Implementation of Steganoflage Using Skin Tone Espial

Nagaveni.S.A, Chandrappa.D.N

***Abstract*— This paper exploits one of the biometric aspects like skin tone regions in an image to implement Steganoflage. Steganoflage is the technique of hiding the any form of data in another transmission medium for a classified communication. Here the confidential information or data is embedded in the skin toned pixel regions of an image, which provides an exemplary and secure location for hiding the data. In order to recognize the skin toned regions in images, HSV (Hue, Saturation and Value) color space is used. In addition to this secret data is embedded using DWT (Discrete Wavelet Transform). Confidential data is hidden in one of the high frequency sub-spaces of DWT by tracking skin pixels in that sub-space. Another technique employed here is interactive cropping of the image. One of the main significance of cropping is it leads to increase the security because the cropped region acts as a key at the extraction side.**

Keywords—Cropping, Steganoflage, Skin tone detection, HSV, DWT.

I. INTRODUCTION

The word *Steganoflage* is a fusion of two words: "steganography" and "camouflage". Here the term steganography is of the Greek origin with the meaning "covered or concealed writing" and camouflage means "disguising or hiding in plain sight". Steganoflage is hence the art or practice of hiding a message, image or a file within another message, image or file (i.e. computer files). Steganoflage is sometimes used when encryption is not permitted. Computer media files are ideal elements for Steganoflage transmission because of their large size. The change due to Steganoflage is so subtle that a person not specifically looking for it is unlikely to notice it.

There raises the question of necessity of the application of steganography. In today's world, most of the communication means are digital. Since there is a possibility of the message being stolen, hacked, copied, modified or even destroyed, safe and secure means of communication becomes significant. Encryption is a well-know procedure for secured data transmission [1]. Even though encryption provides security, it also attracts unnecessary attention of the people as someone who is curious may try to decrypt it. As an example, the cover text [2]: "I'm feeling really stuffy. Emily's medicine wasn't strong enough without another febrifuge", hides the sentence "Meet me at nine" If the reader retains the second letter of each word in sequence. But in Steganoflage technique, there is no chance of the secret data being detected as the message will be not visible and also confidential.

In this paper, Image Steganoflage is used, that is, the secret message is hidden inside an image. Here the image in which the confidential data is hidden is called as "*cover-image*". And the image in which the confidential or secret message is hidden is called "*stego-image*". Also in this paper, the secret data or message is in the text format. 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]. While designing the steganoflagic system, invisibility factor i.e. human eyes should not distinguish the difference between original and stego image should be considered [4]. The next following section gives an insight on some of the existing Steganoflage methods.

II. EXISTING METHODS

A. Spatial Domain Techniques

The simplest and more than often used spatial domain technique is LSB (Least Significant Bit) substitution method. Here the confidential information is directly ingrained into the least suasive plane of the cover image. The basic notion of LSB substitution is to ingrain the confidential data at the rightmost bits (bits with the smallest weighting) so that the ingraining procedure does not affect the original pixel value greatly [5]. This method is easy and straight-arrow but this has low ability to carry some signal processing or noises. And confidential data can be facilely filched by extracting whole LSB plane.

B. Transform Domain Techniques

Transform domain steganoflagic methods hide data in the coefficients of the represented demesne. After mapping the signals to another demesne such as DFT, cosine transform, Hartley transform, and wavelet transforms, the obtained coefficients are amended or reinstated. The methods are more robust than spatial domain ingraining techniques while maintaining better image condition. They are also unbiased to various image file formats either lossy or lossless image formats; however, have lower capacity [6].

C. Adaptive Steganography

Adaptive steganoflage is exclusive case of two aforementioned methods. It is also known as "Statistics aware ingraining" and "Masking". This method takes statistical global features of the image before attempting to ingrain

Manuscript received March 1, 2015.

Nagaveni.S.A*, M.Tech (Digital Electronics), Dept. of ECE, GMIT, Davangere, India,*

Chandrappa.D.N, *Associate Professor, Dept. of ECE, GMIT, Davangere, India*

ISSN: 2278 – 909X

confidential data in DCT or DWT coefficients. The statistics will edict where to make changes [4].

III. PROPOSED METHOD

The method proposed in this paper mainly exploits the perceptibility or sensitivity of the Human Visual System (HVS). Here the confidential data is ingrained in the skin tones regions of an image as modifications in skin regions of an image is not much responsive to human visual system [7]. A meticulous outline of some of the stages used in this paper is as follows:

A. Skin Tone Espial

Skin tone espial is nothing but process of detecting the skin toned pels in an image. In this paper, for the intent of detection of skin toned pels, HSV (Hue, Saturation and Value) colour space is used. HSV is a transformation of an RGB colour space and its elements and colorimetry are proportional to the RGB colour space from which it was deduced.

Skin is the most widely used primitive in human image processing research and computer vision with applications ranging from face detection to person tracking. The process of skin tone espial is typically used as a pre-processing step to find regions that potentially have human faces and limbs and other body parts in images. A skin locator typically transforms a given pixel into an appropriate colour space (in this case HSV colour space) and then uses a skin segregator to label the pixel whether it is a skin or a non-skin pel. A skin segregator defines a decision boundary of the skin colour class in the skin colour space based on a training database of skin-coloured pels.

The colour of human skin is a combination of blood (red) and melanin (brown, yellow) which gives it a limited range of hues. Human skin is not deeply saturated either, therefore the human skin color likely occupies a specific (clustered) region of any color space. This suggests that we can try to model skin color distribution based on specifications of the skin color cluster. Sobottaka and Pitas defined a face localization based on HSV. They found that human flesh can be an approximation from a sector out of a hexagon with the constraints:

Smin= 0.23, Smax =0.68, Hmin =0^{0} and Hmax=50^{0} [4].

B. Discrete Wavelet Transform (DWT)

The wavelet transform describes a multi-resolution disintegration process in terms of expanse of an image. Discrete Wavelet Transformation has its own excellent space frequency localization property [8]. The DWT splits the signal into high and low frequency segments. The high frequency segment contains information about the edge elements, while the low frequency part is split again into high and low frequency segments.

The high frequency elements are usually used for steganoflage since the human eye is less sensitive to changes in those components. In two dimensional applications, for each level of disintegrations, DWT is first performed vertically and then in horizontal direction. When applying DWT on an image, four different sub-images are obtained as follows:

(1) Low-Low (LL): This is a crude approximation to the authentic image comprising the overall information about the complete image. It is obtained by applying the low-pass filter on both coordinates.

(2) High-Low (HL) and Low-High (LH): These are obtained by applying the high-pass filter on one of the coordinate and the low-pass filter on another.

(3) High-High (HH): This gives the high frequency element of the image in the diagonal direction. It is achieved by applying the high-pass filter on both coordinates.

Since human eyes are much sensitive to the low frequency region (Low-Low sub-image), Low-Low is the most important element in the reconstruction process [9]. The ingraining procedure is as shown below in figure 1.

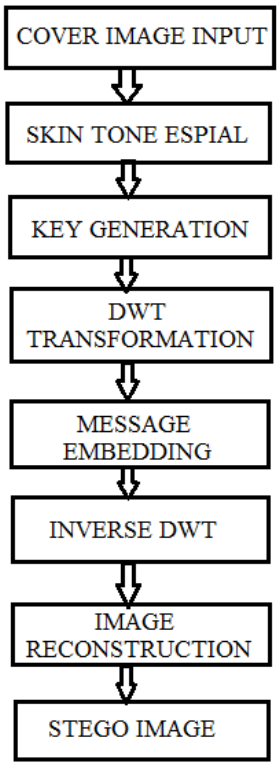

Figure 1. Embedding Process

C. Embedding Process

In the ingraining procedure, the following different steps are involved as shown in figure 1:

1) Cover image (MxN) is loaded.
2) Apply skin tone detection on cover image which will lead to the production of the mask image that contains skin and non skin pels.
3) The user is asked to perform cropping interactively on unmasked image (Mn×Nn). After this, the authentic image is also cropped of same area. The cropped zone should contain skin regions such as face, hand etc since confidential data is hidden in skin pels of one of the sub-space of DWT. Here cropping is executed for security purposes. Cropped rectangle will act as key at receiving side. If someone tries to perform

ISSN: 2278 – 909X

DWT on whole image and in such a case, attack will be unsuccessful because we are applying DWT on specific cropped zone only.

4) Apply DWT to only cropped zone (Mn×Nn). Here the DWT is not applied to the whole image (M×N). This yields 4 sub-spaces (All 4 sub-spaces are of the same area of (Mn/2, Nn/2).

5) Confidential data is ingrained in one of the sub-space which was attained earlier by tracking skin pels in that sub-space. Instead of Low-Low, any high frequency sub-space can be selected for ingraining as Low-Low contains important information. Ingraining in Low-Low sub-space will affect the image quality very much. In this paper, high frequency High-High sub-space is chosen. Ingraining is implemented in Green-plane and Blue-plane but stringently not in Red-plane as contribution of Red plane in skin color is more than Green or Blue plane. So if we are modifying Red plane pixel values, extraction side doesn't retrieve data at all as skin detection at decoder side gives different mask than retrieval side. Embedding is done as per raster-scan order that ingrains confidential data coefficient by coefficient in selected sub-space, if coefficient is skin pixeled.

6) Inverse DWT is performed to combine all the four sub-bands.

7) Finally reconstruction is done by merging the cropped image which contains the confidential data with the cover image. The image obtained is called as the stego-image.

IV. SIMULATION RESULTS

The simulation results of before and after the embedding of the secret message is as shown in figure 2 and 3 below. It can be seen that there is no visible changes in the stego-image even after embedding.

Figure 2. Cover Image and Stego-Image.

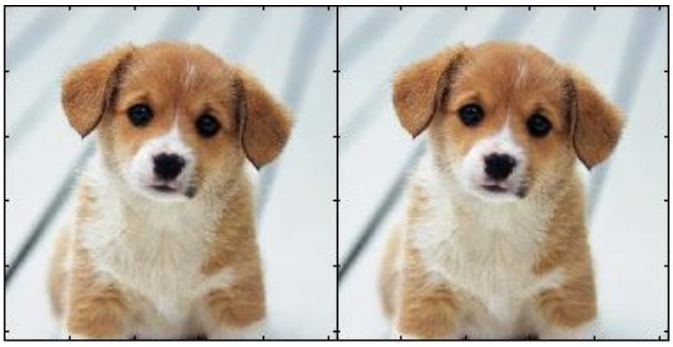

Figure 3. Cover Image and Stego-Image.

The simulation results were obtained using MATLAB R2013a software. Both the images used as cover images are of size 512x512. The method proposed in this paper can take input images of any resolution. But high resolution images take more processing time. Also the cover image format can be any of the generally used formats such as .jpg, .png, .bmp.

Table-1. PSNR Evaluation

Cover Image (512x512)	**PSNR (dB)**
JPEG image	73.71
PNG image	75.90
BMP image	78.50

For analysis 512x512 images of formats .jpg, .png and .bmp were used. PSNR (Peak Signal to Noise Ratio) for each of these images was calculated and tabulated as shown in in Table-1 above. It was seen that bitmap images (.bmp) give more PSNR than the other two image formats. Even though JPEG format images are most commonly used images for steganoflage, the other formats give better results. But in general, image of any format mentioned above with any resolution can be used to implement the proposed method.

V. CONCLUSION

Digital steganoflage proposed in this paper uses one of the most primitive biometric features, skin tone for the concealing or embedding of the secret data along with the features like cropping. Even though cropping ensures security, it is necessary that the cropped region be present at the retrieving side as it acts as the key. This approach may further be extended to other transfer domains for better results. As seen from the simulation results, the proposed approach provides better image quality.

REFERENCES

ISSN: 2278 – 909X

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

[2] 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

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

[4] Anjali A. Shejul, Umesh L. Kulkarni "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011,1793-8201

[5] 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

[6] Swati Kumravat, "An Efficient Steganographic Scheme Using Skin Tone Detection and Discrete Wavelet Transformation", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 4 No. 07 Jul 2013

[7] 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

[8] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, (IJCSS), Vol. 4, No. 6, 2010, pp 561-570

[9] Ahmed A. Abdelwahab and Lobna A. Hassaan,"A Discrete Wavelet Transform Based Technique for Image Data Hiding", 25th [6] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt,"Biometric Inspired Digital Image Steganography", 15 National Radio Science Conference (NRSC), March 18-20, 2008

BIOGRAPHIES

Nagaveni.S.A has completed her B.E in E&CE discipline from Visvesvaraya Technological University at UBDTCE. She is currently pursuing M.Tech in Digital Electronics from Visvesvaraya Technological University at GMIT.

Dr. Chandrappa.D.N has completed his B.E in ECE discipline at Kuvempu University and M.Tech in Digital Communication & Networking at Davangere University. He secured his Ph.D from Gulbarga University in the discipline Microstrip antennas for wireless communications. He has published 7 international journals and has attended a national and international conference. He is currently working as Associate Professor in Dept. of ECE at GMIT, Davangere, Karnataka.

ISSN: 2278 – 909X