International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

Survey on Steganography Using Wavelet Transform and Biometrics

[1] K.Mallesh Goud [2] K.Radhika [3] D.Jamuna

Abstract:

In this paper, Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. 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. 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. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side. This study shows that by adopting an object oriented steganography mechanism, in the sense that, we track skin tone objects in image, we get a higher security. And also satisfactory PSNR (Peak-Signal-to-Noise Ratio) is obtained.

Keywords: Steganography and water marking, Biometrics; Skin tone detection, DWT,

`1.INTRODUCTION:

In this highly digitalized world, the Internet serves as an important role for data transmission and sharing. However, since it is a worldwide and publicized medium, 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, and in this paper covers and secret messages are restricted to being digital images. 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. 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.

In the existing system we are using the different techniques like LSB and HSB. In these techniques the water mark can be inserted anywhere in the image which can reduces the quality of the image and makes the water mark reveals to HVS. 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. 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. Hence, a simple permutation of the extracted mi gives us the original confidential data. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane.

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. 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. Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" 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.

The main purpose of the proposed system is to develop an efficient stenographic system that can provide security using water marking techniques. Here we are using the biometric based techniques which can more security and efficiency. Here it is taking biometric based technique in which we are hiding the image in selected regions of the image unlike anywhere in other watermarking techniques. The main objective of the system is to provide the security to the data in an efficient way that can stores the data in the Container image which is not much sensitive to the HVS.This application using the biometric based techniques which are efficient and more secure than the existing systems like LSB, HSB etc. Scope of the proposed system reveals the application requirements in different views which are used to estimate the cost of the application. Skin Detection in Container Image. Water Mark Image Cropping, DWT on watermark image, Merging with original Image.

It 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 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

2. Steganography and Watermarking:

.Watermarking is very similar to Steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Digital watermarking is the technique of embedding digital marks inside a container so that there is a logical way of extracting the data embedded, while not harming the container in any perceived way. Steganography uses cover files to deliver its messages. On the other hand watermarking considers the cover file as the important data that is to be preserved. In Steganography purpose of embedded data is to deliver secret communication. In watermarking, purpose of embedded data is to supply some additional information about the cover image such as image owner to verify image's ownership to achieve control over the copy process of digital data. In Steganography, the object of communication is the hidden message. In digital water-marks, the object of communication is the cover. In short, Steganography pay attention to the degree of invisibility while Watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image Operations.

3. Implementaion:

3.1Discrete Wavelet 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 pass 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 . 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

3.2. Skin detection:

Skin color has proven to be a useful and robust cue for face detection, localization and tracking. Image content filtering, content aware video compression and image color balancing applications can also benefit from automatic detection of skin in images. Face detection and tracking has been the topic of an extensive research for several decades. Many heuristic and pattern recognition based strategies have been proposed for achieving robust and accurate solution. Among feature-based face detection methods, the ones using skin color as a detection cue have gained strong popularity. Color allows fast processing and is highly robust to geometric variations of the face pattern. Also, the experience suggests that human skin has a characteristic color, which is easily recognized by humans. When building a system, that uses skin color as a feature for face detection, the researcher usually faces three main problems. First, what color space to choose, second, how exactly the skin color distribution should be modeled, and finally, what will be the way of processing of color segmentation results for face detection.

3.3. Colour spaces

Colorimetry, computer graphics and video signal transmission standards have given birth to many color spaces with different properties. A wide variety of them have been applied to the problem of skin color modeling.

A. RGB

RGB is a color space originated from CRT (or similar) display applications, when it was convenient to describe color as a combination of three colored rays (red, green and blue). It is one of the most widely used color spaces for processing and storing of digital image data. However, high correlation between channels, significant perceptual non-uniformity, mixing of chrominance and luminance data makes RGB not a very favorable choice for color analysis and color based recognition algorithms.

B. YCbCr

YCbCr is an encoded nonlinear RGB signal, commonly used by European television studios and for image compression work. Color is represented by luma (which is luminance, computed from nonlinear RGB), constructed as a weighted sum of the RGB values, and two color difference values Cr(Chrominance red) and Cb(Chrominance blue) that are formed by subtracting luma from RGB red & blue components. The transformation simplicity and explicit separation of Luminance and chrominance components make this color space attractive for skin color modeling.

C. HSV (Hue, Saturation, Value)

Hue-saturation based colorspaces were introduced when there was a need for the user to specify color properties numerically. They describe color with intuitive values, based on the artist's idea of tint, saturation and tone. Hue defines the dominant color (such as red, green, purple and yellow) of an area; saturation measures the colorfulness of an area in proportion to its brightness. The "intensity", "lightness" or "value" is related to the color luminance. The intuitiveness of the color space components and explicit discrimination between luminance and chrominance properties made these colorspaces popular in the works on skin color segmentation.

3.4. Embedding Process:

Suppose C is original 24-bit color cover image of M×N Size. It is denoted as: C= {xij, yij, zij |1 ≤ i ≤ M, 1 ≤ j ≤ N, xij, yij, zij Є {0,1,..,255}}

Let size of cropped image is Mc×Nc where Mc≤M and Nc≤N and Mc=Nc. 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. 1 represents flowchart of embedding process. Different steps of flowchart are given in detail below.

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 (Mc×Nc). 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 DWT. 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.

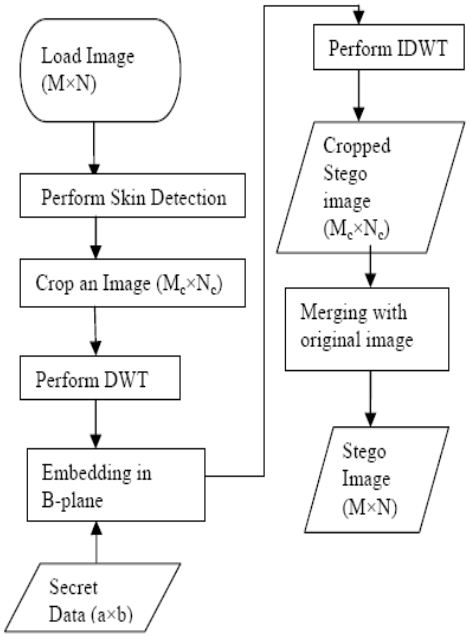

Fig:3.4. Flowchart of Embedding Process

3) Step 3: Apply DWT to only cropped area (Mc×Nc) not whole image (M×N). This yields 4 sub-bands denoted as HLL, HHL, HLH, HHH . (All 4 sub-bands are of same size of Mc/2, Nc/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 subband 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 (as shown in Fig) that embeds secret data coefficient by coefficient in selected sub-band [6], if coefficient is skin pixel.

5) Step 5: Perform IDWT to combine 4 sub-bands.

6) Step 6: A cropped stego image of size Mc×Nc 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 Mc× Nc, So we need to merge the cropped stego image

3.5 Extraction Watermarking:

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 HHH sub-band of DWT secret data is retrieved. Extraction procedure is represented using Flowchart.

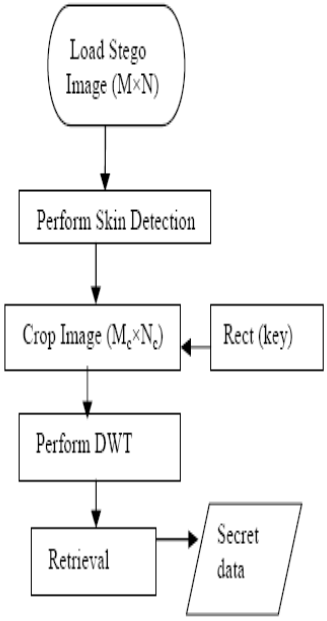

Fig 3.5Flowchart of Extraction Process

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.

4. Related work:

Steganography can be improved if properties of the cover image could be exploited. 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. Different sub-bands of frequency domain coefficients give significant information about where a vital and non vital pixel 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 low robustness to different attacks. In contrast, embedding in the lower frequencies helps to withstand many attacks but creates perceptible impact on the media. So, middle frequency bands 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 either in DCT or DWT

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 LLsub-band . As other three sub-bands are high frequencies sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. In this work, we use simplest DWT, Haar-DWT, to transform images into frequency domain.

1) Advantages of Haar Wavelet transform as follows:
• Best performance in terms of computation time.
• Computation speed is high.
• Simplicity.
It performs two steps, row and column transformation respectively. Entire row of an image matrix is taken, then do the averaging, differencing is done. After we treated entire row of an image matrix, then do the averaging and differencing process for the entire each column of images.
2) Procedure for Haar Wavelet Transform: To calculate the Haar transform of an array, procedure is given below].
• Find the average of each pair of samples.
• Find the difference between each average and the Samples it was calculated from.
• Fill the first half of the array with averages.
• Fill the second half of the array with differences.
Haar-DWT can be performed using matrix multiplication• Repeat the process on the first half of the array. The steganography is used in the covert communication to transport secrete information

6. Conclusion:

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.

References:

[1] 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

[2] 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).

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

[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,

[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] Raja K B, C R Chowdary, Venugopal K R, L M Patnaik. (2005) :"A Secure Steganography using LSB, DCT and Compression Techniques on Raw Images," IEEE International Conference on Intelligence Sensing and Information processing, pp.171-176.

[7] Kumar V and Kumar D. (2010): "Performance Evaluation of DWT Based Image ," IEEE International Conference on Advance Computing, pp. 223-228.

[8] O El Safy, H H Zayed and A El Dessouki (2009): "An Adaptive Steganographic Technique Based on Integer Wavelet Transform,"International Conference on Networking and Media Convergence, pp.111-11.

Author's Information

[1] **K.Mallesh goud** pursuing M.Tech CSE from jaya prakash Narayana College of Engineering & Technology B.Tech from jaya prakash narayana College of Engineering. His areas of interest include Data mining, Network Security, Software Engineering and Sensor Network.

[2]K.RadhikaD., Working as Associate Professor CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(SE) from Sri Sai Jyothi engineering collge, JNTUH, Hyderabad. B.Tech (CSE) from Jayaprakash Narayan College of Engineering, Mahabubnagar Experience 8 Years in Teaching Profession. Her areas of Interest are in Wireless Sensor Networks

[3] **Prof.D.Jamunna**, Working as Professor & Head of CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(SE) from School of Information Technology, JNTUH, Hyderabad. BE (CSE) from Vijayanagara Engineering College, Bellary. Experience 17 Years in Teaching Profession. Her areas of Interest are in Wireless Sensor Networks, Data Mining, and Networking and guided M. Tech and B. Tech Students IEEE Projects.