International Journal of Electronics, Communication & Soft Computing Science and Engineering (IJECSCSE)
ISSN: 2277-9477, Volume 2, Issue 1

"Image Stegnography by Skin Tone Detection"

VIKAS GUPTA DEEPALI BHAMARE P. B. SALUNKHE

Abstract - **Steganography is the art of hiding the existence of data in another transmission medium, archive secrete communication.[1] The goal of steganography is to hide an information message inside harmless cover medium in such way that it is not possible even to detect that secrete message. It does not replace cryptography but rather boosts the security using its obscurity features. Steganography method used in this paper is based on biometrics. And the biometric feature used to implement steganography is skin tone region of images [2]. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach – DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. With the help of cropping an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side. So with this object oriented steganogaphy we track skin tone objects in image with the higher security and satisfactory PSNR (Peak-Signal-to-Noise Ratio) .Modern steganography's goal is to keep its mere presence undetectable.**

Keywords - **Biometrics; Skin tone detection; DWT; DCT; Cropping; Security; PSNR**

I. INTRODUCTION

In this highly digitalized world, the Internet serves as an important role for data transmission and sharing. Some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-know procedure for secured data transmission frequently used encryption methods include RSA, DES (Data encryption standard). Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach called "steganography" arises. In steganography secret message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. The message embedding technique is strongly dependent on the structure of the cover. The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image should resemble the cover image under casual inspection and analysis. In addition, for higher security requirements. We can encrypt the message data before embedding them in the cover-image to provide further protection [3]. For this the encoder usually employs a stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image. For proposed method cover image is cropped interactively and that cropped region works as a key at decoding side yielding improved security. There are two things that need to be considered while designing the steganographic system: Invisibility: Human eyes cannot distinguish the difference between original and stego image. (b) Capacity: The more data an image can carry better it is. However large embedded data may degrade image quality significantly.

A modern steganogaphy system contains following modules. Modern steganographic system, as shown in Fig.1.attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes [3, 4].

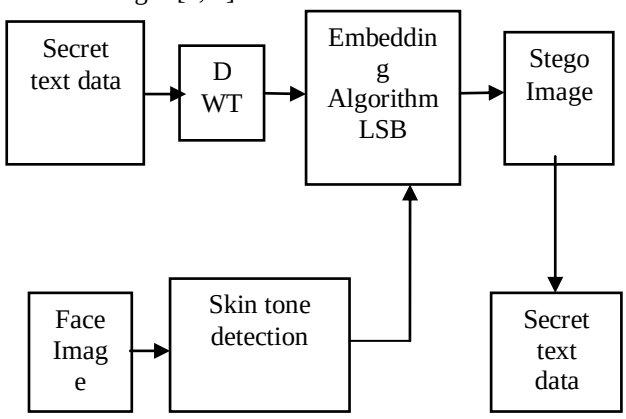


Figure 1. A modern steganography system.

Three basic types of stego systems are available:

Pure stego systems - no key is used.
Secret-key stego systems - secret key is used.
Public-key stego systems - public key is used.

II. LSB Encoding

This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. A digital image consists of a matrix of color and intensity values. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [5]. The mathematical representation for LSB is:

$$X_i' = X_i - X_i \bmod 2^k + m_i \qquad (1)$$

In Eq.1 xi ' represents i the pixel value of the stego-image and xi represents that of the original cover- image. mi represents the decimal value of the i th block in the confidential data. The number of LSBs to be substituted is k.[6] The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$$m_i = X_i \bmod 2^k \qquad (2)$$

Hence, a simple permutation of the extracted mi as in Eq.2 gives us the original confidential data [7]. The advantage of LSB embedding is its simplicity.LSB Embedding also allows high perceptual transparency.[8]

III. Steganography In Frequency Domain

Robustness of steganography can be improved if properties of the cover image could be exploited. For example it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to human HVS (Human Visual System). Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it [9]. Different sub-bands of frequency domain coefficients give significant information about where vital and non vital pixels of image resides. 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 either in DCT or DWT.

A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or biorthogonal, scalar or multiwavelets [10].

IV. Adaptive Steganography

Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" [10]and "Masking". This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

V. Proposed Method

Proposed method introduces a new method of embedding secret data within skin as it is not that much sensitive to HVS (Human Visual System).This takes advantage of Biometrics features such as skin tone, instead of embedding data anywhere in Image, data will be embedded in selected regions. Overview of method is briefly Introduced as follows. At first skin tone detection is performed on input image using HSV (Hue, saturation, value) color space. Secondly cover image is transformed in

Frequency domain. This is performed by applying Haar-DWT, the simplest DWT on image leading to four sub-bands. Then payload (number of bits in which we can hide data) is calculated. Finally secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band. Before performing all steps Cropping on input image is performed and then in only cropped region embedding is done, not in whole image. Cropping results into more security than without cropping.

Since cropped region works as a key at decoding side. Here embedding process affects only certain Regions of Interest (ROI) rather than the entire image. So utilizing objects within images can be more advantageous. This is also called as Object Oriented steganography .

VI. Skin Color Tone Detection

Detecting human skin tone is of almost importance in numerous applications such as video surveillance, face and gesture recognition, human computer interaction and steganography.

Detection of human skin tone is regarded as a two class classifications deals with biometrics and computer vision aspects.

A skin detector typically transforms a given pixel into an appropriate 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 defines a decision boundary of the skin color class in the color space. Using Bay's rule skin classifier detects skin color as in Eq.3

P(skin/c)=p(c/skin)p(skin)/p(c/skin)
p(skin)+p(c/not skin)p(not skin pixels) (3)

Although this is a straightforward process has proven quite challenging. Therefore, important challenges in skin detection are to represent the color in a way that is invariant or at least insensitive to changes in illumination.[11] and Another challenge comes from the fact that many objects in the real world might have skin-tone colors. This causes any skin detector to have much false detection in the background if the environment is not controlled [12] The simplest way to decide whether a pixel is skin color or not is to explicitly define a boundary. RGB matrix of the given color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. There exists several color spaces.Mainely two kinds 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.

VII. DISCRETE WAVELATE TRANSFORM (DWT)

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 resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT. DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as
LL – Horizontally and vertically low pass
LH – Horizontally low pass and vertically high pass
HL - Horizontally high passes and vertically low pass
HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band [14]. As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. DWT used in this work is Haar-DWT, the simplest DWT.

VIII. EMBEDDING PROCESS

Suppose C is original 24-bit color cover image of M×N Size.

$C = \{X_{ij}, Y_{ij}, Z_{ij} 1 \le i \le M, 1 \le j \le N, X_{ij}, Y_{ij}, Z_{ij} \in 0,1.....255\}$

Let size of cropped image is $M_c \times N_c$ where

$M_c \le M and N_c \le N and M_c = N_c$ (4)

i.e. Cropped region must be exact square as we have to apply DWT later on this region.

Let S is secret data. Here secret data considered is binary image of size a×b. Fig.2 represents flowchart of embedding process. Different steps of flowchart are given in detail below.

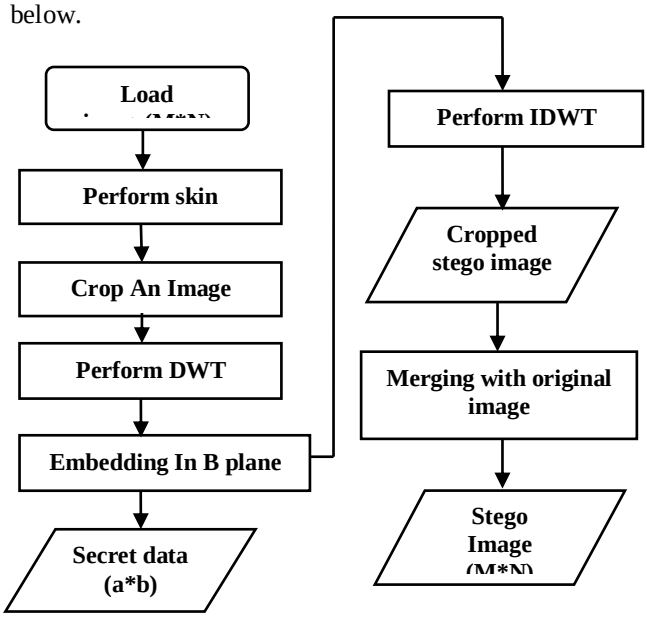


Figure 2. Flowchart of Embedding Process

1)Step 1:Once image is loaded, apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.

2) Step 2: Ask user to perform cropping interactively on mask image $M_c \times N_c$. After this original image is also cropped of same area. Cropped area must be in an exact square form as we have to perform DWT later and cropped area should contain skin region such as face, hand etc since we will hide data in skin pixels of one of the sub-band of WT. Here cropping is performed for security reasons. Cropped rectangle will act as key at receiving side. If it knows then only data retrieval is possible. Eavesdropper may try to perform DWT on whole image; in such a case attack will fail as we are applying DWT on specific cropped region only.

3) Step 3: Apply DWT to only cropped area $M_c \times N_c$ not whole image (M×N). This yield sub-bands denoted as $H_{LL}, H_{HL}, H_{LH}, H_{HH}$. (All 4 sub-band are of same size of $M_c / 2, N_c / 2$. Payload of image to hold secret data is determined based on no. of skin pixels present in one of high frequency sub-band in which data will be hidden.

4) Step 4: Perform embedding of secret data in one of sub-band that we obtained earlier by tracing skin pixels in that sub-band. Other than the LL, low frequency sub-band any high frequency sub-band can be selected for embedding as LL sub-band contains significant information. Embedding in LL sub-band affects image quality greatly. We have chosen high frequency HH sub-band. While embedding, secret data will not be embedded in all pixels of DWT sub-band but to only those pixels that are skin pixels. So here skin pixels are traced using skin mask detected earlier and secret data is embedded. Embedding is performed in G-plane and B-plane but strictly not in R-plane as contribution of R plane in skin color is more than G or B plane. So if we are modifying R plane pixel values, decoder side doesn't retrieve data at all as skin detection at decoder side gives different mask than encoder side.

Embedding is done as per raster-scan order that embeds secret data coefficient by coefficient in selected sub-band [6], if coefficient is skin pixel

5) Step 5: Perform IDWT (Inverse discrete wavelet transform)to combine 4 sub-bands.

6) Step 6: A cropped stego image of size $M_c \times N_c$ is obtained in above step (step 5). This should be similar to original image after visual inspection but at this stage it is of size $M_c \times N_c$, So we need to merge the cropped stego image with original image to get the stego image of size M×N. To perform merging we require coefficients of first and last pixels of cropped area in original image so that r calculated. Thus a stego image is ready for quality evaluation.

IX. EXTRACTION PROCESS

Secret data extraction is explained as follows: 24 bit color stego image of size M×N is input to extraction process. We must need value of cropped area to retrieve data. Suppose cropped area value is stored in 'rect' variable that is same as in encoder. So this 'rect' will act as a key at decoder side. All steps of Decoder are opposite to Encoder. Care must be taken to crop same size of square as per Encoder. By tracing skin pixels in H HH sub-band of DWT secret data is retrieved. Extraction procedure is represented using Flowchart in Fig. 3

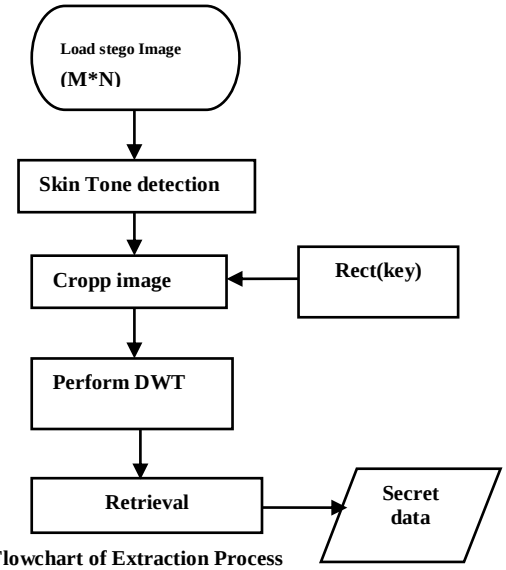


Figure 3. Flowchart of Extraction Process

X. PERFORMANCE MEASURE

Performance measurement for image distortion is well known as peak signal to noise ratio (PSNR) which is classified under the difference distortion metrics can be applied on stego images.

We use Peak signal to noise ratio (PSNR) to evaluate quality of stego image after embedding the secret message.

A 24 bit color image is employed as cover image of size 256*256 shown in figure 4, shows sample secret message to hide inside cover image. Secret message should be any word.

The performance in terms of capacity and PSNR (in dB) is demonstrated for the method in the following subsections. PSNR is defined as per Eq.5,

$$PSNR = 10\log_{10}(255^2 / MSE) \quad (5)$$

Where MSE is

$$MSE = (1/(M \times N))\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij}Y_{ij})^2 \quad (6)$$

X ij and y ij represents pixel values of original cover image and stego image respectively as in Eq.6 The calculated PSNR as in Eq.5 usually adopts dB value for quality judgment, the larger PSNR is, higher the image quality (which means there is a little difference between cover image and stego image).On the contrary smaller dB value means there is a more distortion.

PSNR values falling below 30dB indicate fairly a low quality. However, high quality strives for 40dB or more .

RESULT

Result is generally divided into three parts as skin detection, embedding and extraction. First cover image is browse in any format (JPEG) as shown inFig.4.after that skin tone detection is done from which cropping of image is taken out as shown in Fig.5. for the histogram modification.

Before embedding secret message in cropping region , secret key is generated with the help of DWT.After embedding the message, image is reconstructed called as stego image as in Fig.6. At the receiver side , secret message can be extracted in Fig.7.from stego image by IDWT(inverse discrete wavelet transform) and cropping. Then from stego image and cover image easily calculate MSE & PSNR with the Eq.5in Eq.6. From more than 40 images taken for the result 5 images are included in the result table.

But if method is implemented with cropping then it will ensure more security than without cropping case. As with cropping case we need cropped region at the decoder side then only secret data extraction is possible. So cropped region works as a key at decoder side. From the table it is observed that as MSE is less than the PSNR will high as because they are inversely proportional to each other.

The drawback of the proposed method is the computational overhead. Method requires resources from computer hardware (mainly processor, speed and memory like RAM. With the fast development in hardware manufacturing area , this problem will become trivial. [13]

First image for result

Figure 4 cover Image **Figure 5 cropped Image**

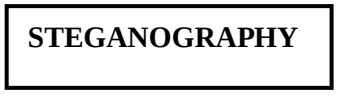


Figure 6 stego Image **Figure 7 secret message**

Second Image for result

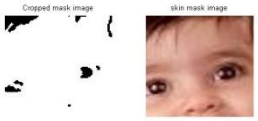
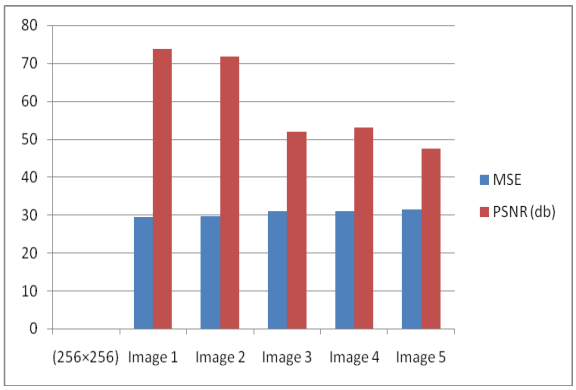


Figure 8 cover Image **Figure 9 cropped Image**

Figure 10 stego Image **Figure 11 secret message**

TABLE 1. MSE AND PSNR OF 5 FINAL STEGO IMAGES IN PROPOSED METHOD

SR NO	COVER IMAGE (256×256)	MSE	PSNR (db)	TEXT
1)	Image 1	29.453	73.7539	Message Normal size text (more than 100 characters)
2)	Image 2	29.5744	71.7198	
3)	Image 3	30.1358	63.0236	
4)	Image 4	30.8829	53.0626	
5)	Image 5	30.9742	51.9589	
5)	Image 6(radhu)	31.3674	47.4609	
6)	Image 7	32.5882	35.8314	



APPLICATIONS

The three most popular and researched uses for steganography in an open systems environment are convert channels, embedded data and digital watermarking.

CONCLUSION

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. In this paper biometric steganography is presented that uses skin region of images in DWT domain for embedding secret data. By embedding data in only certain region (here skin region) and not in whole image security is enhanced. Also image cropping concept introduced, maintains security at respectable level since no one can extract message without having value of cropped region. Features obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. According to simulation results, proposed approach provides fine image quality.

ACKNOWLEDGMENT

All work done, images shown in this paper are for educational purpose and not for commercial purpose.

REFERENCE SECTION

[1] AnjaliA. Shejul. Prof.U.L.Kulkarni"ADWT based approach for steganography using biometrics," in: Proceedings of the 2010 International conference on data storage and data Engineering.

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

[3] Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer,31 (2): 26-34, Feb 1998.

[4] Ali Al-Atab ,Fawzi Al-Naima-Iraq "A modified high Capacity Image steganography based on wavelate Transform"in International Arab Journal of information technology ,Vol-7 No.4 Oct2010

[5] Lin, E. T. and Delp, E. J.:"A Review of Data Hiding in Digital Images". Retrieved on 1.Dec.2006 from Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999

[6] Petitcolas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

[7] Fridrich, J., Golsjan, 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.

[8] 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

[9] 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).

[10] Provos,N. and Honeyman, P: "Hide and Seek: An introduction to steganography". IEEE security and privacy, 01 (3): 32-44,May-June 2003

[11] Abbas Chedda, Joan Condell, Kevin Curran and Paul Mc Kevitt "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography" , School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, BT48 7JL, Londonderry, Northern Ireland, UK,2008

[12] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009

[13] Chen,P. Y.and Liao,E.C., :A new Algorithem for Haar Wavelet Transform," 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp.453-457(2002)

AUTHOR'S PROFILE

VIKAS GUPTA
Electronics & Communication Engineering
TIT, BHOPAL
vgup24@yahoo.com

DEEPALI BHAMARE
Electronics & Communication Engineering
TIT,BHOPAL
deepali2402@yahoomail.com

P. B. SALUNKHE
Electronics & Communication Engineering
S.S.V.P.S.COE.
pallavinc.1982@rediffmail.com