

Skin Tone Based Secret Data Hiding in Images Using Wavelet Transform

^{a*}Vemula Harini, ^bJeevan kishor G

^a email: harini040@gmail.com

^b email: jeevankishor1989@gmail.com

Abstract

Biometric feature accustomed implement steganography is skin tone region of pictures. Here secret information is embedded inside skin region of image that may offer a wonderful secure location for information activity. For this skin tone detection is performed exploitation HSV (Hue, Saturation and Value) colour area to boot secret information embedding is performed exploitation frequency domain approach – DWT (Discrete rippling Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one in all the high frequency sub-band of DWT by tracing skin pixels therein sub-band. Four bit secret key and cropping results into associate degree increased security than activity information without cropping i.e. in whole image therefore cropped region works as a key at secret writing aspect. This study shows that by adopting an object orienting steganography mechanism, in the sense that, we have a tendency to track skin tone objects in image, we get a higher security

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

1. Introduction

In this extremely digitalized world, the web is associate degree important role for knowledge transmission and sharing. However, since it's a worldwide and advertised medium, some confidential knowledge may well be taken, copied, modified, or destroyed by associate degree inadvertent observer. Therefore, security problems become an important issue.

Encoding could be a well know procedure for secured knowledge transmission [2]. Frequently used encoding ways embrace RSA, DES (Data encoding standard). Though encoding achieves certain security effects, they create the key messages unreadable and unnatural or unmeaning. These unnatural messages typically attract some inadvertent observers' attention. This can be the rationale a replacement security approach known as "steganography" arises. As associate degree example, the quilt text [3]: "I'm feeling extremely stuffy. Emily's medication wasn't sturdy enough while not another medicinal drug." Hides the sentence "Meet American state at nine" If the reader retains the second letter of every word in sequence.

*corresponding author
E-mail: harini040@gmail.com

In steganography secret message is that the knowledge that the sender desires to stay confidential and may be text, images, audio, video, or the other knowledge which will be represented by a stream of bits. The quilt or host is that the medium during which the message is embedded and serves to hide the presence of the message. The message embedding technique is powerfully keen about the structure of the quilt, and during this paper covers and secret messages are restricted to being digital pictures. The cover-image with the key knowledge embedded is named the "Stego-Image". The Stego-Image should correspond the quilt image underneath casual review and analysis. Additionally, for higher security necessities, we can write in code the message knowledge before embedding them in the cover-image to supply additional protection [4]. For this the encoder typically employs a stego-key that ensures that only recipients WHO apprehend the corresponding secret writing key will be ready to extract the message from a stego-image. For proposed methodology cowl image is cropped interactively and that cropped region works as a key at secret writing facet yielding improved security. There are 2 things that require to be thought-about whereas designing the steganographic system: Invisibility: Human eyes cannot distinguish the distinction between original and stego image. Capacity: The a lot of knowledge a picture will carry better it's. But giant embedded knowledge might degrade image quality considerably. Rest of the paper is organized as follows. Section II presents literature survey and theoretical background. In section III projected methodology is delineated intimately with skin tone detection, DWT, embedding and extraction procedure step by step. Section IV incontestable the experimental results. Finally conclusions ar provided in section V.

2. Literature survey

A. Steganography in abstraction Domain

This is a simplest steganographic technique that embeds the bits of secret message directly into the smallest amount significant bit (LSB) plane of the duvet image. During a gray level image, each component consists of eight bits. The essential conception of LSB substitution is to implant the confidential information at the rightmost bits (bits with the littlest weighting) in order that the 2010 International Conference on information Storage and information engineering embedding procedure doesn't have an effect on the initial component worth greatly [5]. The mathematical illustration for LSB is: $x_i' = x_i - x_i \bmod 2k + m_i$ (1) In equation (1), x_i' represents the i th component worth of the stego-image and x_i represents that of the initial cover image. m_i represents the decimal worth of the i th block in the confidential information. The quantity of LSBs to be substituted is k . The extraction method is to repeat the k -rightmost bits directly. Mathematically the extracted message is represented as: $m_i = x_i \bmod 2k$ (2) Hence, a straightforward permutation of the extracted m_i offers North American country the original confidential information [6]. This technique is simple and straightforward however this has low ability in-tuned some signal processing or noises. And secret information may be simply purloined by extracting whole LSB plane.

B. Steganography in Frequency Domain

Robustness of steganography may be improved if properties of the duvet image can be exploited. For example it's usually desirable to cover message in strident regions instead of drum sander regions as degradation in smoother regions is a lot of noticeable to human HVS (Human Visual System). Taking these aspects into thought working in frequency domain becomes a lot of engaging. Here, sender transforms the duvet image into frequency domain coefficients before embedding secret messages in it [7]. Totally different sub-bands of frequency domain coefficients give vital data regarding wherever very important and non very important pixels of image resides. These ways ar a lot of complicated and slower than spatial domain methods; but they're more secure and tolerant to noises. Frequency domain transformation may be applied either in DCT or DWT.

C. Adjustive Steganography

Adaptive steganography is special case of 2 former methods. It's conjointly referred to as "Statistics aware embedding" [8] and "Masking" [4]. This technique takes applied mathematics world features of the image before making an attempt to plant secret knowledge in DCT or DWT coefficients. The statistics can dictate where to form changes.

3. Proposed method

Proposed methodology introduces a brand new methodology of embedding secret information inside skin because it isn't that a lot of sensitive to HVS (Human Visual System) [1]. This takes advantage of statistics options like skin tone, instead of embedding information anyplace in image, information are going to be embedded in selected regions. Summary of methodology is concisely introduced as follows. Initially skin tone

detection is performed on input image mistreatment HSV (Hue, saturation, value) colour house. Second cowl image is remodelled in frequency domain. This can be performed by applying Haar-DWT, the only DWT on image resulting in four subbands. Then payload (number of bits within which we are able to hide data) is calculated. Before embedding process we have to generate secret key finally secret information embedding is performed in one among the high frequency sub-band by tracing skin pixels in this band. Before activity all steps cropping on input image is performed then in barely cropped region embedding is completed, not in whole image. Cropping results into a lot of security than while not cropping. Since cropped region and secret key works as two keys at secret writing facet. Here embedding method affects solely sure Regions of Interest (ROI) instead of the complete image. Therefore utilizing objects within pictures are often a lot of advantageous. This can be additionally referred to as Object homeward steganography [1]. Next sub-sections briefly introduce skin tone detection and DWT. A. skin colour Tone Detection. A skin detector generally transforms a given element into an acceptable Colour house then uses a skin classifier to label the element whether or not it's a skin or a non-skin element. A skin classifier defines a choice boundary of the skin colour category in the Colour house. Though this can be a simple method has tested quite difficult. Therefore, important challenges in skin detection area unit to represent the colour in an exceedingly way that's invariant or a minimum of insensitive to changes in illumination.[9] and Another challenge comes from the actual fact that many objects within the world might need skin-tone colours. This causes any skin detector to own a lot of false detection within the background if the surroundings aren't controlled [10]. The simplest thanks to decide whether or not a element is skin Colour or not is to expressly outline a boundary. RGB matrix of the given Colour image are often born-again into totally different Colour areas to yield distinguishable regions of skin or close to skin tone. There exists many Colour areas. Mainely 2 kinds of colour areas area unit exploited within the literature of biometrics that area unit HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) areas It is by experimentation found and in theory tested that the distribution of human skin colour perpetually resides in an exceedingly certain vary inside those 2 colour areas [1]. Colour house used for skin detection during this work is HSV.

$$S_{\min}=0.10, S_{\max}=0.68, H_{\min}=0^0, H_{\max}=25^0$$

4. Separate ripple remodel (DWT):

This is another frequency domain during which steganography is enforced. DCT is calculated on blocks of freelance pixels, a secret writing error causes` discontinuity between blocks leading to annoying block artefact. This downside of DCT is eliminated victimization DWT. DWT applies on entire image. DWT offers higher energy compaction than DCT with none block whole. DWT splits element into varied frequency bands known as sub bands referred to as

LL – Horizontally and vertically low pass

LH – Horizontally low pass and vertically high pass

HL - Horizontally high pass and vertically low pass

HH - Horizontally and vertically high pass

Since Human eyes square measure way more sensitive to the low frequency half (LL sub band) we will hide secret message in other 3 elements while not creating any alteration in LL sub band [12]. As alternative 3 sub-bands square measure high frequency sub-band they contain insignificant information. Concealment secret information in these sub-bands doesn't degrade image quality that abundant. DWT utilized in this work is Haar-DWT, the best DWT.

5. Embedding method

Suppose C is original 24-bit Colour cowl image of M×N Size. It's denoted as: $C= 1 \leq i \leq M, 1 \leq j \leq N, x_{ij}, y_{ij}, z_{ij} \in \{0,1,\dots,255\}$

Let size of cropped image is $M_c \times N_c$ wherever $M_c \leq M$ and $N_c \leq N$ and $M_c = N_c$. i.e. Cropped region should be precise sq. as we've to use DWT anon this region. Let S is secret knowledge. Here secret knowledge thought-about is binary image of size $a \times b$. Fig. one represents flow sheet of embedding process.

1) Step 1: Once image is loaded, apply skin tone detection on cowl image. this can turn out mask image that contains skin and non skin pixels.

2) Step 2: raise user to perform cropping interactively on mask image ($M_c \times N_c$). when this original image is additionally cropped of same space. Cropped space should be in a particular square type as we've got to perform DWT later and cropped area ought to contain skin region like face, hand etc since we will hide knowledge in skin pixels of 1 of the sub-band of DWT. Here cropping is performed for security reasons. Cropped parallelogram can act as key at receiving aspect. If it knows then solely knowledge retrieval is feasible. Snooper may attempt to perform DWT on whole image; in such a case attack can fail as we have a tendency to square measure applying DWT on specific cropped region solely.

3) Step 3: Apply DWT to solely cropped space ($M_c \times N_c$) not whole image ($M \times N$). This yields four sub-bands denoted as HLL, HHL, HLH, and HHH. (All four sub-band ar of same size of $M_c/2, N_c/2$). Payload of image to carry secret knowledge is determined supported no. of skin pixels gift in one amongst high frequency sub-band during which knowledge are going to be hidden.

4) Step 4: Perform embedding of secret knowledge in one amongst sub-band that we have a tendency to obtained earlier by tracing skin pixels in that sub-band. apart from the LL, low frequency sub-band any high frequency sub-band will be hand-picked for embedding as LL sub-band contains important data. Embedding in LL sub-band affects image quality greatly. We have chosen high frequency HH sub-band. Whereas embedding, secret knowledge won't be embedded all told pixels of DWT sub band but to solely those pixels that ar skin pixels. So here skin pixels ar copied victimization skin mask detected earlier and secret knowledge is embedded. Embedding is performed in G-plane and B-plane however strictly not in R-plane as contribution of R plane in Colouring is over G or B plane. therefore if we have a tendency to ar modifying R plane constituent values, decoder facet doesn't retrieve knowledge in the slightest degree as skin detection at decoder facet offers different mask than encoder facet. Embedding is finished as per raster-scan order (as shown in Fig.2) that embeds secret knowledge constant by constant in selected sub-band [6], if constant is skin constituent.

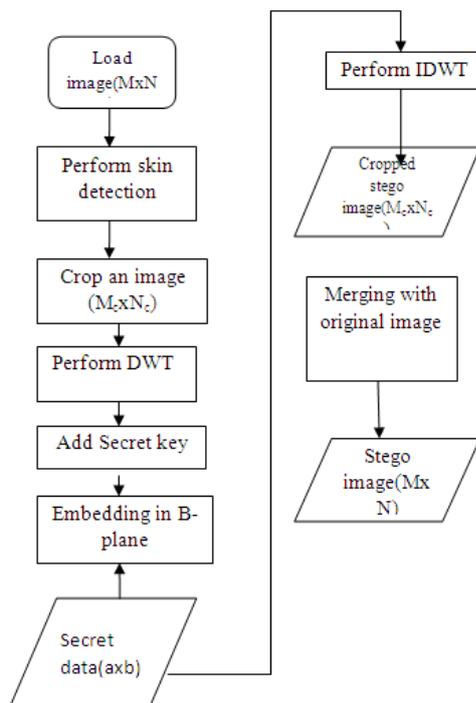


Figure1: Flow chart for embedding process

5) Step 5: Perform IDWT to mix four sub-bands. 6) Step 6: A cropped stego image of size $M_c \times N_c$ is obtained in higher than step (step 5). this could be the same as original image when visual scrutiny however at this stage it's of size $M_c \times N_c$, thus we'd like to merge the cropped stego image with original image to urge the stego image of size $M \times N$. To perform merging we have a tendency to need coefficients of 1st and last pixels of cropped space in original image so r calculated. Thus a stego image is prepared for quality analysis.

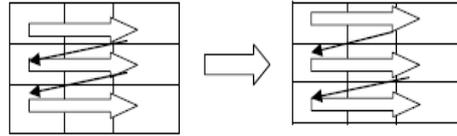


Figure2: Raster scans order

6. Extraction method

Secret knowledge extraction is explained as follows: 24 bit Colour stego image of size $M \times N$ is input to extraction process. We have a tendency to should want price of cropped space to retrieve data.

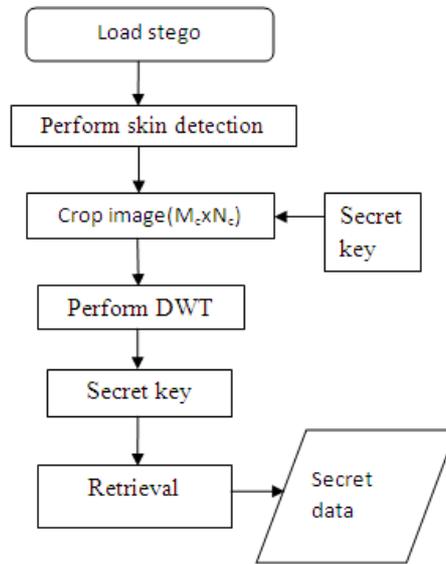


Figure 3. Flow sheet of Extraction method

Suppose four bit secret key keep in 'D' and cropped space price is keep in 'rect' variable that is same as in encoder. Thus this 'rect' and 'D' can act as two keys at decoder facet. All steps of Decoder area unit opposite to Encoder. Care should be taken to crop same size of sq. as per Encoder. By tracing skin pixels in HHH sub-band of DWT secret knowledge is retrieved. Extraction procedure is pictured using flow sheet in Fig. 3

7. Simulation

In this section we tend to demonstrate simulation results for proposed theme. This are enforced victimization MATLAB 7.5. A twenty four bit Colour image is utilized as cover-image of size 256×256 , shown in Fig. 4. Fig. five shows sample secret image cow1} within cover image.

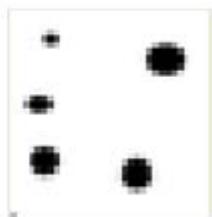


Figure4: Cover image

Figure5: Image to hide

The secret message S is binary image of size 32×32. We use Peak signal to noise quantitative relation (PSNR) to gauge quality of stego image when embedding the key message. The performance in terms of capability and PSNR (in dB) is demonstrated for the strategy within the following subsections. PSNR is outlined as per equivalent weight.3 and Eq.4.

$$PSNR = 10\log_{10} (255^2/MSE) \quad (3)$$

x_{ij} and y_{ij} represents picture element values of original cowl image and stego image severally. The calculated PSNR sometimes adopts decibel worth for quality judgement, the larger PSNR is, higher the image quality (which means that there's somewhat difference between cowl image and stego image).On the contrary smaller decibel worth means that there's a a lot of distortion. PSNR values falling below 30dB indicate fairly a coffee quality. However, top quality strives for 40dB or a lot

8. Performance of the planned methodology

After embedding secret knowledge in cropped image, resulted cropped stego image is shown in Fig. 6. (Result of step five of embedding process). As this doesn't seem like cowl image merging is performed to get final stego image that's shown in Fig. 9. (Result of step half-dozen of embedding process). For merging co-ordinates of 1st and last pixels of cropped image in original image square measure calculated. once playacting extraction method retrieved image is shown in figure eight. Above methodology uses cropping. Same planned methodology is implemented for while not cropping case. In while not cropping case secret knowledge is hidden in one among the sub-band that is obtained by playacting the DWT on whole image and not only to cropped region. PSNR is calculated for four totally different final stego pictures resulted from a thought of image and three additional sample pictures. This PSNR for various cases is shown in table one. Average PSNR of planned methodology is calculated supported the obtained PSNR. Performing biometric steganography with cropping or without cropping, each square measure having its own benefits and disadvantages. However if methodology is enforced with cropping then it'll guarantee additional security than while not cropping case. As with cropping case we want cropped region at the decoder aspect then solely secret knowledge extraction is feasible. So cropped region works as a key at decoder aspect. For while not cropping methodology interloper could try and perform DWT randomly and may hack secret knowledge from sub-band with trial and error methodology. From the table one it's obvious that PSNR of while not cropping case is over with cropping case. So, this is often trade off that happens if we want additional security.



Fig6:Cropped Skinmask image Figure7:Cropped mask image



Fig8:Mask image Fig9:Stego image after embedding process

Table: 1 capacity and psnr of 4 final stego images in proposed method

Cover image(256x256)	Capacity of cover image		PSNR		Size of logo
	Case A	Case B	Case A	Case B	
Image 1	7173	5294	53.0	50.3	32x32

Image2	1067	1056	51.9	49.5	32x32
Image3	1452	1354	51.1	49.2	32x32
Image4	4850	2572	46.4	45.4	32x32
Average PSNR			50.7	48.5	

Case A- Without Cropping

Case B- With Cropping

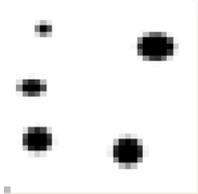


Fig10: Retrieved image

9. Conclusion

Digital Steganography may be a fascinating scientific space which falls underneath the umbrella of security systems. In this paper biometric steganography is bestowed that uses skin region of pictures in DWT domain for embedding secret knowledge. By embedding knowledge in mere bound region (here skin region) and not in whole image security is increased. Also image cropping idea introduced, maintains security at respectable level since nobody will extract message while not having worth of cropped region. Options obtained from DWT coefficients square measure utilised for secret knowledge embedding. This additionally will increase the standard of stego as a result of secret messages square measure embedded in high frequency sub-bands that human eyes square measure less sensitive to. in line with simulation results, projected approach provides fine image quality.

References

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, “Biometric inspired digital image Steganography”, in: Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS’08), Belfast, 2008, pp. 159-168.

[2] Petitcolas, F.A.P.: “Introduction to info Hiding”. In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) info activity Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

[3] Lin, E. T. and Delp, E. J.:“A Review of information activity in Digital Images”. Retrieved on one.Dec.2006 from laptop Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999

[4] Johnson, N. F. and Jajodia, S.: “Exploring Steganography: Seeing the Unseen.” IEEE laptop, thirty one (2): 26-34, Feb 1998.

- [5] Fridrich, J., Goljan, M. and Du, R., (2001). "Reliable Detection of LSB Steganography in Grayscale and Colour pictures." Proceedings of ACM, session on multimedia system Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.
- [6] Po-Yueh subgenus Chen and Hung-Ju designer "A DWT primarily based Approach for Image Steganography", International Journal of subject area and Engineering, 2006. 4, 3: 275-290
- [7] Chang, C. C., Chen, T.S and Chung, L. Z., "A steganographic methodology based upon JPEG and quantisation table modification," info Sciences, vol.[4], pp. 123-138(2002).
- [8] Provos,N. and Honeyman, P: "Hide and Seek: Associate in Nursing introduction to steganography". IEEE security and privacy, 01 (3): 32-44,May-June 2003
- [9] Abbas Chedda, Joan Condell, Kevin Curran and Paul megacycle Kevitt "A Skin Tone Detection formula for Associate in Nursing adaptational Approach to Steganography" , college of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, BT48 7JL, Londonderry, European country, UK,2008
- [10] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", reference of biometry by Springer-Verlag Berlin Heidelberg 2009
- [11] Sobottka, K. and Pitas, I.:"Extraction of facial regionsand options using Colour and form info." Proc. IEEE International Conference on Image process, pp. 483-486.(1996)