International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 1, January 2013 ISSN 2319 - 4847

AES BASED STEGANOGRAPHY

Manoj gowtham.G.V[1], Senthur.T[2], Sivasankaran.M[3], Vikram.M[4], Bharatha Sreeja.G[5]

[1,2,3,4] Final Year ECE, [5] Assistant Professor
SNS College Of Engineering, Coimbatore, India

ABSTRACT

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 encrypted by AES (Advanced Encryption Standard) and embedded within skin region of image that will provide an excellent secure location for data hiding. For simplicity and better results this skin tone detection is performed using RGB thresholding technique rather than the HSV (Hue Saturation Value) colour space technique. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet 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. Security is increased by giving password for cropped regions. So cropped region works as a key at decoding side. This work shows that the skin tone objects tracked with higher security and also satisfactory PSNR (Peak-Signal-to-Noise Ratio) is obtained.

Key-words: AES, Biometrics, Skin tone detection, DWT.

1. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing".

Skin detection is a very popular and useful technique for detecting and tracking human-body parts. It receives much attention mainly because of its wide range of applications such as, face detection and tracking, naked people detection, hand detection and tracking, people retrieval in databases and Internet, etc.

A Two Way security mechanism introduced in steganography using skin colour detection scheme as well as cryptography. In spatial domain steganography the secret data modifies cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the simplicity[14],[18],[37].

New algorithms keep emerging prompted by the performance of their ancestors (Spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS(Human Visual System), its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain. DCT is used extensively in Video and image (i.e., JPEG) lossy compression[7],[18],[25],[28].

Adaptive Steganography is a special case of the two former methods (Spatial Domain, Frequency Domain). It is also known as “Statistics-aware embedding” and “Masking” .This method takes statistical global features of the image before attempting to interact with its DCT coefficients. The statistics dictate where to make the changes. This method is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD (Standard Deviation) .The latter is meant to avoid areas of uniform colour e.g., smooth areas. It is proven to be robust with respect to compression, cropping and image processing[1],[4],[10],[13].

Objective of this work is to embed the data in the image by using Discrete Wavelet Transform by tracing the skin pixels in one of the high frequency sub band and the secret data is encrypted [AES] before embedded into the cover image.

This will increase the security of secret data. The skin pixels are classified based on colour segmentation using HSV colour space. In future this work can also be implemented for embedding secret image (binary) into the cover image.

2. 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)[1].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 subbands. 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[1]. Next sub-sections briefly introduce skin tone detection and DWT.

2.1 Skin Tone Colour Detection using HSV

The goal of skin colour detection is to build decision rule that will discriminate between skin and non-skin pixels. A skin detector typically transforms a given pixel into an appropriate colour space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel. The skin detection algorithm produces a mask, which is simply a black and white image[35]. The black pixel values are 0 (false) and the white pixel values are 1 (true). This mask of ones and zeros acts as a logic map for skin detection (i.e., if a pixel is 1 this pixel location is likely skin).The simplest way to decide whether a pixel is skin colour or not is to explicitly define a boundary. RGB matrix of the given colour image can be converted into different colour spaces to yield distinguishable regions of skin or near skin tone. Mainly two kinds of colour spaces are available HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces. For this work HSV colour space is chosen. It is experimentally found and theoretically proven that the distribution of human skin colour constantly resides in a certain range within the colour space. The skin in channel H is characterized by values between 0 and 50, in the channel S from 0.23 to 0.68 for Asian and Caucasian ethnics[8].

Fig. 1: Original image

Fig. 2: Image in HSV

Fig. 3: Skin Region Detected Image.

Figure 1 illustrates the original image. Figure 2 shows the same image of figure 1 convert from RGB to HSV, considering now each channel HSV represented on the R, G and B channels. Figure 3 illustrates an intermediary image, where all pixels classified as skin (using the range in channel H already established) were set to value 255, and

non-skin pixels was fixed to 0. In the image of figure 3 there are having many noises, in the classification of pixels like skin and non-skin.

Next step minimize these noises, using a 5x5 structuring element in morphological filters. First, the structuring element introduced with a dilatation filter that expands the areas in the skin regions. After that the same structuring element used to erode the image and reduce all the imperfections that the dilatation created. These technique used, by approximation, to fill all the spaces that were by H channel range supposed that is skin or non-skin. Then, a 3x3 median filter used to soften more the results achieved by the dilatation and erosion, because these techniques adulterated regions in contours[12].Finally, only skin regions are represented as white pixels. This result is shown in the below Fig 4.

Fig. 4: Morphological (erosion and dilution) Processed Image

2.2 Discrete 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 by 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 subbands 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 subband) secret message is hided in other three parts without making any alteration in LL subband. 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.

2.3 AES (Advanced Encryption Standard)

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations.

The main loop of AES performs the following functions:

SubBytes()

SubBytes() adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

ShiftRows()

ShiftRows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.

MixColumns()

MixColumns() also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics

AddRoundKey()

The actual 'encryption' is performed in the AddRoundKey() function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule.

2.4. Embedding Process

Suppose C is original 24-bit colour cover image of M×N Size. It is denoted as $C=\{X_{ij}, Y_{i,j}, Z_{i,j} | 1 \leq i \leq M, 1 \leq j \leq N, X_{ij}, Y_{i,j}, Z_{i,j} \in \{0,1, \ldots 255\}\}$. 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 to apply DWT later on this region. Let S is secret data. Here secret data considered is binary image of size a=b. Different steps of embedding process are given in detail below.

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.

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 to perform DWT later and cropped area should contain skin region such as face, hand etc since the data is hided 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.

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 and 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 the number of skin pixels present in one of high frequency sub-band in which data will be hidden.

Step 4

Encrypt the data by using the AES encryption method.

Step 5

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. Here high frequency HH sub-band is chosen. 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 pixels are traced using skin mask detected earlier and secret data is embedded. Embedding is performed in G-plane and B-plane. So if R plane pixel values are modified, decoder side doesn't retrieve data at all as skin detection at decoder side gives different mask than encoder side.

Step 6

Perform IDWT to combine 4 sub-bands.

Step 7

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 the cropped stego image is merged with original image to get the stego image of size M×N. To perform merging, coefficients of first and last pixels of cropped area are required in original image so that are calculated. Thus a stego image is ready for quality evaluation.

2.5 Extraction Process

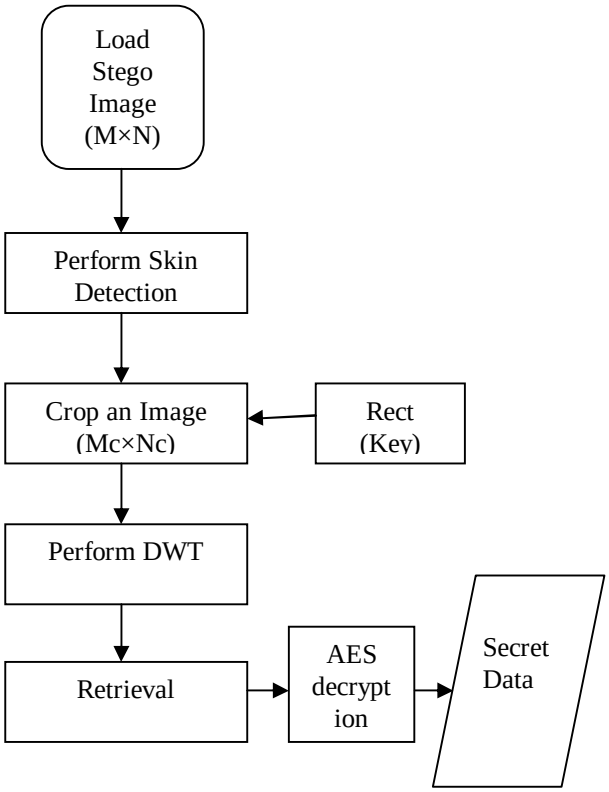

Fig. 5: Flow Chart of Extraction Process

A 24 bit colour stego image of size M×N is input to extraction process. The value of cropped area is needed 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 HH sub-band of DWT encrypted data is retrieved. The data is decrypted by AES decryption method and the secret data is obtained. Extraction procedure is represented using flowchart

3. RESULT AND DISCUSSION

In this section demonstrates the simulation results for proposed scheme. These have been implemented using MATLAB 2010a.

Fig. 6: skin detected image

Fig. 7: cropped image

Fig. 8: DWT HH image

Fig. 9: Resized image

Fig. 10: Stego image

Fig. 11: Input image

Skin detected image is shown in figure 6. Then each white pixel is replaced by corresponding RGB pixel value is shown in figure 7. DWT applied to the figure 7 and the HH subband image is shown in figure 8 and resized image is in figure 9. Then the input text 'SNSCollegeofEng' is encrypted by using AES algorithm and embedded in the figure 9. The output stego image is shown in figure 10. There is no visual difference between the output image and input image.

The secret message S is text of 16 characters. Peak signal to noise ratio (PSNR) is used to evaluate quality of stego image after embedding the secret message. The performance in terms of capacity and PSNR (in dB) is demonstrated for the method in the following subsections.

PSNR is defined as

$$PSNR = 10\log\left(\frac{255^2}{MSE}\right)$$

Where,

$$MSE = \left(\frac{1}{M \times N}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij})^2$$

X_{ij} and Y_{ij} represents pixel values of original cover image and stego image respectively. The calculated PSNR usually adopts dB value for quality judgement, 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.

There are several problems that have arisen when it comes to steganalysis. Since it is a relatively new and growing field, all the problems have not quite been worked out. One of the biggest problems is getting a high number of false positives. This can be attributed to the large amount of images and other kinds of media, and the wide range of sources of these files. A digital camera is a good example of this. There are over 20 different manufacturers of digital cameras, and they all have several models. Between all the different models, form all the different manufacturers, there are over a hundred different formats, using different algorithms for compression. These images can be manipulated by the camera, or image editing programs on the computer. All of this editing and compressing makes it very difficult to determine a normal format for which to compare other images against. Monotone pictures and drawings also come up with high false positive rates. It is also extremely hard to detect small messages of 50 bytes or less, the best results, at least for Stegdetect, are with messages that are 150 bytes or more.

Another big problem is that many times steganography programs also encrypt the information. Therefore, even if someone was able to detect steganographic images, it is exceptionally difficult to retrieve this information. That is a big problem that Niels Prevos has been having. He developed Stegbreak, that launches a dictionary based attack, but it only works really well on small, easy passwords. It also takes a lot of time and often several machines to successfully break even one password.

In this work skin region act as secure location for secret data. But the problem is detection of skin pixel. Because in the real world most of the objects have skin colour. So the skin detection method introduced in this work based on skin colour will also detects the pixel which is not skin pixel but has the same colour of skin. This work adopts the HSV based skin segmentation.

Another one challenge is the size of secret data. In this work the AES (Advanced Encryption Standard) is used to encrypt the secret data. This will increase the size of secret data results low PSNR value. Due low PSNR value the quality of stego image is also get reduced. This can be avoided by compressing the data before encryption.

In this work the secret data is text message and the cover medium is colour image. The use of colour image will increase the complexity of the algorithm.

4. CONCLUSION AND FUTURE ENHANCEMENTS

In this paper a new high capacity steganography method in wavelet domain is introduced. In order to achieve a higher quality of the stego image, we firstly estimate the capacity of each DWT block using the BPCS. The embedding process is then performed over the whole block, rather than in its bit-planes. This approach to the embedding ensures that no noisy bit-plane is left unused. Therefore, we achieve a much greater capacity as compared to that offered by previous methods, as confirmed by analysis and experiments. The proposed approach to the embedding process may also be extended to other transform domains to improve the compromising interrelation between capacity and imperceptibility in image steganography.

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 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 image 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.

REFRENCES

[1] Ahsan, K. & Kundur, D., “Practical Data hiding in TCP/IP”, Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002 [1]

[2] Albiol, L. Torres, and E. J. Delp. “Optimum colour spaces for skin detection.” In proceedings of the 2001 international conference on image processing, volume 1,vol. 1, pp. 122-124 ,2001.

[3] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998

[4] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001

[5] Avcibas, I. Memon, N. and Sankur, B.: Image Steganalysis with Binary Similarity Measures. Proceedings of the international conference on Image Processing, 3: 645-648. 24-28 June 2002.

[6] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal, Vol 35, 1996

[7] Castleman, K.R., Digital Image Processing. Second ed. 1996, Englewood Cliffs, New Jersey: Prentice-Hall.

[8] Chandramouli, R., Kharrazi, M. & Memon, N., “Image steganography and steganalysis: Concepts and Practice”, Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[9] Chin-Chen Chang, Piyu Tsai and Min-Hui Lin.: An Adaptive Steganography for Index-Based Images Using Codeword Grouping. PCM (3) 2004: 731-738. (2004).

[10] Digital Image Processing Second Edition Rafael C. Gonzalez University of Tennessee Richard E. Woods MedData Interactive Prentice Ch9 Morphological Image Processing

[11] Fard, A. M., Akbarzadeh-T, M. and Varasteh-A, F: A New Genetic Algorithm Approach for Secure JPEG Steganography. Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22-23 April 2006, 1- 6.

[12] Fridrich, J., Goljan, M. and Du, R.., (2001). Reliable Detection of LSB Steganography in Grayscale and Colour Images. Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.

[13] Fridrich, J., Goljan, M. and Hogeg, D.: Steganalysis of JPEG Images: Breaking the F5 Algorithm. Proceedings of Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, 2578/2003: 310-323, October 7-9, 2002.

[14] Handel, T. & Sandford, M., “Hiding data in the OSI network model”, Proceedings of the 1st International Workshop on Information Hiding, June 1996

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

[16] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998

[17] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, Proceedings of the 2nd Information Hiding Workshop, April 1998

[18] Kermani, Z. Z. and Jamzad, M.: A Robust Steganography Algorithm Based on Texture Similarity using Gabor Filter. Proceedings of IEEE 5th International Symposium on Signal Processing and Information Technology, 18-21 Dec. 2005, 578- 582.

[19] 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.

[20] Lee, Y.K. & Chen, L.H proposed the paper "High capacity image steganographic model"(2000)

[21] Marvel, L. M. and Retter, C. T.: A Methodology for Data Hiding Using Images. Proceedings of IEEE Military Communications Conference (MILCOM98) Proceedings, Boston, MA, USA, 18-21 Oct 1998, 1044-1047.

[22] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[23]N.F.Johnson,S.Jajodia,Exploringsteganography:seeingtheunseenIEEE Computer31(2)(1998)26–34.

[24] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information Hiding – A survey", Proceedings of the IEEE, 87:07, July 1999

[25] Popescu, A.C.: Statistical Tools for Digital Image Forensics. Ph.D. Dissertation, Department of Computer Science, Dartmouth College, USA, (2005). Retrieved from: http://www.cs.dartmouth.edu/~farid/publications /apthesis05.html on 16-05-07 at 12:20.

.[26] Potdar, V. M., Han, S. and Chang, E.: Fingerprinted Secret Sharing Steganography for Robustness against Image Cropping Attacks. Proceedings of IEEE's 3rd International Conference on Industrial Informatics (INDIN), Perth, Australia, 10-12 August 2005

.[27] Provos, N. and Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security and Privacy, 01 (3): 32-44, May-June 2003

[28] R. C. Gonzalez and R. E. Woods, Digital Image Processing (2nd Edi-Vtion). Prentice Hall, January 2002.

[29] S. G. Mallat, \A theory for multiresolution signal decomposition: the wavelet representation," vol. 11, pp. 674{693, July 1989.

[30] S. L. Phung, A. Bouzerdoum, D. Chai, "Skin Segmentation Using Colour Pixel Classification: Analysis and Comparison", IEEE transactions on pattern analysis and machine intelligence, vol. 27, no. 1, pp. 148-154, 2005.

[31] Shirali-Shahreza, M. H. and Shirali-Shahreza, M.: A New Approach to Persian/Arabic Text Steganography. Proceedings of 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006), 10-12 July 2006.