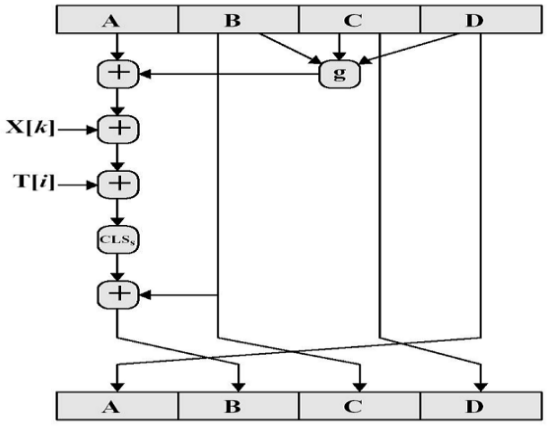

Fig 8 Elementary MD5 operation (single step)

F(X, Y, Z) = XY v not (X) Z
G(X, Y, Z) = XZ v Y not (Z)
H(X, Y, Z) = X xor Y xor Z
I(X, Y, Z) = Y xor (X v not (Z))

In each bit position, F acts as a conditional: if X then Y else Z. The function F could have been define using + instead of v since XY and not (X) z will never have 1's in the same bit position.
The G, H, and I are similar to the function F ,which act in "bitwise parallel" to produce the output from the bits of X,Y and Z, in such manner that if the corresponding bits of X,Y and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), I(X,Y,Z), will be independent and unbiased is the bit-wise "xor" or "parity" function of its inputs.
This step uses a 64-element table T [1…..64] constructed from the sine function.

Step 5.Output
The message digest-produced as output is A, B, C, D. i.e., we begin with the low-order byte A, and end with the high-order byte of D.

C. *Securing data using DWT technique*
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 leading in annoying blocking artefacts. This drawback of DCT is eliminated using DWT.DWT applies on entire image. DWT extends better energy 40

compaction than DCT without any blocking artefact. DWT splits component into 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 due to the sensitivity Human eyes to the low frequency part (LL sub band) we can hide secret message in other three parts without making any modification in LL sub band.

As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't lose the originality of image that much.

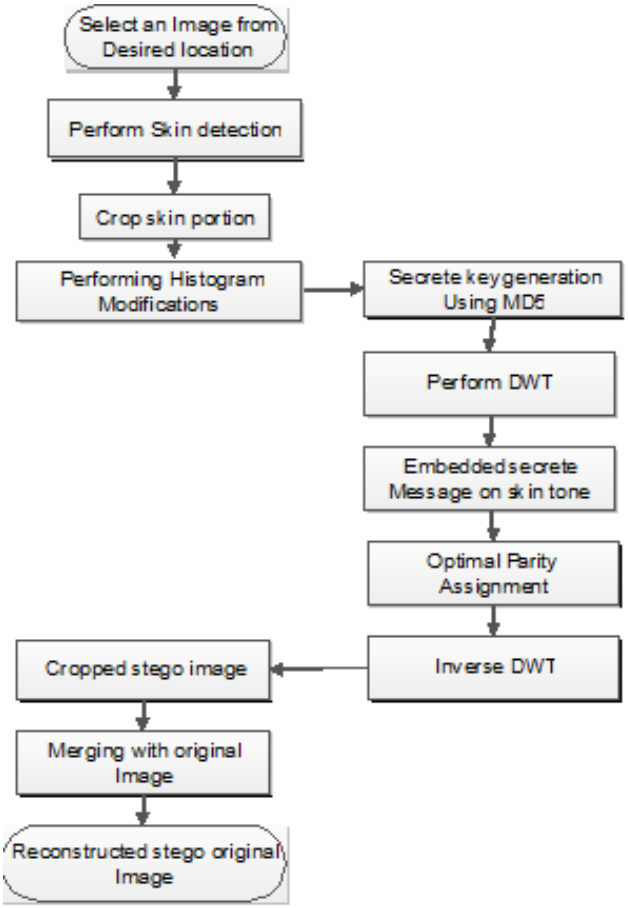

Fig 3.4 flow chart of proposed system

1. Initially load the cover object in which we will hide the secret message (text).
2. After loading the cover object, skin tone detection is performed. This enables us to know where and how much data can be hidden.
3. Cropping: From the detected skin portion, cropping is performed. This is done so that within skin pixels data is hidden at only limited pixel positions.

This feature of cropping enhances security, as any eavesdropper cannot detect secret message just by detecting the skin pixels.

4. Histogram Modification: This is performed to adjust the contrast of the colors.
54. Key Generation: This is the step where the secret message to be selected and is encrypted using MD5.
6. DWT: Discrete Wavelet Transform is applied to the cropped skin portion.
7. Secret encrypted message is now merged into the transformed skin pixels.
8. Optimal Parity Assignment is used to assign secret code values to limited areas of cropped skin portion.
9. Inverse DWT: Now the transformed image has secret code which is ready to be merged with the original cover object. The first step to merge this transformed secret message embedded image, with cover object is to inverse transform it.

D. *Masking and Filtering*

Masking and filtering techniques are usually restricted to less no. of bits or greyscale images for hiding a message. This is achieving for example by modifying the lightning of parts of the image. As masking alters the visible property of an image, it can be done in such a way that the human eye will not observe the anomalies.

As masking uses visible aspects of the image; which become more robust than LSB modification with respect to cropping compression, and different kinds of image processing. In masking the information is not hidden at the "noise" level, instead it is inside the visible part of the image.

IV. CONCLUSION

Digital Stegnography is a fascinating scientific area, which falls under the umbrella of security system. The proposed system based on biometric stegnography i.e. skin tone region. In this paper skin, tone detection is done in effective way i.e. color likelihood method, which find skin tone by finding skin probability of image to hide, secrete message. Skin likelihood method has gain high detection accuracy, high detection speed and reduces the false detecting rate.

Secrete message is encrypted using Hash-based approach for secure skin tone stegnography which is very robust and effective approach. The designed technique first generate the hexadecimal message digest of input secrete key for hiding message withoutt reduction the quality of the image up to maximum extent of limit.

ACKNOWLEDGMENT

R.D.Kalambe Author thanks to Prof. Rakesh Pandit, project guide, Prof. Sachin Patel H.O.D., Department of Information Technology, Patel Group of Science & Technology, Indore, MP, India, for their precious guidance, encouragement and continuous monitoring throughout the presented work.

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 Engg.of Computer-Based Systems (ECBS'08), Belfast, 2008, pp. 159-168.
2. Anjali A. Shejul, Umesh L. Kulkarni "A Secure Skin Tone based Steganography Using Wavelet Transform"
3. Crystal Muang and Dunxu Hu "Skin Detection - a Short Tutorial" Department of Computer Science, Rutgers University, Piscataway, NJ, 08902, USA
4. Patidar, N.K Pareek, and K.K Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," Communications in Nonlinear Science and Numerical Simulation, 14(7)(2009) 3056-3075.
5. Burger, W., Burge, M.: Digital Image Processing, an Algorithmic Introduction Using Java. Springer (2008)
6. Fridrich, J., Goljan, M. and Du, R.., (2001).Reliable Detection of LSB Steganography in Grayscale and Color Images." Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.
7. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Securing Information Content using New Encryption Method and Steganography"
8. Petit colas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petit colas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.
9. Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998.
10. B. Pfitzmann, .Information Hiding Terminology,. Proc. First International Workshop Information Hiding, Lecture Notes in Computer Science No.1,174, Springer-Verlag, Berlin, 1996, pp. 347-356.A. Brown, S-Tools for Windows, 1994, ftp://idea.sec. dsi.unimi.it/pub/security/crypt/code/s-tools3.zip.
11. Chang, C. C., Chen, T.S and Chung, L. Z.,"A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol. [4], pp. 123-138(2002).
12. E. Koch, J. Rindfrey, and J. Zhao, .Copyright Protec-tion for Multimedia Data,. Proc. Int.l Conf. Digital Media and Electronic.
13. Publishing, Leeds, UK, 1994.Yang, Wan, Liao iaofeng. Xiao Di., and Wong Kwok-Wo. (2008). One-way hash function construction based on 2D coupled map lattices. Journal of Information Sciences.
14. 178 (2008) 1391- 1406 [11]. Aruna Mittal, "Object Oriented Steganography using Skin Tone Detection and RSA Encryption Scheme".
15. Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290

